CHAPTER 8

Configuring the Security Key for Administrative Communication

This chapter describes how to replace the default key used to secure administrative communications between the Cisco ACE XML Gateway and Manager. It covers these topics:

Overview

When the Manager establishes an SSL connection with a managed Gateway to deploy the policy or perform other administrative functions, it presents an X.509 client certificate and expects the Gateway to present its own server certificate in response. The Manager also uses a certificate to sign the Manager Audit Log, ensuring the integrity of logged information.

For enhanced security, you should replace the default certificates used for these purpose with your own. Each X.509 certificate's unique identity is based on a set of PKI keys. In addition to installing new certificates at initial configuration time, you may choose to install new keys periodically or in response to a possible security breach.

Your certificates can use software- or hardware-based cryptographic keys. Software-based keys are used by default. For greater security, it is recommended that you use a hardware-based keystore to generate and protect your keys.

To use hardware-based keys, your appliance must be equipped with nCipher hardware-based keystores and you must configure the appliances to use them, as described in Chapter 7, "Using Hardware Keystores and Security Worlds."

Installing Hardware-Backed Certificates

Configuring appliances to use hardware-based keys for bilateral authentication is a two-part process:

- You must install a new server certificate on each ACE XML Gateway in a cluster and inform the Manager that the ACE XML Gateway presents this certificate for bilateral authentication.

- You must install a new client certificate on the Manager and inform each ACE XML Gateway that the Manager presents that certificate for bilateral authentication.

Although the installation procedures are parallel in concept, the details pertinent to each vary slightly. To ensure successful installation, be sure to follow each section's step-by-step instructions carefully.

Note Installation of each hardware-backed certificate requires you to execute certain commands on the Manager appliance, and others on the Gateway appliance. When installing bilateral authentication certificates on a Gateway cluster, you must execute the Gateway-based commands on each Gateway appliance in the cluster.

Before you begin, make sure you have met the following prerequisites:

- One or more trusted Certificate Authorities (CAs) must be available for signing administrative certificates. Note that the Manager and Gateway are not required to use the same CA.
- You must already have configured each appliance as a gateway, manager, or standalone machine.
- You must already have configured each appliance to use an nCipher security world, as described in Chapter 7, "Using Hardware Keystores and Security Worlds."
- You must already have already enabled the use of a hardware-based SSL engine. For details, see "Enabling SSL Acceleration" section on page 9-61.

The steps are divided into two procedures:

- Gateway-to-Manager Authentication, page 8-46
- Manager-to-Gateway Authentication, page 8-49

Gateway-to-Manager Authentication

To configure an ACE XML Gateway to use hardware-backed keys in bilateral authentication, complete the following tasks:

- Inform the Manager of the CA that signed the certificate that the Gateway presents in bilateral authentication.
- On the ACE XML Gateway, generate a certificate signing request (CSR).
- Send the CSR to the Gateway's trusted CA for transformation into the Gateway's server certificate.
- Install the server certificate on the Gateway.

The following procedures provide details on these steps

Caution Before continuing, make sure that message traffic is diverted away from the Gateways that are to be configured. To do so, take the Gateways offline at the load-balancer that precedes them in your network. If you do not take the Gateways offline, in-progress transactions may be cut off when you perform these steps. Also, stop all Gateway services by setting it to inactive from the appliance shell (that is, from **Network Configuration** > **Cluster Configuration** menu item).

To install a hardware-backed certificate on the ACE XML Gateway, follow these steps:

Step 1 On the Manager appliance, run `bash` as the `root` user.

Step 2 Place a copy of the self-signed root certificate of the Gateway's trusted Certificate Authority (CA) in the Manager appliance's `/usr/local/reactivity/private` directory.

You can use any means you prefer to copy the file. For example, you can `ssh` to the Manager machine from the Gateway's `bash` shell and then use the `scp` command to copy the CA certificate. These instructions refer to this certificate as the Gateway CA certificate.

Note All Gateways this Manager controls must present the same Gateway CA certificate. If you need to configure your systems differently, contact Cisco support for assistance. The Manager and Gateway are not required to use the same CA. However, if you choose not to use the same CA for both sides of bilateral certificate exchange, be sure to install the correct CA certificate on each machine.

