DNCS System Release 5.0 Security Configuration Guide

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco Logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

Contents

Chapter 7 DNCS Web Services Security 53

About This Guide

Introduction

As networks become more complex, the requirements for data security become more important. It is no longer feasible to consider that the DNCS exists in a 'walled environment'; therefore, we have taken steps to enhance the security of your DNCS.

Notes:

- These changes were initiated due to the requests of our customers.
- If your password management and/or user account management is administered by an external LDAP, RADIUS, or Sudo system, you must manage your passwords and user accounts on that system and not on the DNCS. For more information, see *Enable RADIUS and LDAP Support in a DBDS for SR 5.0 Configuration Guide* (part number 4017610) or contact your system administrator for more information.

Purpose

This document contains instructions on changing your security defaults.

We recommend that you keep the operating system defaults to obtain the most benefit from these security features for your network. However, there may be times when you might need to change those defaults temporarily; for example, when you need to troubleshoot or when you need to unlock a user account. This document contains instructions on many of the DNCS security features. Any changes should be performed by a DNCS system administrator in collaboration with Cisco personnel so that your system remains fully functional. The DNCS system administrator should be well versed in the administration of a Sun/Solaris UNIX platform and must understand the ramifications of changing the security defaults.

You need to use your best judgment and abide by your company security policies and guidelines when changing or removing any DNCS security features associated with this system release.

Important: We recommend that you do **not** change the system defaults to retain the highest level of system security. Cisco® Systems, Inc. is not responsible for any damage that might occur to your DNCS or DBDS if you choose to change the system defaults.

Audience

This document is written for our customers' DNCS system administrators who are responsible for the security policies of their site. These system administrators should be well versed in UNIX security procedures and policies. Our engineers may also find this document to be useful.

Acronyms Used in This Document

The following table lists the acronyms used in this document and their description.

Acronym	Stands For...	Description
BSM	Solaris Basic Security Module	Auditing utility that logs significant amounts of information about system activity.
DBDS	Digital Broadband Delivery System	The entire (end-to-end) Cisco digital video network architecture.
DNCS	Digital Network Control System	A server that operates as a network control element that provides command and control data for most Cisco network elements that reside within the Cisco video control plane.
FTP	File Transfer Protocol	A protocol used to transfer files over a TCP/IP network. FTP includes the ability to log in to the network, list directories, and copy files.
HTTP	HyperText Transfer Protocol	The communications protocol used to connect to Web servers on the Internet or on a local network.
HTTPS	HyperText Transport Protocol Secure	A common, widely used protocol which includes a combination of the HTTP and SSL/TLS protocols that provide encrypted communication and secure identification of a given network web server. HTTPS is used to create secure communication channels over insecure networks.
OS	Operating System	A computer's or server's master control program.
RBAC	Role-Based Access Control	A Sun/Solaris security package which enables you to separate superuser capabilities and to package them in special user accounts (or *roles)* for assignment to specific individuals according to their job requirements.
RNCS	Regional Network Control System	Also known as a LIONN (lights-out network node); distributes parts of the control plane to provide hub-level control over specific aspects of the system's command and control data (for example, BFS and EAS).
SCP	Secure Copy Protocol	A secure version of the UNIX remote copy command.
SFTP	SSH File Transfer Protocol	A file transfer protocol using the secure SSH protocol.

Acronym	Stands For...	Description
SSL/TLS	Secure Sockets Layer / Transport Layer Security	SSL validates the identity of a Web site and creates an encrypted connection for sending data. TLS is a security protocol based on SSL. It uses digital certificates to authenticate the user as well as authenticate the network.
SSH	Secure Shell	A security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs, and serves as a secure client/server connection for applications.

Document Version

This is the first formal release of this document.

1

System Defaults and Access Control

Introduction

This chapter discusses the operating system defaults and role-based access control.

In This Chapter

Operating System Defaults

Important: Upgrading the DNCS System Release will invalidate any customized security settings you might have made. We recommend that you record any customized settings for future reference.

Note: The following defaults are applicable to the DNCS, the RNCS, and the Application Server, except where noted.

- **Operating System:** Solaris 10
- **Security Features:**
  - **Secure by Default** - OS is installed with minimal network services
  - **Networking**
    - SSH, FTP, and TFTP are the only network listening services installed by default for remote access; others are set to off or configured for only local machine access
    - X11 forwarding is also enabled for remote X-based UI access using SSH
  - **Restricted Network Resources** - Authorized users have access to all network resources, but the system itself has minimal exposure to the network, making unauthorized access very difficult
  - **System Monitoring** - Basic Security Module (BSM) provides monitoring of system events for logging and auditing (applies to the DNCS and RNCS only)

Operating system defaults are set up during system installation.

Important: We recommend that you do **not** change the system defaults to retain the highest level of system security. Cisco Systems, Inc. is not responsible for any damage that might occur to your DNCS or DBDS if you choose to change the system defaults.

System Access Overview

The method used for accessing the DNCS, RNCS, and Application Server has been expanded and modified in SR 5.0 to increase security while maintaining ease of use.

- Access to the Administrative Console is limited to users created on the DNCS.
- Remote terminal access on the DNCS, RNCS, and Application Server is also limited to users created on the DNCS, RNCS, and Application Server.

To create users, the create_users script is delivered with the DNCS, RNCS, and Application Server.

- Use the script delivered on the DNCS to create users that can log into the system remotely using SSH and access the Administrative Console. The users you create with the script on the DNCS can also access the DNCS locally on the console.
- Use the script delivered on the RNCS and Application Server to create users that can log into the system remotely using SSH or locally on the console.

Important: The create_users script on the DNCS creates two separate users with the same username:

- One instance of the username is for remote terminal access and local console access (OS User).
- The other instance of the username is for access to the Administrative Console (Web Interface User).

Although the username is exactly the same, the two instances of the username must be managed separately after the user is created.

For example, changing the password for the OS User will not apply to the Web Interface User. The password must be changed separately for the OS User and Web Interface User.

Role-Based Access Control

We have implemented role-based access control (RBAC) as part of the DNCS, RNCS, and Application Server operating systems. This access control allows system administrators to assign specific administrative control of parts of the operating system to users.

Important: You cannot log in directly or remotely to the DNCS, the RNCS, or the Application Server as the dncs user. You cannot log in remotely to the DNCS as the root user. You will need to set up individual user accounts for everyone who uses the DNCS, including support personnel and third-party applications. See ***User Account Defaults*** (on page 8) for more information.

Roles and Accounts Available on the DNCS, the RNCS, and the Application Server

This section describes the roles and accounts available on the DNCS, RNCS, and Application Server.

Roles

- **dncs Role —** The dncs role is the application administrator and user.

  Important: You cannot log in directly or remotely to the system as the dncs user.

- **dbreader Role —** DNCS Database Read-Only Role. This role can be used by remote clients to access the DNCS database in a read-only mode. For example, third-party scripts that run without dncs privileges can be authorized to assume the dbreader role so they can access the DNCS database in a read-only mode.

  Important: You cannot log in directly to the DNCS using "dbreader" and the dbreader role password.

Accounts

- **root User —** The root user is the system administrator account and has all privileges and rights except for access to the DNCS Web User Interface (WUI).

  Important: You cannot log into the DNCS remotely as the root user. However, you can log in at the DNCS console and at the ALOM port as the root user.

- **DNCS Administrator —** DNCS Administrator accounts are the only system accounts (other than root) that have permission to switch to the dncs role. These users have access to the DNCS Administrative Console.

- **DNCS Operator —** DNCS Operator accounts can be used on the system only to view logs and other application files.

- **Regular Users —** Regular User accounts do not have permission to view application logs or other application files. You can change a regular user to a

DNCS Administrator by adding the dncs role to that user account. See ***Assigning the dncs Role to a User Account*** (on page 13) for more information.

