



APPENDIX **D**

Generating SSL Certificates

SSL certificates on a Cisco IPICS server expire after three years and must be replaced. Complete the following instructions to manually generate SSL certificates on a Cisco IPICS server.



Caution

This procedure automatically restarts the Cisco IPICS server software. Perform this procedure only when restarting the Cisco IPICS server software will not interrupt critical operations.




Note

If the Cisco IPICS servers are configured with high availability (HA), you must temporarily disable HA before you generate the SSL certificates. You must generate the certificates on both the primary and standby servers, and then reenale HA before installing the certificates on the iPhone.

To generate SSL certificates, perform the following procedure.

Procedure

- Step 1** (HA configurations only) Unconfigure HA on the active Cisco IPICS server as described in the [“Unconfiguring HA” section on page 10-6](#).
 - Step 2** At the end of the [“Unconfiguring HA” section on page 10-6](#), complete the optional steps to delete the HA security certificates.
 - Step 3** Use a secure shell (SSH) client to log in to the primary Cisco IPICS server using the root account.
 - Step 4** Enter these commands to generate new SSL certificates:

```
[root]# cd /opt/cisco/ipics/security
[root]# sudo -u ipicsadmin ./security-manager unsetup
[root]# sudo -u ipicsadmin ./security-manager setup
[root]# service ipics start
```
 - Step 5** Wait a few minutes for the Cisco IPICS server software to restart.
 - Step 6** Log in to the Cisco IPICS administration console again and verify that the server operates correctly.
- **Note** If your web browser displays an error regarding the certificates, go to the browser certificate management page and delete the old trusted certificates.
- Step 7** (HA configurations only) Generate SSL certificates for the secondary Cisco IPICS server:
 - a. Use a secure shell (SSH) client to log in to the secondary Cisco IPICS server using the root account.

- b. Repeat [Step 3](#) through [Step 5](#) to generate SSL certificates for the secondary Cisco IPICS server.

Step 8 Log in to the Cisco IPICS Administration Console and reconfigure HA.

See the “[Configuring Cisco IPICS Servers for HA](#)” section on [page 10-3](#) for instructions. Be sure to establish trust between the HA servers, as described in [Step 8](#).