Step 3 In the Manager shell, change directories to the private directory, as follows:

```
cd /usr/local/reactivity/private/
```

Step 4 Execute the following command to back up the Manager's current database of trusted CAs:

```
mv trustkeystore private/trustkeystore.bak
```

This command renames the `trustkeystore` file as the `trustkeystore.bak` file. The `trustkeystore` file is the list of CAs the Manager trusts. In the next step, you generate a new `trustkeystore` file.

Note In the next example and in the rest of this chapter, commands longer than a single line wrap to the next line. The backslash character ("\") indicates a line that wraps in this way. When typing these examples (or your own commands) into the `bash` shell, do not include the backslash characters.

Step 5 In the Manager shell, execute the following command to generate a new trusted CA database that contains an entry for the newly installed Gateway CA certificate:

```
/usr/java/j2sdk1.4.2_04/bin/keytool \
    -import -trustcacerts -alias ca_cert \
    -keystore trustkeystore \
     -storetype jks -file GCACERT.CRT \
    -storepass approuter
```

Where *`GCACERT.CRT`* is the filename of the local copy of the Gateway CA certificate you installed previously.

Step 6 Enter yes in response to the **Trust this certificate?** prompt.

The new certificate is added to the keystore and the **Certificate was added to keystore** message appears.

Step 7 On the Gateway machine, run bash as the root user.

The command prompt appears. Subsequent instructions refer to this terminal session as the Gateway shell.

Step 8 In the shell, change to the private directory:

```
cd /usr/local/reactivity/private/
```

Step 9 Execute the following command to back up the Gateway's current administrative server certificate:

```
mv server.pem server.pem.bak
```

Note To install certificates on a Gateway cluster, you must execute Gateway-based commands (such as this one) on each Gateway machine in the cluster.

Step 10 In the Gateway shell, generate a key and corresponding CSR by executing the `generatekey` command to generate a new nCipher-protected private key and corresponding certificate-signing request (CSR) for the Gateway, as follows:

```
/opt/nfast/bin/generatekey --batch embed \
protect=module recovery=1 size=1024 \
embedsavefile=server.pem \
x509dnscommon="gatewayhost" \
x509org="OrganizationName" x509locality="Belmont" \
x509province="California" x509country="US"
```

In your command, replace italicized text with values appropriate for your site. It is suggested that the value of the `x509dnscommon` parameter be the fully-qualified hostname the Manager uses to contact the Gateway, although this is not a hard requirement.

The system writes the CSR into `private/server_req.pem` and the shell displays information about the key generation operation. If successful, **Key successfully generated** appears at the bottom of the listing.

Step 11 Send the CSR data (the `server_req.pem` file) to the Gateway's trusted CA for transformation into a signed X.509 certificate.

The CA sends a signed certificate in reply. This certificate is the Gateway's server certificate; in other words, it is the certificate the Gateway presents to the Manager.

Step 12 If you receive the signed certificate from the CA as the body of an email, place only the certificate contents in a text file:

- Include the entire `BEGIN CERTIFICATE` line, the entire `END CERTIFICATE` line, and everything in between.
- On your local file system, save the file using a valid Linux filename, that is, don't use spaces, apostrophes, ampersands, and other unusual characters in this filename.

Step 13 In the Gateway shell, execute the following command in the `private` directory to install the signed certificate on the Gateway:

```
$ cat GCERT.CRT >> server.pem
```

In your command, replace the *`GCERT.CRT`* with the filename of the signed certificate.

Note Be sure to use the >> output redirection operator to append the signed certificate to the `server.pem` file rather than replacing it. If the file is replaced, the private key that the `generatekey` tool placed in this file will be lost, and the keystore will not recognize the certificate as valid. To recover from this error, you must repeat all the instructions in this section to generate a new key, a new CSR, and a new certificate to install.

If you have completed all of these steps successfully, this Gateway is now configured to use hardware-backed keys for bilateral certificate exchange: the Gateway's hardware-backed administrative certificate is installed, and the Gateway has been informed of the CA to use to validate the certificate the Manager presents.

You can now configure other Gateways in the cluster similarly.

Manager-to-Gateway Authentication

To configure a Manager to use hardware-backed keys in bilateral authentication, you must complete these tasks:

- Inform the ACE XML Gateways of the CA that signed the certificate the Manager presents in bilateral authentication. You must perform this particular step on each ACE XML Gateway in the cluster.
- Generate a certificate signing request (CSR) that utilizes hardware-based keys on the Manager.
- Send the CSR to the Manager’s trusted CA for transformation into the Manager's client certificate.
- Install the client certificate on the Manager.