Role and Account Privileges for the DNCS Application

Role	WebUI Access	Files*		Commands		
		Read	Write	Read	Write	Alter
Root user	N	Y	Y	Y	Y	Y
DNCS role	N	Y	Y	Y	Y	N
DB Read Only role	N	N	N	Y	N	N
DNCS Administrator account	Y	Y	N	N	N	N
DNCS Operator account	N	Y	N	N	N	N
Regular users	N	N	N	N	N	N

*Refers to DNCS application files and DNCS executables only.

2

User Accounts and Roles

Introduction

This chapter discusses user accounts and roles, including how to add, edit, and delete user accounts and how to assign certain roles to user accounts.

Important: If your password management and/or user account management is administered by an external LDAP, RADIUS, or Sudo system, you must manage your passwords and user accounts on that system and not on the IBDS element.

In This Chapter

User Accounts

User Account Defaults

Regular User

- Cannot log into the Administrative Console
- Can log into the operating system (Solaris)
- Cannot read or write DNCS files
- Cannot execute DNCS application files
- Cannot switch to the dncs role

Operator

- Cannot log into the Administrative Console
- Can log into the operating system (Solaris)
- Can read but cannot write DNCS files
- Cannot execute DNCS application files
- Cannot switch to the dncs role

Administrator

- Can log into the Administrative Console
- Can log into the operating system (Solaris)
- Can read but not write DNCS files
- Cannot execute DNCS application files
- Can switch to the dncs role. Once switched to the dncs role:
  - Can read and write DNCS application files
  - Can execute DNCS application executable files

Creating a User Account

Important: If your password management and/or user account management is administered by an external LDAP, RADIUS, or Sudo system, you must manage your passwords and user accounts on that system and not on the DNCS. For more information, see *Enable RADIUS and LDAP Support in a DBDS for SR 5.0 Configuration Guide* (part number 4017610) or contact your system administrator for more information.

All applications (including third-party applications) and users who access the DNCS, RNCS, or Application Server require an updated user account. You can no longer log into the DNCS, RNCS, or Application Server using the generic dncs user credentials.

Note: The user will be required to change their password during their first successful operating system login session.

Important: We recommend creating an individual username for each user that will access the system. We do **NOT** recommend creating a single, generic username for use by multiple users.

1. Open an xterm window on the system.
2. Log into the system as root user.
3. Type `/dvs/admin/create_users` and press **Enter**. The create_users menu opens.
4. Type the number of the type of user you want to create:
   - 1: Add Regular User
   - 2: Add Operator
   - 3: Add Administrator

   Example: To add a regular user, type **1**.

   Note: See ***User Account Defaults*** (on page 8) for more information on the user types.
5. Type the name of the new user account and press **Enter**.

   Notes:
   - The username must be between 6 and 8 alphanumeric characters.
   - The username cannot contain special characters.

   Result: The **Do you wish to continue adding this user (Y/N)?** message appears.
6. Type **y** (for yes) and press **Enter**.
7. Type the **temporary OS password** for the user and press **Enter**.
8. Re-type the **temporary OS password** for the user and press **Enter**.

9 Did you select the option to create an Administrator account (option 3 in step 4)?

- If **yes**, the system prompts for the WebUI password. Follow these steps:

  a Type the user's **WebUI Administrative Console password** and press **Enter**.

  b Re-type the user's **WebUI Administrative Console password** and press **Enter**.

- If **no**, the create_users program reappears. Go to the next step.

10 Do you need to add another user?

- If **yes**, repeat this procedure from step 4.
- If **no**, type **q** (for quit) to close the create_users menu.

Change the User's Command Line Prompt and Enable Command Line vi Commands

Follow these instructions to change the new user's command line prompt and to enable vi commands at the command line.

1 Type `cd /export/home/[username]` and press **Enter**. The user's home directory becomes the active directory. Do not type the brackets in the command.

2 Open the user's **.profile** file in a UNIX text editor.

3 Add the following lines to the .profile file:

```
export PS1="$LOGNAME@'hostname':$PWD>"
set -o vi
```

4 Save and close the user's .profile file.

Unlocking a User Account

Note: This topic applies to the OS login accounts on the DNCS, the RNCS, and the Application Server. Account locking is not applicable to the WebUI users on the DNCS.

1 Open an xterm window on the system.

2 Log into the system as root:

a At the prompt, type `su -` and press **Enter**.

b Type the **root password** and press **Enter**.

3 Type `passwd -s [username]` and press **Enter** to display the user account password attributes.

Notes:

- Substitute the user account name for [username] in the command. Do not type the brackets in the command.
- Locked user accounts display with **LK** immediately after the username.

Examples:

- **Locked user account:** `dncsuser LK 03/11/10 0 91 14`
- **Unlocked user account:** `dncsuser PS 03/11/10 0 91 14`

4 Type `passwd -r files -u [username]` and press **Enter**.

Note: Substitute the user account name for **[username]**. Do not type the brackets in the command.

Result: The user account is unlocked. The user account retains the original password. To change the password, refer to ***Changing User Account Passwords*** (on page 36).

5 Type `exit` and press **Enter** to close the xterm window.

Who Am I?

To determine your current ID or your session role, you can type one of the following from the command line and press **Enter**:

- `id`
- `/usr/ucb/whoami`

  The system returns the user ID of your current session or the session role of your current session.

Note: Command 2000 restricted user accounts are prohibited from executing this command.

Deleting a User Account

Use this procedure to delete users that were added using the create_users script. This procedure is valid for all systems.

Important: Do not delete any default user on the system.

1 Log into the system as root:

  a At the prompt, type `su -` and press **Enter**.

  b Type the **root password** and press **Enter**.

2 Review the user files in the user's home directory and move any files that should be retained to another directory, outside the user's home directory.

3 In an xterm window, type `userdel -r [username]` and press **Enter**. The system deletes the user's home directory.

  Note: Substitute the user's name for [username]. Do not type the brackets **[ ]** in the command.

4 Type `projdel user.[username]` and press **Enter**. The system removes the user from the /etc/project file.

  Note: Substitute the user's name for [username]. Do not type the brackets **[ ]** in the command.

5 Is the user you are deleting a Regular User?

- If **yes**, type `groupdel [username]` and press **Enter**. The system deletes the group associated with that user.

  Note: Substitute the user's name for [username]. Do not type the brackets **[ ]** in the command.

- If **no**, go to the next step.

6 Is the user you are deleting an Administrator Account on the DNCS?

- If **yes**, complete the following steps to delete the WebUI user account:

a Open the **/etc/apache2/user-conf/SAIdncs.digest** file with a text editor.

b Delete the entire line that contains the **username** to be deleted.

c Save and close the SAIdncs.digest file.

- If **no**, you are finished with this procedure.

Important: Even when you delete a user, the username still exists in the password history file. We do **not** recommend that you edit this file. If you delete a user, then add the same user again, that user's old password history remains in effect. Thus, the new account will not be able to change the password to any of the previous 5 passwords used by the old account.

Roles

Assigning the dncs Role to a User Account

Use this procedure to assign the dncs role to an existing user account.

1 Log into the system as root:

   a At the prompt, type `su -` and press **Enter**.

   b Type the **root password** and press **Enter**.

2 In an xterm window, type `roles [user name]` and press **Enter**.

   Note: Substitute the user's name for **[user name]**. Do not type the brackets **[ ]** in the command.

   Result: The system displays the roles currently granted to the user, if any. If the dncs role has not been assigned to the user, continue with this procedure.

3 In the xterm window, type `usermod -R dncs [user name]` and press **Enter**.

   Note: Substitute the user's name for **[user name]**. Do not type the brackets **[ ]** in the command.

   Result: The system assigns the dncs role to the user account.

Authorizing Access to the Administrative Console

Use this procedure to authorize web access to the Administrative Console for an existing OS username.

1 Open an xterm window on the DNCS.

2 Log into the system as root:

   a At the prompt, type `su -` and press **Enter**.

   b Type the **root password** and press **Enter**.

3 Type the following and press **Enter**:

```
/usr/apache2/bin/htdigest /etc/apache2/user-
conf/SAIdncs.digest "Cisco DNCS" [username]
```

   Notes:

   - This is a single command.
   - Substitute the user account name for [username]. Do not type the brackets in the command.