To install a hardware-backed administrative client certificate on the Manager, take the following steps:

Step 1 Place a copy of the self-signed root certificate of the Manager's trusted Certificate Authority (CA) in the following directory of each Gateway machine this Manager controls:

```
/usr/local/reactivity/private/
```

Use scp or the secure file transfer mechanism you prefer to copy the file. The scp utility would be run from the Manager's `bash` shell to copy the Manager's CA certificate onto the Gateway appliance as follows:

```
ssh gatewaymachine -l root
cd /usr/local/reactivity/private/
scp root@manangername:/pathToMCACert/MCAERT.CRT .
```

In this example, *`MCACERT.CRT`* file is the self-signed root certificate of the CA who signed the certificate the Manager presents to the Gateway. Subsequent instructions refer to this certificate as the Manager CA certificate. In the example code, this file resides on the *`managername`* computer in the *`pathToMCACert`* directory. The `scp` command copies this file into the `/usr/local/reactivity/private` directory on the *`gatewaymachine`* Gateway appliance.

The *`MCACERT.CRT`* file must be the PEM-format, self-signed, root certificate of the CA that signs the certificate the Manager presents in bilateral certificate exchanges. The Gateway and Manager need not both use the same CA to verify the respective certificates presented to them. However, if you choose not to use the same CA for both sides of the bilateral certificate exchange, be sure to install the correct CA certificate on each machine.

Step 2 On the Gateway machine, run `bash` as the `root` user.

Step 3 In the Gateway shell, execute the following command to set the working directory to the top-level directory:

```
cd /usr/local/reactivity/private/
```

Step 4 In the Gateway shell, execute the following command to back up the Manager CA certificate currently installed on the Gateway:

```
mv ca.crt ca.crt.bak
```

This command line renames the `ca.crt` file as the `ca.crt.bak` file. Shortly, you'll install a new `ca.crt` file.

Step 5 In the Gateway shell, execute the following command to install a new Manager CA certificate on the Gateway:

```
cp MCACERT.CRT ca.crt
```

Replace *`MCACERT.CRT`* with the filename of the local copy of the CA certificate you installed previously.

Step 6 On the Manager appliance, run `bash` as the `root` user.

Step 7 On the Manager shell, change to the private directory as follows:

```
cd /usr/local/reactivity/private/
```

Step 8 In the shell, execute the following command to back up the Manager's current hardware key database:

```
mv client.ncipher client.ncipher.bak
```

This command renames the `client.ncipher` file as `client.ncipher.bak`. This file contains hardware-based private keys the Manager uses to connect to the Gateways it manages. In the next step, you generate a new `client.ncipher` file.

Step 9 In the Manager shell, execute the following command from the `reactivity` directory to generate a new nCipher-protected private key for use with the certificate the Manager's web-based interface presents:

```
bin/ncipherkeytool -genkey -keystore private/client.ncipher -alias mykey -keyalg RSA
-keysize 1024 -dname "CN=managerhostname, O=CompanyName,L=Belmont,ST=California,C=US"
```

Replace the *`italicized`* values for the `CN,O,L, and ST` fields with values that are appropriate for your site. In particular, the `CN=` value must be the fully-qualified hostname of the Manager machine on which you are installing the certificate.

Step 10 In the Manager shell, enter the following command to generate a CSR based on the new nCipher-protected private key:

```
bin/ncipherkeytool -certreq -keystore private/client.ncipher -alias mykey -file
client.req
```

The system writes the CSR into the `client.req` file. If you like, you can inspect this file to ensure that it contains a valid certificate signing request.

Step 11 Send the CSR data (the `client.req` file) to the Manager's trusted CA for transformation into a signed X.509 certificate.

Keep in mind that this certificate is the Manager's client certificate, that is, the one the Manager presents to Gateways.

Step 12 When you receive the signed certificate from the CA as an email, paste only the certificate contents into a text file:

- Include the entire `BEGIN CERTIFICATE` line, the entire `END CERTIFICATE` line, and everything in between.
- On your local file system, save the file using a valid Linux filename: don't use spaces, apostrophes, ampersands, and other unusual characters in this filename.