4 Type the **new Web Interface password** for the user and press **Enter**.

5 Type the **new password again** and press **Enter**. The system compares the two password entries.

6 Did the "They don't match, sorry" message appear?

- If **yes**, the two passwords do not match. Go back to step 3 and re-type the command.
- If **no**, the system prompt is returned. You are finished with this procedure.

Removing the dncs Role From a User Account

Use this procedure to remove the dncs role from an existing user.

Important: This procedure removes ALL roles from the user account. If this user account is assigned to multiple roles, you will need to reassign those roles to the user account after completing this procedure.

1 Log into the system as root:

a At the prompt, type `su -` and press **Enter**.

b Type the **root password** and press **Enter**.

2 In an xterm window, type `roles [user name]` and press **Enter**.

Note: Substitute the user's name for **[user name]**. Do not type the brackets **[ ]** in the command.

Result: The system displays the roles currently granted to the user, if any. If the dncs role has been assigned to the user, continue with this procedure.

3 In the xterm window, type `usermod -R "" [user name]` and press **Enter**.

Note: Substitute the user account name for **[user name]**. Do not type the brackets **[ ]** in the command.

Example: Type `usermod -R "" jmodelo` and press **Enter** to remove the dncs role from user account **jmodelo**.

Result: The system removes all roles from the user account. Any remaining roles listed in step 2 must be re-added to the system.

Disable Access to the Administrative Console

Use this procedure to disable web access to the Administrative Console for an existing user.

1 Log into the system as root:

a At the prompt, type `su -` and press **Enter**.

b Type the **root password** and press **Enter**.

2 Open the **/etc/apache2/user-conf/SAIdncs.digest** file with a text editor.

3 Delete the entire line that contains the **username** to be deleted.

4 Save and close the SAIdncs.digest file.

3

Sessions

Introduction

This chapter discusses sessions, including how to log in, how to deal with timeouts and session locks, and how to kill sessions.

In This Chapter

Logging into the DNCS, RNCS, and the Application Server

This section details the procedures for logging onto the DNCS from a CDE terminal, from a Windows PC, and from an Apple Macintosh. This section also includes information for logging into the RNCS and Application Server from a Windows PC or from an Apple Macintosh.

Logging into the DNCS from the CDE Terminal

Follow this procedure to log into the CDE at the DNCS terminal.

1 At the DNCS terminal, type your **DNCS administrator user name** and press **Enter**.

2 At the prompt, type your **password** and press **Enter**.

Note: If this is your first time logging into the system, you will need to complete the following steps:

a A prompt appears for you to select your default desktop. Select **Common Desktop Environment (CDE)** and click **OK**.

Important: The Java Desktop System is not supported in this system release.

Result: A message similar to the following appears:

```
CDE has been deprecated
```

b Click **Do not show this message again** and click **OK**.

3 Before you execute any DNCS commands (such as dncsStart or dncsStop) or launch any DNCS user interface windows (such as the Administrative Console), type `sux - dncs` and press **Enter**.

Type the **dncs role password**. An xterm window session opens when the dncs role opens.

Logging into the Administrative Console Remotely

The Administrative Console is accessible using a web browser on a remote computer.

Note: The web server on the DNCS must be configured to allow remote access to the Administrative Console. The necessary web server configuration should be implemented during the upgrade or initial installation of DNCS 5.0. See ***DNCS Web Services Security*** (on page 53) for more information.

Supported Browser

When viewing the Web UIs (WUIs) in SR 5.0, Cisco recommends using Firefox version 3.0.7 for Solaris and version 3.6.16 for both Windows, Linux and Mac operating systems.

Notes:

- Cisco engineers tested the WUIs with Firefox 3.0.7 on Solaris and version 3.6.16 on Windows, Linux, and Mac operating systems.
- Firefox version 4.0 is **not** supported.
- The Safari and Opera browsers, for Windows or for Mac, are **not** supported.

Accessing the Administrative Console

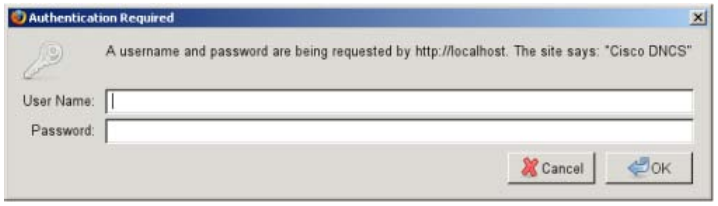
1 Navigate to the following location in the web browser on your computer.

`http://[DNCS IP Address]/dncs/`

Example:

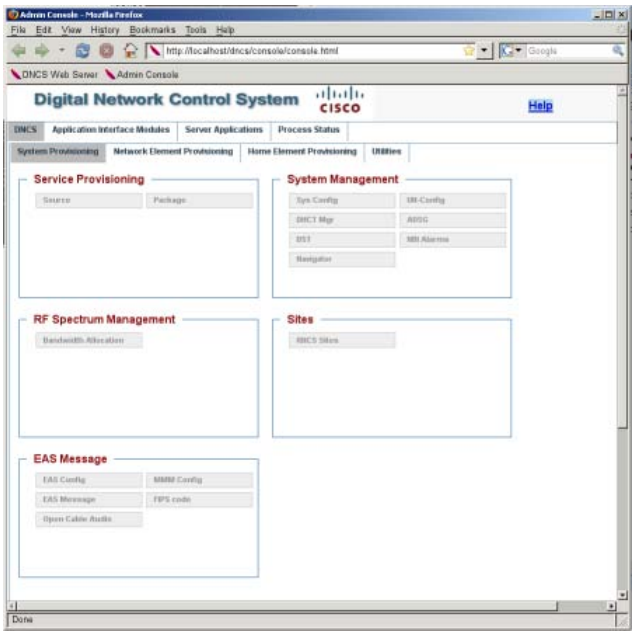
`http://10.1.1.1/dncs`

Result: A login prompt opens.



2 Type your DNCS Administrator **username** and **password**, and click **OK**.

Result: The DNCS Administrative Console opens.



Logging into the DNCS, RNCS, and Application Server from a Windows PC

Telnet and XDMCP have been disabled on the DNCS, RNCS, and Application Server to decrease security vulnerabilities.

SSH and X11 forwarding are available on the systems to allow remote access to X-based user interfaces such as dncsContol, lionnControl, and appControl.

Note: The Administrative Console can be accessed remotely using this connection method; however, we do **NOT** recommend this because of the display delay. We recommend using a Web Browser on a remote computer to access the Administrative Console.

To access your DNCS, RNCS, or Application Server using a Windows PC, you need to set up an xterm terminal emulator, such as PuTTY and an x-client, such as Exceed. We recommend using one of the following X Windows terminal programs:

- Exceed
- X-WIN 32
- Reflection X

PuTTY Settings

Note: PuTTY is not required with Exceed. You can use Exceed's Connectivity Secure Shell.

Use the following settings when you configure PuTTY.

Category	Field	Description
Session	Host Name (or IP Address)	IP address of the DNCS.
	Connection Type	Select the **SSH** option.
	Saved Sessions	Enter a host and username. **Example:** Type **DNCS - Fred Flintstone**.
Connection > Data	Auto-login username	Enter your DNCS username. **Note:** This is not mandatory, but it prevents you from having to enter your username each time you log into the DNCS.
SSH > X11	Enable X11 forwarding	Select this option (a checkmark displays when selected).
	X display location	Type **localhost**.
	Remote X11 authentication protocol	Select the **MIT-Magic-Cookie-1** option (a checkmark displays when selected).

Configuring PuTTY

Follow these directions to configure PuTTY.

1. Install and launch PuTTY. The PuTTY Configuration window opens.
2. In the **Category** list, click **Session** under the Connection section.
3. In **Host Name (or IP Address)**, type the IP address of the system.
4. Under **Connection Type**, select the **SSH** option.
5. Under **Saved Sessions**, enter a host name and username.

   Example:

   ```
   DNCS - FredFlintstone
   ```
6. In the **Connection** list, click **Connection > Data**.
7. In **Auto-login username**, type your username.

   Notes:

   - This is not mandatory, but it prevents you from having to enter your username each time you log into the DNCS.
   - Do NOT use this on PCs that are shared by multiple users, because the shared password will be reused.
8. In the **Category** list, click **SSH > X11**.
9. Select the **Enable X11 forwarding** option.
10. In the **X display location** box, type **localhost**.
11. Under **Remote X11 authentication protocol**, select the **MIT-Magic-Cookie-1** option.

12 In the **Category** list, click **Session**.

13 Click **Save**.

Configuring Exceed

Follow these directions to configure Exceed.

1 Install Exceed on your Windows PC.

2 Click **Start > Programs > Hummingbird Connectivity > Exceed Tools > Xconfig**. The Xconfig window opens.

3 Click **Communication**. The Communication window opens.

4 In **Mode**, select the **Passive** option from the drop-down list.

5 In **Common Actions**, click **Validate and Apply Changes**.

6 Close the Xconfig window.

Configure X-Win 32

There is no configuration necessary to use X-Win 32 with the DNCS, the RNCS, or the Application Server.

Configure Reflection X

There is no configuration necessary to use Reflection X with the DNCS or the RNCS.

Logging into the DNCS, RNCS, or Application Server Remotely

This section describes how to use Exceed and a terminal emulation program to log in remotely to the DNCS, RNCS, or Application Server.

1 Make sure you have set up your terminal emulation program correctly on your local PC. See ***Configuring PuTTY*** (on page 19) and ***Configuring Exceed*** (on page 20) for more information.

2 Launch one of the following programs on your local PC:

- Exceed
- X-Win 32
- Reflection X

Let this program run in the background.

3 Open PuTTY. The PuTTY configuration window opens.

4 In **Saved Sessions**, select the session that corresponds to the DNCS you want to log into.

5 Click **Load**.

6 Click **Open**. A keyboard authentication screen opens.

7 Did you configure PuTTY with your username for this server?

- If **yes**, go to step 8.
- If **no**, type your **username** and press **Enter**.

8 Type your **password** and press **Enter**. If your login credentials are correct, you will see a command prompt.

9 Do you need to open any DNCS GUI windows (such as the Administrative Console)?

- If **yes**, type `suxterm - dncs` and press **Enter**. Type the **password** and press **Enter** after the prompt.
- If **no**, go to the next step.

10 If you do not see a prompt in the window, maximize the program you launched in step 2.

11 To launch the DNCS Control window, type **dncsControl** and press **Enter**.

Logging into the DNCS, RNCS, or Application Server Using an Apple Mac

Follow these directions to login into the DNCS, the RNCS, or the Application Server remotely using an Apple Mac using SSH with x11 forwarding.

1 On an xterm window on the Mac, type `ssh -X -l [username] [DNCS IP address]` and press **Enter**.

Note: The `-l` in the command is a lowercase L, not the number 1 (one).

2 To open any GUIs (such as the Administration Console or the DNCS Control Panel), type `suxterm - dncs` and press **Enter**. The suxterm command opens a new xterm window that allows you to run the DNCS Control Panel (dncsControl) and other UI applications.

Session Limitations

You can only have one active OS login session for any single username. This applies to the DNCS, the RNCS, and the Application Server.

Notes:

- Session limits do NOT apply to remote web access to the Administrative Console.
- Session limitations do NOT apply to the following users:
  - dncs role
  - root user
  - easftp user
  - dncsftp user
  - Existing users:
    - Users that existed before the SR upgrade that included the security enhancements
    - Users that existed before the security enhancements were enforced

This restriction can be changed for a user by modifying the project file entry for that user. See ***Overriding Session Limitations*** (on page 22) for the procedure.

Overriding Session Limitations

By default, users are restricted to having one active OS login session. This section describes how to override this default.

Note: This topic applies to the OS login access to the DNCS, the RNCS, and the Application Server.

1. Log into the system as root:
   a. At the prompt, type `su -` and press **Enter**.
   b. Type the **root password** and press **Enter**.
2. Type the following command and press **Enter**:

   ```
   projmod -K 'project.max-tasks=(priv,x,deny)' user.[username]
   ```

   Example:

   ```
   projmod -K 'project.max-tasks=(priv,2,deny)' user.dncsadmin
   ```

   Notes:

   - The **x** in (priv,x,deny) is the number of active sessions the user is allowed to have open at a time.
   - Make sure that there is a space between **deny)'** and **user**.

- Substitute the username for **[username]**. Do not type the brackets **[ ]** in the command.
- You will need to log out of the system and log back in for the changes to take effect.

Session Timeout

Session Timeout Defaults

Notes:

- This topic applies to the DNCS, the RNCS, and the Application Server.
- Session timeout does NOT apply to remote web access to the Administrative Console.
- The session locking time does not affect the root user.
- Session locking also affects SSH, xterms, consoles on the CDE, and shells launched during a session.

The system will close an OS login session that has been idle for a configurable period of time. After a session is closed, users must log back into the system.

- Session locking default time: 30 minutes (1800 seconds)
- Recovery: User logs in again

Changing the Session Timeout Default

You can change the OS login session timeout default for an individual user or for a session.

Changing the Session Timeout Default for a User

Note: This topic applies to OS login sessions on the DNCS, the RNCS, and the Application Server.

1. Open an xterm window on the system.
2. Type `cd /export/home/[user account]` and press **Enter**.
3. Open the **.profile** file in a UNIX text editor.
4. Add the following line to the .profile file:

   ```
   export TIMEOUT=[seconds]
   ```

   Notes:

   - Do not type the brackets **[ ]** in the command.
   - Enter the time as a number of seconds.

Examples:

- To enter a session locking time of **5 minutes**, change the field to `export TIMEOUT=300`
- To enter a session locking time of **15 minutes**, change the field to `export TIMEOUT=900`

- We recommend that you keep the session locking time to as short a time as possible. This helps prevent unauthorized use of your system.

5 Save the .profile file and close the text editor.

6 In the xterm window, type `. ./.profile` and press **Enter**. The system will use the updated .profile file.

Note: Be sure to type a space between the first two periods.

Changing the Session Timeout Default for a Session

The timeout default for a single OS login session can be set to never timeout during a session. This can be useful if you are completing an activity on the system where the session timeout could cause issues that prevent you from completing your task.

Note: This topic applies to OS login sessions on the DNCS, the RNCS, and the Application Server.

To set the session timeout to never expire, follow these directions.

1 Log into the system.

2 Open an xterm window on the system.

3 Type `export TMOUT=0` and press **Enter**. The session will not timeout until you close the xterm window.

Session Lock

Session Lock Defaults

The system will lock an OS user account after a configurable number of unsuccessful OS login attempts. After the account is locked, an administrator must unlock the account.

Note: Session lock does NOT apply to web access to the Administrative Console.

- Default number of unsuccessful login attempts before the user account is locked: 5
- Recovery: Administrator must reset the user account

Changing the Session Lock Number

Note: This topic applies to OS logins to the DNCS, the RNCS, and the Application Server.

1. Open an xterm window on the system.
2. Log into the system as root:
   a. At the prompt, type `su -` and press **Enter**.
   b. Type the **root password** and press **Enter**.
3. Type `cd /etc/default` and press **Enter**.
4. Open the **login** file in a UNIX text editor.
5. Locate the following line in the login file:
   `#RETRIES=5`
6. Uncomment the line (remove the **#** from the beginning of the line) and change the number of retries to the number that you prefer.
   Important:
   - We recommend that you keep the number of retries to as few as possible. This helps prevent unauthorized use of your system.
   - **DO NOT** set this number to 0 (zero). This provides 0 attempts to log into the system.
7. Save the login file and close the text editor.
8. Type `exit` and press **Enter** to close the xterm window.
9. Log out of the system and log back in to make the changes effective.