Step 13 In the Manager shell, execute the following command to install the Manager's trusted CA certificate in the Manager's nCipher-protected keystore:

```
bin/ncipherkeytool -import -trustcacerts \
   -keystore private/client.ncipher -alias ca_cert -file MCACERT.CRT
```

When you type this command, replace the *`MCACERT.CRT`* parameter with the filename of the local copy of the Manager CA certificate you installed previously.

The Shell prompts you to confirm the operation. Its output looks similar to the following:

```
Owner: EMAILADDRESS=name@example.com,
  CN=Some CA, OU=Engineering, O="Beagle, Inc.",
  L=Belmont,  ST=California, C=US Issuer:
  EMAILADDRESS=name@example.com, CN=Some CA,
  OU=Engineering, O="Beagle, Inc.", L=Belmont,
  ST=California, C=US Serial number: 0
Valid from: Thu Dec 09 20:31:59 UTC 2004
     until: Wed Dec 09 20:31:59 UTC
  2009
Certificate fingerprints:
           MD5:  XX:   hellip  :XX
           SHA1: XX:   hellip  :XX
Trust this certificate? [no]:
```

The Manager and Gateway are not required to use the same CA to verify the certificates presented to them. However, if you choose not to use the same CA for both sides of the bilateral certificate exchange, be sure to install the correct CA certificate on each machine.

Step 14 In the Manager shell, enter `yes` to trust this certificate.

The shell adds the new certificate to the keystore and displays the **Certificate was added to keystore** message.

Step 15 In the Manager shell, enter the following command to install the new Manager client certificate in the Manager's nCipher keystore:

```
bin/ncipherkeytool -import  \
     -keystore private/client.ncipher \
     -alias mykey -file MCERT.CRT
```

When you type this command, replace the *`MCERT.CRT`* parameter with the filename of a local copy of the signed X.509 certificate the Manager's trusted CA returned in response to your certificate signing request.

If the ncipherkeytool command installed the manager's client certificate successfully, the shell displays the **Certificate reply was installed in keystore** message.

Step 16 To have the Manager's present the new certificate for browser connections to the web console:

a. Open for editing the following Manager properties file:
`/usr/local/reactivity/config/webapp.properties`

b. Change the following line:

```
ssl.client.keystore=/usr/local/reactivity/private/client.p12
```

to:

```
ssl.client.keystore=/usr/local/reactivity/private/client.ncipher
```

c. Change the following line:

```
ssl.client.storetype=pkcs12
```

to:

```
ssl.client.storetype=ncipher.sworld
```

Step 17 In the Manager shell, execute the following command to set agateway as the owner and group of the webapp.properties file:

```
chown agateway:agateway
   /usr/local/reactivity/config/webapp.properties
```

Step 18 Verify the ownership change by typing the following command:

```
ls -la /usr/local/reactivity/config
```

The shell lists the contents of the `config` directory. In the listing, the owner and group assigned to the `webapp.properties` file should be agateway, as displayed in the following:

```
-rw-r--r-- 1 agateway agateway 2874 Feb 8 00:34 webapp.properties
```

Once you complete these steps, the Manager uses hardware-backed keys for bilateral certificate exchange. If you also configured all Gateways that this Manager controls, the Manager and Gateways can now use their newly installed hardware-backed certificates for bilateral authentication.

To test the certificate change, see "Testing the Administrative Certificate Change" section on page 8-57.

Installing Software-Backed Certificates

Instead of using hardware-backed keys, you can install new software-backed keys for bilateral authentication. The process entails two parts:

- You must install a new server certificate on each ACE XML Gateway in a cluster and inform the Manager that the ACE XML Gateway presents this certificate for bilateral authentication.
- You must install a new client certificate on the Manager and inform each ACE XML Gateway that the Manager presents that certificate for bilateral authentication.

Although the installation procedures are parallel in concept, the details pertinent to each vary slightly. To ensure successful installation, be sure to follow each section's step-by-step instructions carefully.

Before you begin, make sure you have met the following prerequisites:

- One or more trusted Certificate Authorities (CAs) must be available for signing administrative certificates. Note that the Manager and Gateway are not required to use the same CA.
- You must already have configured each appliance as a gateway, manager, or standalone machine.

The steps are divided into two procedures:

- Gateway-to-Manager Authentication, page 8-52
- Manager-to-Gateway Authentication, page 8-54

Gateway-to-Manager Authentication

To configure an ACE XML Gateway to use software-backed keys in bilateral authentication, complete the following tasks:

- Inform the Manager of the CA that signed the certificate that the Gateway presents in bilateral authentication.
- On the ACE XML Gateway, generate a certificate signing request (CSR).
- Send the CSR to the Gateway's trusted CA for transformation into the Gateway's server certificate.
- Install the server certificate on the Gateway.