Unlocking a User Account

Note: This topic applies to the OS login accounts on the DNCS, the RNCS, and the Application Server. Account locking is not applicable to the WebUI users on the DNCS.

1. Open an xterm window on the system.
2. Log into the system as root:
   a. At the prompt, type `su -` and press **Enter**.
   b. Type the **root password** and press **Enter**.
3. Type `passwd -s [username]` and press **Enter** to display the user account password attributes.

   Notes:

   - Substitute the user account name for [username] in the command. Do not type the brackets in the command.
   - Locked user accounts display with **LK** immediately after the username.

   Examples:

   - **Locked user account:** `dncsuser LK 03/11/10 0 91 14`
   - **Unlocked user account:** `dncsuser PS 03/11/10 0 91 14`
4. Type `passwd -r files -u [username]` and press **Enter**.

   Note: Substitute the user account name for **[username]**. Do not type the brackets in the command.

   Result: The user account is unlocked. The user account retains the original password. To change the password, refer to ***Changing User Account Passwords*** (on page 36).
5. Type `exit` and press **Enter** to close the xterm window.

Login Time Limit

Login Time Limit Defaults

The system will stop responding after a configurable number of seconds if the user does not log into the OS during that time.

Note: The session login time does NOT apply to remote web access to the Administrative Console.

- Default number of seconds before sessions stop: 10 minutes
- Recovery: User must restart and log into sessions again

  Note: Some software behaves differently from others; some freeze and must be restarted, others do not freeze, but must be logged into again.

Changing the Login Time Limit for SSH and SFTP

Note: This topic applies to the OS login on the DNCS, the RNCS, and the Application Server.

1. Open an xterm window on the system.
2. Log into the system as root:
   a. At the prompt, type `su -` and press **Enter**.
   b. Type the **root password** and press **Enter**.
3. Type `cd /etc/ssh` and press **Enter**.
4. Open the **sshd_config** file in a UNIX text editor.
5. Locate the following line in the login file:
   `LoginGraceTime 600`
6. Change the login time limit to the time that you prefer.

   Notes:

   - Enter the time as a number of seconds.

     Examples:

     – To enter a login time limit of **3 minutes**, change the field to `LoginGraceTime 180`
     – To enter a login time limit of **15 minutes**, change the field to `LoginGraceTime 900`
     – To disable the login time limit, change the field to `LoginGraceTime 0`
   - We recommend that you keep the time limit as short as possible. This helps prevent unauthorized use of your system.
7. Save the sshd_config file and close the text editor.

8 In the xterm window, type `svcadm restart ssh` and press **Enter**. The system restarts the SSH process.

9 Type `exit` and press **Enter** to close the xterm window.

CDE Screen Lock

CDE Screen Lock Default

The DNCS, RNCS, and Application Server are set up by default to lock the CDE screen after 30 minutes of inactivity.

Modifying the CDE Screen Lock

1. From the CDE window, right-click on the main screen and select **Tools > Desktop Controls**. The Application Manager - Desktop_Controls window opens.
2. Double-click **Screen Style Manager**.
3. Change the **Screen Lock** and **Start Lock** values.
4. Click **Save**.

Killing a Session

There might be times when a user closes an OS login session, but the session 'hangs' without closing; that is, the system still considers the session active even though the user terminated the session. If this happens, the user cannot start a new session until the session timer expires.

If the user needs to start a new session immediately, an administrator can kill a hung session using the following instructions.

Note: This topic applies to the OS login session on the DNCS, the RNCS, and the Application Server.

1. Open an xterm window on the system.
2. Log into the system as root:
   a. At the prompt, type `su -` and press **Enter**.
   b. Type the **root password** and press **Enter**.
3. Type `/usr/ucb/ps auxwww | grep [username]` and press **Enter** to search for the ssh process for the user.

   Note: Type the username of the user for **[username]**. Do not type the brackets in the command.

   Example: For user jersande, type `/usr/ucb/ps auxwww | grep jersande` and press **Enter**. You would see a display similar to the following:

   ```
   root      6311  0.0  0.0 1272 1024 pts/19   S 11:11:26  0:00 grep jersande
   jersande  6811  0.0  0.1 8768 2776 ?        S 09:24:16  0:00 /usr/lib/ssh/sshd
   jersande  6823  0.0  0.0 1448 1344 pts/19   S 09:24:17  0:00 -ksh
   ```
4. Locate the PID for the ssh process. In the example above, it is **6811** (the second line).
5. Type `kill -9 [PID]` and press **Enter**. The system kills the ssh process.

   Example: From the example above, type `kill -9 6811` and press **Enter**.

4

Password Management

Introduction

Regardless of password management rules enforced by a system, users must still be encouraged to choose difficult-to-guess (strong) passwords. Proper system management of passwords is important but the primary responsibility for strong passwords ultimately rests with the user.

Important: If your password management and/or user account management is administered by an external LDAP, RADIUS, or Sudo system, you must manage your passwords and user accounts on that system and not on the IBDS element.

In This Chapter

Password Guidelines

Note: These guidelines apply to all systems in your network.

Users must select a very strong, complex password. Strong passwords have the following general characteristics:

- Contain 8 or more characters
- Contain characters from at least two of the following:
  - Lower-case letters
  - Upper-case letters
  - Digits
  - Special characters
- Do **not** consist of only one character type (**aaaaaaa** or **11111111**)
- Do **not** contain any aspects of a date
- Are **not** proper names or words you would find in the dictionary
- Are **not** the same as previous passwords with an added capitalization
- Are **not** telephone numbers or similar numeric groups
- Are **not** user IDs, user names, group IDs, reversed user names, or other system identifiers
- Do **not** contain more than two (2) consecutive occurrences of the same character
- Are **not** consecutive keyboard patterns (for example, **qwerty**)
- Are **not** the product name, the manufacturer name, or variants thereof

System Password Retention

Note: This topic applies to the OS login user accounts on the DNCS, the RNCS, and the Application Server.

The system sets the following restrictions on re-using passwords:

- The system retains the last 5 passwords each user uses.
- The system does not allow you to re-use any of the last 5 passwords each user has used.

Changing User Account Passwords

Important: If your password management and/or user account management is administered by an external LDAP, RADIUS, or Sudo system, you must manage your passwords and user accounts on that system and not on the DNCS. For more information, see *Enable RADIUS and LDAP Support in a DBDS for SR 5.0 Configuration Guide* (part number 4017610) or contact your system administrator for more information.

We recommend that you change the default passwords for the root and for the dncs role at a minimum to increase the security level on the DNCS, the RNCS, and the Application Server. Our recommendations for other account passwords are as follows:

- **informix account:** Do not change the informix account password. Remote login for this user is disabled by default.
- **dncsSSH account:** Do not change the dncsSSH account password. Remote login for this user is disabled by default.
- **easftp and dncsftp accounts:** Modifying these account passwords should be done only in collaboration with the administrators of the EAS, DNCS, third-party systems, and billing systems.

  Notes:

  - The dncsftp password is not applicable to the RNCS.
  - The easftp and dncsftp users are not applicable to the Application Server.

A user account password can be changed by the user or by the system administrator.

Changing Your Own OS Password

Note: This topic applies to the OS login user accounts on all systems.

1. Open an xterm window on the system.
2. Type `passwd -r files` and press **Enter**. The system will prompt you for your existing password.
3. Enter your **existing password** and press **Enter**. The system will prompt you for your new password.
4. Enter your **new password** and press **Enter**. The system prompts you to re-enter your new password.
5. Type your **new password** again and press **Enter**. The system compares your two password entries. If they match, the **password successfully changed** message appears. If they do not match, you must re-enter the new password.
6. Type `exit` and press **Enter** to close the xterm window.

7 Log out of the system.

8 Log into the system with your new password.

Changing Another OS User's Password

Notes:

- Users can change their own account password. Only the root user can change other users' account passwords.
- This procedure applies to the OS user accounts on all systems.

1 Open an xterm window on the system.

2 Log into the system using an existing user account.

3 Type `passwd -r files [username]` and press **Enter**.

Example: For user **jonesx**, type the following and press **Enter**:

```
passwd -r files jonesx
```

4 Type the new password for the user and press **Enter**.

5 Type the **new password** again and press **Enter**. The system compares your two password entries. If they match, the **password successfully changed** message appears. If they do not match, you must re-enter the new password.

6 Type `exit` and press **Enter** to close the xterm window.

7 Have the user log out of the system.

8 Have the user log into the system with the new password. If you used the **-f** option during password creation (the **-f** option forces the user to change their password at the next login), the user must enter the one-time password you created. Then, the system prompts the user to create a new password.

Changing the Web Interface User's Password

Note: Only the root user (or a user with the DNCS role) can change a Web Interface user account password.

1 Open an xterm window on the system.

2 Log into the system as root, or assume the DNCS role.

3 Type the following and press **Enter**:

```
/usr/apache2/bin/htdigest  /etc/apache2/user-
conf/SAIdncs.digest "Cisco DNCS" [username]
```

Notes:

- This is a single command.
- Substitute the user account name for [username]. Do not type the brackets in the command.

4 Type the **new Web Interface password** for the user and press **Enter**.

5 Type the **new password again** and press **Enter**. The system compares the two password entries.

6 Did the "They don't match, sorry" message appear?

- If **yes**, the two passwords do not match. Go back to step 3 and re-type the command.
- If **no**, the system prompt is returned. You are finished with this procedure.

Changing the Root Password

Note: This topic applies to all systems.

1 Open an xterm window on the system.

2 Log into the system as root:

a At the prompt, type `su -` and press **Enter**.

b Type the **root password** and press **Enter**.

3 Type `passwd -r files root` and press **Enter**.

4 Type the new password for the root user and press **Enter**.

5 Type the new password again and press **Enter**. The system changes the root password.

Password Expiration Period

Password Expiration Period Defaults

If your password management and/or user account management is administered by an external LDAP, RADIUS, or Sudo system, you must manage your passwords and user accounts on that system and not on the DNCS. For more information, see *Enable RADIUS and LDAP Support in a DBDS for SR 5.0 Configuration Guide* (part number 4017610) or contact your system administrator for more information.

WARNING:

Do not enable password aging for any of the default users (root, dncs, informix, dncsSSH, dncsftp, or easftp). The system (or components within the system) will become unstable if any of these default user passwords expire.

Important: You should not change the informix or the dncsSSH password. The informix password is locked by default and the dncsSSH password is a no-login account. Changing the easftp and dncsftp passwords should be done only in coordination with the administrator of the EAS and the DNCS, respectively.

Password expiration is disabled for all critical users on the system by default.

For all other users on the system:

- Default number of weeks a password is valid: 13
- Default number of weeks prior to password expiration when the user receives a warning message to change passwords: 2
- The default values are applied to a user account at the time it is created
- Recovery: Administrator must reset the user account by changing the password

Notes:

- The default values are applied to an OS user account at the time the account is created.
- Password expiration does not apply to web access login accounts.

Changing a User Password Expiration Period

Note: This topic applies to OS login accounts on the DNCS, the RNCS, and the Application Server.

Use this procedure to change the password expiration period for an individual user account.

WARNING:

Do not enable password aging for any of the default users (root, dncs, informix, dncsSSH, dncsftp, or easftp). The system (or components within the system) will become unstable if any of these default user passwords expire.

1 Open an xterm window on the system.

2 Log into the system as root:

   a At the prompt, type `su -` and press **Enter**.

   b Type the **root password** and press **Enter**.

3 Type `passwd -r files -x [days] [username]` and press **Enter**.

   Notes:

   - Type the number of days before a user password expired for **[days]**.
   - Type the username for **[username]**.
   - Do not type the brackets **[ ]** in the command.

   Example: For user **jonesx**, type the following and press **Enter**:

   ```
   passwd -r files -x 180 jonesx
   ```

4 Verify the expiration period by typing `passwd -s [username]` and press **Enter.**

   Example: Type `passwd -s jonesx` and press **Enter**. The system displays a message similar to the following:

   ```
   jonesx    PS            09/02/10    0      180    14
   user      pw_status     date        MIN    MAX    WARN
   ```

   - The **date** (09/02/10) is the date the password was set by the user (jonesx).
   - The **MIN** (0) is the minimum number of days before a user is allowed to change the password. We recommend that you leave this field blank.
   - The **MAX** (180) is the number of days after the date that the password is valid.
   - The **WARN** (14) is the number of days before the password expires that a warning banner is displayed.

5 Type `exit` and press **Enter** to close the xterm window.

Disabling a User Password Expiration Period

Note: This topic applies to OS login accounts on the DNCS, the RNCS, and the Application Server.

Use this procedure to change the password expiration period for an individual user account.

1. Open an xterm window on the system.
2. Log into the system as root:
   a. At the prompt, type `su -` and press **Enter**.
   b. Type the **root password** and press **Enter**.
3. Type `passwd -r files -x -1 [account name]` and press **Enter**.

   Notes:

   - Type the username for **[account name]**.
   - Do not type the brackets **[ ]** in the command.
4. Verify the expiration period by typing `passwd -s [username]` and press **Enter**.

   Example: For user **jonesx**, type the following and press **Enter**:

   ```
   passwd -s jonesx
   ```

   The system displays a message similar to the following:

   ```
   jonesx      PS
   user        pw_status     date    MIN    MAX    WARN
   ```

   Note: Only PS should be listed after the account name for an account with a disabled expiration period. If numbers appear after the PS, repeat step 3.
5. Type `exit` and press **Enter** to close the xterm window.

5

SSH, SFTP, and SCP Connections

Introduction

This chapter discusses SSH, SFTP, and SCP connections, including security file errors and changing the connection retries parameter.

In This Chapter

Overview

SSH, SFTP, and SCP connections use the RETRIES and the MaxAuthTries parameters to control the maximum number of login attempts. You typically want the MaxAuthTries parameter value to be one less than the RETRIES parameter value.

Notes:

- With SSH and SFTP, these attempts are password attempts only, not username/password combination attempts.
- If the RETRIES parameter value is lower than the MaxAuthTries parameter value, the RETRIES value takes precedence.
- If the MaxAuthTries parameter value is lower than the RETRIES parameter value by 2 or more, the MaxAuthTries value takes precedence.
- The maximum value for the RETRIES parameter is 15.
- Some clients have their own retries parameters. These usually override the system retries parameters.

SSH Security File Errors

The DNCS, RNCS, and Application Server are configured for strict RSA key checks, ensuring the highest level of security.

The following error might occur when you attempt to connect to a remote server:

```
# ssh dncsadm@10.90.176.173

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Someone could be eavesdropping on you right now (man-in-the-
middle attack)!

It is also possible that the RSA host key has just been changed.

The fingerprint for the RSA key sent by the remote host is

6c:e1:cf:83:41:1a:e4:06:bd:2b:7e:9c:0e:55:a1:88.

Please contact your system administrator.

Add correct host key in /.ssh/known_hosts to get rid of this
message.

Offending key in /.ssh/known_hosts:13


RSA host key for 10.90.176.173 has changed and you have requested
strict checking.

Host key verification failed.
```

This occurs if the remote host has been replaced or OS reinstalled. If neither scenario has happened, it is possible that something malicious is going on.

Clearing the Error

Note: This topic applies to the DNCS, the RNCS, and the Application Server.

If the reason for the RSA Key change is known and not fraudulent, follow these instructions:

1. In a UNIX text editor, open the file specified in the error message.

   Example: In the above example, you would open the **/.ssh/known_hosts** file in the text editor.

2. Search for the IP address of the system giving the error.

Example: In the above example, you would search for **10.90.176.173** in the file. Delete the line containing the IP address.

3 Save and close the file.

Using SFTP and SCP

There are several open-source or freeware sftp/scp applications available on the Internet that work well on Windows-based PCs and Apple Macs. Search for an application that is appropriate for your site.