The following procedures provide details on these steps.

⚠ **Caution** Before continuing, make sure that message traffic is diverted away from the Gateways that are to be configured. To do so, take the Gateways offline at the load-balancer that precedes them in your network. If you do not take the Gateways offline, in-progress transactions may be cut off when you perform these steps. Also, stop all Gateway services by setting it to inactive from the appliance shell (that is, from **Network Configuration** > **Cluster Configuration** menu item).

To install a software certificate on the ACE XML Gateway, follow these steps:

Step 1 On the Manager appliance, run bash as the root user.

Step 2 Place a copy of the self-signed root certificate of the Gateway's trusted Certificate Authority (CA) in the Manager appliance's /usr/local/reactivity/private/ directory.

You can use any means you prefer to copy the file. For example, you can ssh to the Manager machine from the Gateway's bash shell and then use the scp command to copy the CA certificate. These instructions refer to this certificate as the Gateway CA certificate.

Note All Gateways this Manager controls must present the same Gateway CA certificate. If you need to configure your systems differently, contact Cisco support for assistance. The Manager and Gateway are not required to use the same CA. However, if you choose not to use the same CA for both sides of bilateral certificate exchange, be sure to install the correct CA certificate on each machine.

Step 3 In the Manager shell, change directories to the following directory:

```
cd /usr/local/reactivity/private/
```

Step 4 Execute the following command to back up the Manager's current database of trusted CAs:

```
mv trustkeystore trustkeystore.bak
```

This command renames the trustkeystore file as the trustkeystore.bak file. The trustkeystore file is the list of CAs the Manager trusts. In the next step, you generate a new trustkeystore file.

Note In the next example and in the rest of this chapter, commands longer than a single line wrap to the next line. The backslash character ("\") indicates a line that wraps in this way. When typing these examples (or your own commands) into the bash shell, do not include the backslash characters.

Step 5 In the Manager shell, execute the following command to generate a new trusted CA database that contains an entry for the newly installed Gateway CA certificate:

```
/usr/java/j2sdk1.4.2_04/bin/keytool \
    -import -trustcacerts -alias ca_cert \
    -keystore private/trustkeystore \
     -storetype jks -file GCACERT.CRT \
    -storepass approuter
```

Where *GCACERT.CRT* is the filename of the local copy of the Gateway CA certificate you installed previously.

Step 6 Enter yes in response to the **Trust this certificate?** prompt.

The new certificate is added to the keystore and the **Certificate was added to keystore** message appears.

Step 7 On the Gateway machine, run bash as the root user.

The command prompt appears. Subsequent instructions refer to this terminal session as the Gateway shell.

Step 8 In the Gateway shell, change directories to:

```
cd /usr/local/reactivity/private/
```

Step 9 Execute the following command to back up the Gateway's current administrative server certificate:

```
mv server.pem server.pem.bak
```

Note To install certificates on a Gateway cluster, you must execute Gateway-based commands (such as this one) on each Gateway machine in the cluster.

Step 10 In the Gateway shell, generate a key and corresponding CSR by entering the following two commands:

```
$ openssl genrsa -out server.pem 1024
$ openssl req -key server.pem \
-out server_req.pem -new -subj \
"/CN=gatewayhost/OU=myorgunit/O=MyCompany/L=Belmont/ST=California/C=US"
```

In your command, replace italicized text with values appropriate for your site. It is suggested that the CN value be the fully-qualified hostname the Manager uses to contact the Gateway, although this is not a hard requirement.

Step 11 Send the CSR data (the `server_req.pem` file) to the Gateway's trusted CA for transformation into a signed X.509 certificate.

The CA sends a signed certificate in reply. This certificate is the Gateway's server certificate; in other words, it is the certificate the Gateway presents to the Manager.

Step 12 If you receive the signed certificate from the CA as the body of an email, place only the certificate contents in a text file:

- Include the entire `BEGIN CERTIFICATE` line, the entire `END CERTIFICATE` line, and everything in between.
- On your local file system, save the file using a valid Linux filename, that is, don't use spaces, apostrophes, ampersands, and other unusual characters in this filename.

Step 13 From the Gateway shell, execute the following command in the private directory to install the signed certificate on the Gateway:

```
$ cat GCERT.CRT >> server.pem
```

In your command, replace the *`GCERT.CRT`* with the filename of the signed certificate.

Note Be sure to use the >> output redirection operator to append the signed certificate to the `server.pem` file rather than replacing it. If the file is replaced, the private key that the `generatekey` tool placed in this file will be lost, and the keystore will not recognize the certificate as valid. To recover from this error, you must repeat all the instructions in this section to generate a new key, a new CSR, and a new certificate to install.

If you completed all of these steps successfully, this Gateway is now configured to use the new key for bilateral certificate exchange; that is, the Gateway's administrative certificate is installed and the Gateway has been informed of the CA to use to validate the certificate the Manager presents.

You can now configure other Gateways in the cluster similarly.

Manager-to-Gateway Authentication

To configure a Manager to use software-backed keys in bilateral authentication for communications with the Gateway, complete these tasks:

- Inform the ACE XML Gateways of the CA that signed the certificate the Manager presents in bilateral authentication. You must perform this particular step on each ACE XML Gateway in the cluster.
- Generate a certificate signing request (CSR) for the key on the Manager.
- Send the CSR to a CA for transformation into the Manager's client certificate.
- Install the client certificate on the Manager.

To install a software-backed client certificate on the Manager, follow these steps:

Step 1 Place a copy of the self-signed root certificate of the Manager's trusted Certificate Authority (CA) in the following directory of each Gateway machine this Manager controls:

```
/usr/local/reactivity/private/
```

Use scp or the secure file transfer mechanism you prefer to copy the file. The scp utility would be run from the Manager's `bash` shell to copy the Manager's CA certificate onto the Gateway appliance as follows:

```
ssh gatewaymachine -l root
cd /usr/local/reactivity/private/
scp root@manangername:/pathToMCACert/MCAERT.CRT .
```

In this example, *`MCACERT.CRT`* file is the self-signed root certificate of the CA who signed the certificate the Manager presents to the Gateway. Subsequent instructions refer to this certificate as the Manager CA certificate. In the example code, this file resides on the *`managername`* computer in the *`pathToMCACert`* directory. The `scp` command copies this file into the `/usr/local/reactivity/private` directory on the *`gatewaymachine`* Gateway appliance.

The *`MCACERT.CRT`* file must be the PEM-format, self-signed, root certificate of the CA that signs the certificate the Manager presents in bilateral certificate exchanges. The Gateway and Manager need not both use the same CA to verify the respective certificates presented to them. However, if you choose not to use the same CA for both sides of the bilateral certificate exchange, be sure to install the correct CA certificate on each machine.

Step 2 On the Gateway machine, run `bash` as the `root` user.

Step 3 In the Gateway shell, execute the following command to set the working directory to the top-level directory:

```
cd /usr/local/reactivity/
```

Step 4 In the Gateway shell, execute the following command to back up the Manager CA certificate currently installed on the Gateway:

```
mv ca.crt ca.crt.bak
```

This command line renames the `ca.crt` file as the `ca.crt.bak` file. Shortly, you'll install a new `ca.crt` file.

Step 5 In the Gateway shell, execute the following command to install a new Manager CA certificate on the Gateway:

```
cp MCACERT.CRT ca.crt
```

Replace *`MCACERT.CRT`* with the filename of the local copy of the CA certificate you installed previously.

Step 6 On the Manager appliance, run `bash` as the `root` user.

Step 7 On the Manager shell, change directories as follows:

```
cd /usr/local/reactivity/private/
```

Step 8 From the `private` directory, execute the following command to back up the Manager's current key database:

```
mv client.p12 client.p12.bak
```

This command renames the `client.p12` file as `client.p12.bak`. This file contains hardware-based private keys the Manager uses to connect to the Gateways it manages. In the next step, you generate a new `client.p12` file.

Step 9 Now generate a key and corresponding CSR by entering the following two commands:

```
$ openssl genrsa -out client.pem 1024
$ openssl req -key client.pem \
-out client_req.pem -new -subj \
"/CN=gatewayhost/OU=myorgunit/O=MyCompany/L=Belmont/ST=California/C=US"
```

In your command, replace italicized text with values appropriate for your site.

Step 10 Send the CSR data (the `client_req.pem` file) to a trusted CA for transformation into a signed X.509 certificate.