Notes:

- When you use SFTP or SCP to login to the system, use your individual username and password.
- You can only have one active session for each username. Consider setting up additional usernames if you require multiple sessions open at the same time.
- This topic applies to the DNCS, the RNCS, and the Application Server.

To open a session for SFTP:

1. Open an xterm window on the system.
2. Type `sftp [username]@[IP address of the system]` and press **Enter**.
3. Type the **sftp password** and press **Enter**.
4. Navigate to your target directory by typing `cd /[target directory]` and pressing **Enter**.
   - **To transfer a file from the system to your computer,** type `get [target file]` and press **Enter**.
   - **To transfer a file from your computer to the system,** type `put [target file]` and press **Enter**.

   Note: If the file transfer fails, make sure that both directories and files have the correct permissions. The following permissions are required for the DNCS Administrator and Operator accounts.

   - If the directory is owned by the root user:

     ```
     drwxr-xr-x  2 root root 512 Aug 24 14:49 [target directory]
     ```

   - If the directory is owned by the dncs role:

     ```
     drwxr-xr--  2 dncs dncs 512 Aug 24 14:49 [target directory]
     ```

   - If the file is owned by the root user:

     ```
     -rw-r--r--  1 root root 2568 Aug 24 14:49[target directory]
     ```

   - If the file is owned by the dncs role:

   - `-rw-r-----  1 dncs dncs 2568 Aug 24 14:49[target directory]`

Changing the SSH and SFTP Connection Retries Parameter

Note: This topic applies to the DNCS, the RNCS, and the Application Server.

1. Change the system session locking default to the number you prefer by following the procedure in ***Changing the Session Lock Number*** (on page 26).
2. In an xterm window on the system where you are logged in as root, type `cd /etc/ssh` and press **Enter**.
3. Open the **sshd_config** file in a text editor.
4. Find the line that contains MaxAuthTries and enter the number of login attempts you prefer.

   Example: `MaxAuthTries 5`
5. Save and close the file.
6. In an xterm window on the system where you are logged in as root, type `svcadm restart ssh` and press **Enter**. The ssh process restarts and uses the new MaxAuthTries parameter.

6

Security Event Logs and Auditing

Introduction

This chapter discusses security logs, including what is logged and where the logs are located, and auditing the system using the Basic Security Module (BSM).

In This Chapter

Security Event Logs

Security event logs are automatically generated by the system. The standard security event logs are located in the **/var/log/authlog** file. This file logs the following events:

- SSH
- SFTP
- Successful and failed login attempts

Note: You need to be logged in as root user to access the /var/log/authlog file.

Other log files you can monitor for security, along with their security restrictions:

- **/var/adm/sulog:** Records all su commands. Root user only.
- **/var/adm/messages:** Records messages from the kernel and daemons. All users can read.
- **/var/log/syslog:** Records messages from sendmail and other processes. All users can read.
- **/var/audit/:** Directory that contains all audit files including all security-related events, for example: logins and logouts, user actions, etc. Root user only.
- **/var/apache2/logs:** Directory that contains the Apache web server log files which include Administrative Console web access events. All users can read.

System Auditing Using BSM

The BSM utility is installed on the system and logs a significant amount of event information, including OS login and logoff events that the authlog and sulog do not capture.

Notes:

- The BSM utility writes binary log files to the **/var/audit/** directory. You cannot view these files using a simple text editor. The **praudit** command converts the binary format to readable text.
- The system generates one BSM binary log file per day and only retains seven days of files.

1. Log into the system as root:
   a. At the prompt, type `su -` and press **Enter**.
   b. Type the **root password** and press **Enter**.
2. To determine the name and location of the current BSM log file, type `auditreduce /etc/security/audit_data` and press **Enter**.

   Example: `/var/audit/20081007040000.not_terminated.filbert`
3. To convert a BSM binary log to readable text, type `cat [path and name of file] | praudit -s` and press **Enter.** This results in a significant amount of information. Please check the auditreduce and praudit man pages for usage information for these commands.
4. To start a new log file, type `audit -n` and press **Enter**.

BSM Auditreduce

The auditreduce command searches across multiple audit files and filters for specific information.

Auditreduce Options

```
auditreduce -a [date/time] -c [audit-class] -u [username]
[file(s)]
```

- `-a [date/time]` — Displays information after the specified date and/or time. The date/time is in the following format: **YYYYMMDDHHMMSS**.
  - The year (YYYY), month (MM), and day (DD) are required.
  - The hour (HH), minute (MM), and second (SS) are optional.
- `-b [date/time]` — Displays information before the specified date and/or time. The date/time is in the following format: **YYYYMMDDHHMMSS**.
  - The year (YYYY), month (MM), and day (DD) are required.
  - The hour (HH), minute (MM), and second (SS) are optional.
- `-c [audit-class]` — Search for certain log data events. Options are:
  - `lo` – login and logout events
  - `ad` – administrative events
  - `ex` – program execution events
- `-u [username]` — Search for activity executed by a particular user.
- `[file(s)]` — Specify the BSM binary file(s) to search.

Note: Do not type the brackets (**[ ]**) in the command.

Additional Information on auditreduce

Please see the auditreduce man page for additional information and options for additional information.

The auditreduce standard output is binary so praudit must be used to convert the output to text.

Example:

```
auditreduce | praudit
```

7

DNCS Web Services Security

Introduction

Two separate web instances exist on the DNCS — one supports the web user interface (Administrative Console WebUI) and the other supports web services.

Two separate web services exist on the DNCS — one web service for BOSS billing transactions and the other for remote set-top box (STB) staging management.

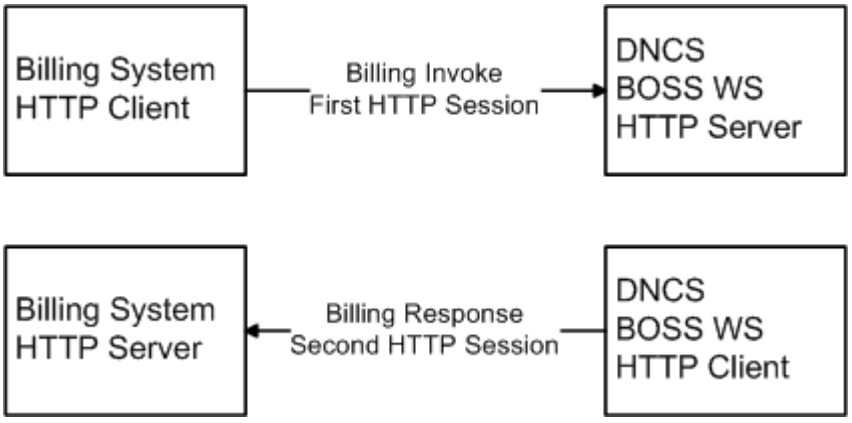
This section contains the procedures necessary to provision access to these web services. Unsecured access (HTTP) to the web services is achieved by allowing specific hosts or IP addresses access to the web service. Secure access to the web services is achieved by installing the necessary certificates, enabling HTTPS (SSL/TLS) and then allowing specific hosts or IP addresses access to the web service. Additional authentication options can also be implemented.

In This Chapter

Overview

By default, the DNCS web services are only accessible internally on the DNCS. That is, the DNCS denies by default all HTTP and HTTPS transaction attempts from outside service requesters. The network interface on the DNCS used for access to the web services must be defined prior to any other configuration. Service requesters are allowed access to specific web services on the DNCS using "Allow from" statements in the web service configuration files. HTTPS access to the BOSS Web Service can be limited to only those devices that present a client certificate trusted by the DNCS using client authentication. A username and password can be created to limit access to the DNCS STB staging web service.

The billing interface is asynchronous, so both the billing system and the BOSS web service must act as an HTTP client as well as an HTTP server. That is, there are two separate HTTP sessions for each billing transaction — one session for the invoke message and a second session for the response message. Therefore, the billing system is both an HTTP client and an HTTP server. Likewise, the DNCS BOSS web service is both an HTTP server and an HTTP client. The following illustration describes this relationship:



To implement HTTPS for the billing interface, the billing system must support SSL/TLS as both a client and a server. If the billing system does not support SSL/TLS, or if the feature is not required, the BOSS web service must be configured to allow HTTP transactions from the billing system.