Step 11 If you receive the signed certificate from the CA as the body of an email, place only the certificate contents in a text file:

- Include the entire `BEGIN CERTIFICATE` line, the entire `END CERTIFICATE` line, and everything in between.
- On your local file system, save the file using a valid Linux filename, that is, don't use spaces, apostrophes, ampersands, and other unusual characters in this filename.

Move the signed certificate to the Manager file system.

Step 12 In the private directory of the Manager shell, execute the following command to install the signed certificate in the `client.pem` file:

```
$ cat GCERT.CRT >> client.pem
```

In your command, replace the *`GCERT.CRT`* with the filename of the signed certificate.

Note Be sure to use the >> output redirection operator to append the signed certificate to the `client.pem` file rather than replacing it. If the file is replaced, the private key that the `generatekey` tool placed in this file will be lost, and the keystore will not recognize the certificate as valid. To recover from this error, you must repeat all the instructions in this section to generate a new key, a new CSR, and a new certificate to install.

Step 13 Convert the client PEM file to a PKCS#12 file with the following command:

```
openssl pkcs12 -export -out client.p12 -in client.pem
```

Step 14 When the prompt appears to enter the export password, enter `approuter` as the password. Confirm the password you typed when prompted.

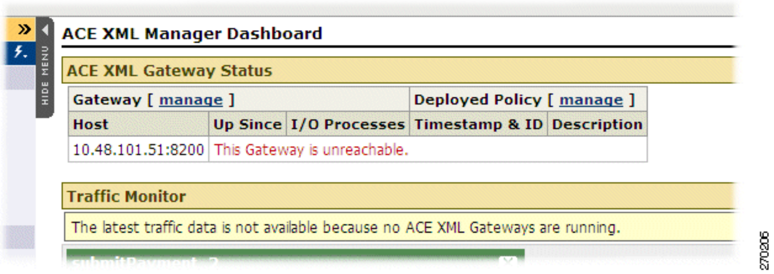
Once you complete these steps, the Manager uses the new keys for bilateral certificate exchange. To test the certificate change, restart the Manager and make sure it has connectivity to the Gateway, as described in the following section, "Testing the Administrative Certificate Change" section on page 8-57.

Testing the Administrative Certificate Change

After configuring the Manager and Gateways as previously described, you can test the installation by viewing the event log in the Manager web console. Navigating to the event log requires the Manager to perform bilateral certificate exchange with each managed Gateway to retrieve the entries in the log.

Once you log into the Manager's web console, make sure that the Dashboard does not display warnings indicating that the Manager cannot contact any Gateway cluster members, as shown in Figure 8-1.

Figure 8-1 Unreachable Gateway



ACE XML Manager Dashboard

ACE XML Gateway Status

Gateway [manage]			Deployed Policy [manage]	
Host	Up Since	I/O Processes	Timestamp & ID	Description
10.48.101.51:8200	This Gateway is unreachable.			

Traffic Monitor

The latest traffic data is not available because no ACE XML Gateways are running.

If you replace the certificates without completing other parts of the installation process correctly, you may be able to log into the Manager web console or establish terminal sessions with the Manager or Gateways while still not having a fully functional installation. Assuming the Gateway was configured correctly prior to installation of the hardware-based keys, errors loading a certificate or reading the keystore may prevent the Gateway from starting successfully. If you see this message, you may be able to discern the problem by examining the Event Log.

While viewing the **Event Log**, look for **Notice**, **Warning** or **Alert** messages that indicate problems with the hardware keystore or other problems starting up.

In order to populate the **Event Log** with entries, the Manager must perform bilateral certificate exchange with each of the Gateways in its cluster as a prerequisite to polling them for new events to enter in the log. Therefore, if you can view an **Event Log** configured at **Notice** level or higher, and it contains no errors related to certificates, hardware keystores, or communications between the Manager and its Gateway cluster, the certificates used for bilateral certificate exchange are installed correctly.

Changing the Audit Log Signing Credential

The Console Audit Log is a Manager web console page that shows the administrative-level changes affecting the system, such as policy deployment, changes to the current policy, changes to the user privileges of administrative accounts, and so on. In addition to the change made, the audit log shows who made the changes.

The audit log uses a PKI credential to authenticate processes before allowing them to edit and sign the audit log. This section describes how to substitute hardware-backed keys in place of the software-based keys that this credential uses normally.

Before completing these procedures, you must:

- Enable the use of the hardware-based SSL engine. For details, see "Enabling SSL Acceleration" section on page 9-61.
- Add the appliance to an nCipher security world.

To change the audit log signing credential:

Step 1 On the Manager machine, log into the appliance shell as the `root` user.

Step 2 Choose the **Manage Gateway Processes** menu item.

Step 3 In the **Manage Gateway Processes** menu, choose **Stop Manager**.

The appliance shuts down the Manager process and displays a status screen indicating the success of this operation.

Step 4 Press the **Enter** key to dismiss the status screen.

Step 5 In the **Manage Gateway Processes** menu, choose **Return to Main Menu**.

Step 6 Choose the **Advanced Options** item from the **Main Menu**.

Step 7 Choose the **Run bash** item from the **Advanced Options** menu.

Step 8 At the `bash` command prompt, change directories to the following directory:

```
cd /usr/local/reactivity
```

Step 9 To generate a new nCipher-protected keystore and self-signed certificate for audit log signing, execute the following command:

```
$ bin/ncipherkeytool -genkey
   -keystore private/auditlog.ncipher
   -alias client -keyalg RSA -keysize 1024
   -dname "CN=auditlog"
```

To verify success of this command, list the contents of the `/usr/local/reactivity/private` directory to verify the presence of a newly-created `auditlog.ncipher` file. For example, you might use the following command to do so:

```
ls -lt private
```

Step 10 Back up the current audit log certificate by entering the command:

```
$ mv private/auditlog.crt private/auditlog.crt.bak
```

This command renames `auditlog.crt` as `auditlog.crt.bak`. To verify the operation, list the contents of the `private` directory. If the rename operation succeeded, this directory contains an `auditlog.crt.bak` file and no `auditlog.crt` file.

Step 11 Execute the following command to extract the new audit log certificate from the keystore for log verification utility use:

```
$ bin/ncipherkeytool -export -rfc -keystore private/auditlog.ncipher
     -alias client -file private/auditlog.crt
```

The shell displays the **Certificate stored in file <private/auditlog.crt>** message.

Step 12 Edit `/usr/local/reactivity/config/webapp.properties` as follows:

a. Change `p12` to `ncipher` in the following line.

```
audit.log.private.key.pcks12= /usr/local/reactivity/private/auditlog.p12
```

to:

```
audit.log.private.key.pcks12= /usr/local/reactivity/private/auditlog.ncipher
```

b. Change `pkcs12` to `ncipher.sworld` in the following line:

```
audit.log.signing.keystore.type=pkcs12
```

to:

```
audit.log.signing.keystore.type=ncipher.sworld
```

Step 13 In the Manager shell, execute the following command to set `agateway` as the owner and group of `webapp.properties`:

```
chown agateway:agateway /usr/local/reactivity/config/webapp.properties
```

Step 14 Confirm the file ownership change by executing the following command to view the owner and group assigned to the `webapp.properties` file:

```
ls -la /usr/local/reactivity/config
```

The shell lists the contents of the `config` directory. In this listing, the owner and group assigned to the `webapp.properties` file should be agateway, as in following example:

```
-rw-r--r-- 1 agateway agateway 2874 Feb 8 00:34 webapp.properties
```

Step 15 Reset the audit log signing state by entering the following command:

```
$ rm auditlogs/audit.console.current
```

This command removes the current audit log. In a subsequent step, you'll generate a new audit log signed with the hardware-based certificate.

Step 16 Exit the `bash` shell.

Step 17 In the **Advanced Options** menu, choose the **Return to Main Menu** item.

Step 18 Choose the **Manage Gateway Processes** menu item.

Step 19 Choose **Start Manager**.

The appliance attempts to restart the Manager process and displays a status screen indicating the status of the operation.

Step 20 Press the **Enter** key to dismiss the status screen.

The **Manage Gateway Processes** menu reappears.

Step 21 Log into the Manager web console (not the appliance shell) as a user with administrator role.

The **Dashboard** appears.

Step 22 Click the **Reports and Tools > Event Log** link.

The **Event Log** should display the following message:

A "/usr/local/reactivity/auditlogs/audit.console.current" not found. This file should only be missing on a newly installed Manager web console.

In the previous step, you removed the `audit.console.current` file, so this error message is to be expected. The Manager writes a new log file in place of the file you removed, so you won't see this message on subsequent logins.