The BOSS web service also supports Client Authentication when acting as a HyperText Transfer Protocol Secure (HTTP-S) client or HTTP-S server. That is, when acting as the HTTP-S server, the BOSS web service can be configured to require a certificate from the billing system. Additionally, when acting as the HTTP-S client, the BOSS web service supports providing a certificate if requested by the billing system. Client Authentication adds an additional step in the SSL/TLS authentication process when the HTTP server requests and validates a certificate from the HTTP client. Client Authentication is not enabled by default for the BOSS web service.

The STB Staging Management interface is synchronous, so the remote STB staging client is always the HTTP client and the DNCS STB staging web service is always the HTTP server. To implement HTTPS for the STB Staging Management interface, the STB staging client must support SSL/TLS as a client. If the STB staging client does not support SSL/TLS, or if the feature is not required, the DNCS STB staging web service must be configured to allow HTTP transactions from the STB staging client. Client authentication is not enabled by default for the DNCS STB staging web service. A username and password can be created to limit access to the DNCS STB staging web service when configured for either HTTP or HTTPS.

Define the Web Service Listening Interface

By default, the DNCS Web Services are only accessible internally on the DNCS. The DNCS Web Service must be configured to operate on an external-facing network interface to allow access for service requesters, such as billing systems and remote set-top staging clients. Complete the procedures in this section to define the DNCS Web Services network interface.

Second Web Instance Consideration

A second web server instance was added to the DNCS in SR 5.0. The existing web server instance supports the web user interface (web UI) and web services.

The new web server instance was added to allow separation of remote web UI traffic and web services. The web services can be configured to operate on the original web server instance; however, we do NOT recommend this approach. You should ONLY configure both the web UI and web services to operate on the same web server instance if there are insufficient network interfaces on the DNCS to support both instances.

The web UI web server instance, http, is configured to listen locally on port 80 by default.

The second web server instance, http-dncsws, is configured to listen on the private dncs interface (TED network) during an initial installation of the DNCS. A remotely accessible network interface must exist or be created on the DNCS if you are going to use the same port number for both web server instances.

Important: The two web server instances cannot listen on the same network interface and port. A second remotely accessible network interface must exist or be created on the DNCS if the same port number will be used for both web server instances.

Notes: http Instance

- The “Listen” definitions exist in the /etc/apache2/user-conf/httpd.ports and /etc/apache2/user-conf/ssl.ports files.
- The instance listens on port 8045 of all interfaces and port 80 on localhost by default.

Notes: http-dncsws Instance

- The "Listen" definitions exist in the /etc/apache2/httpd-dncsws/httpd.conf and /etc/apache2/httpd-dncsws/ssl.conf files.
- The dncsws hostname is assigned to the dncs (TED Network) interface on systems initially installed with DNCS SR 5.0.
- The dncsws hostname is assigned to the loopback2 (127.0.0.2) interface on systems upgraded to SR 5.0 that do not have an existing dncseth interface.

Example Configuration Options

Note: This is not an exhaustive list of web instance configurations.

- Web Services are on a separate web instance and only HTTPS is supported. Only one network interface is required.
  - Web UI listens on dncseth (for example, bge2) Port 80
  - Web Services listens on dncseth (for example, bge2) Port 443
- Web Services are on a separate web instance and only HTTPS is supported. Only one network interface is required but two can be used.
  - Web UI listens on dncseth (for example, bge2) Port 80
  - Web Services listens on dncsws (for example, bge3) Port 443
- Web Services are on a separate web instance and both HTTP and HTTPS are supported. Two network interfaces are required.
  - Web UI listens on dncseth (for example, bge2) Port 80
  - Web Services listens on dncsws (for example, bge3) Port 80 for HTTP traffic
  - Web Services listens on dncsws (for example, bge3) Port 443 for HTTPS traffic
- Web Services are on the same web instance as the web UI and both HTTP and HTTPS are supported.
  - http web instance supports both web UI and web services
  - http web instance listens on dncseth (for example, bge2) Port 80 and 443

Define the Web Service Interface Using a Separate Web Instance

Use the following procedures to define the network interface that will be used for the DNCS Web Services.

Important: A remotely accessible network interface separate from the web UI must be used for this option. Prior to starting this procedure, identify which network interface on the DNCS will be used for access to the DNCS Web Services.

Define the Web Service Hostname

Complete the following procedure to define the web service hostname, dncsws, on the network interface that you will use for access to the web services.

Note: Upon completing this procedure, the web services web instance will be configured for both HTTP and HTTPS support. Complete one of the two following procedures after completing this procedure to allow only HTTP or HTTPS access.

- ***Define the Web Service Interface for HTTP Support Only*** (on page 58)
- ***Define the Web Service Interface for HTTPS Support Only*** (on page 59)

1. Open an xterm window on the DNCS.
2. Log into the system as root:
   a. At the prompt, type `su -` and press **Enter**.
   b. Type the **root password** and press **Enter**.
3. Open the **/etc/hosts** file with a text editor.
4. Move the **dncsws** and **dncswebsvc** nicknames to the separate interface that will be used for the DNCS Web Service instance.

   Notes:

   - The dncswebsvc nickname may not exist on your system.
   - You can use dncsws as the actual hostname.

   Example:

   ```
   172.10.1.2    ossbss dncsws dncswebsvc
   ```
5. Save and close the hosts file.

Define the Web Service Interface for HTTP Support Only

Complete the following procedure to define the listening interface for HTTP access to the web services. Skip this procedure if secured web traffic is required for the web services. Skip this procedure if you require both unsecured and secured (HTTP and HTTPS) web traffic support.

1. Open an xterm window on the DNCS.
2. Log into the system as root:

a At the prompt, type `su -` and press **Enter**.

b Type the **root password** and press **Enter**.

3 Open the **/etc/apache2/httpd-dncsws/ssl.conf** file with a text editor.

4 Comment out all *port 443 Listen* statements by placing "**#**" in front of the line.

Example:

```
#Listen dncsws:443
```

5 Save and close the ssl.conf file.

Define the Web Service Interface for HTTPS Support Only

Complete the following procedure to define the listening interface for HTTPS access to the web services. Skip this procedure if unsecured web traffic is required for the web services. Skip this procedure if both unsecured and secured (HTTP and HTTPS) web traffic support is required

1 Open an xterm window on the DNCS.

2 Log into the system as root:

a At the prompt, type `su -` and press **Enter**.

b Type the **root password** and press **Enter**.

3 Open the **/etc/apache2/ httpd-dncsws/httpd.conf** file with a text editor.

4 Comment out all *port 80 Listen* statements by placing "**#**" in front of the line.

Example:

```
#Listen dncsws:80
```

5 Save and close the httpd.conf file.

Restart the Web Server

Complete the following steps to restart the http-dncsws web server instance to activate the changes.

1 Complete the following steps to stop and start the http-dncsws web server instance on the DNCS.

a Open an xterm window on the DNCS.

b Log into the system as root:

i At the prompt, type `su -` and press **Enter**.

ii Type the **root** password and press **Enter**.

c Type the following command and press **Enter** to stop the http-dncsws instance:

```
svcadm -v disable -st http-dncsws
```

d Type the following command and press **Enter** to refresh the http-dncsws instance configuration:

```
svcadm refresh http-dncsws
```

e Type the following command and press **Enter** to start the http-dncsws instance:

```
svcadm -v enable -s http-dncsws
```

2 Type the following command and press **Enter** to verify that the http-dncsws instance started successfully:

```
svcs -xv http-dncsws
```

Example: Output should be similar to the following:

```
svc:/network/http-dncsws:apache2-dncsws (Apache 2 HTTP server
for STB)
 State: online since Wed Oct 20 14:45:01 2010
   See: man -M /usr/apache2/man -s 8 httpd
   See: /var/svc/log/network-http-dncsws:apache2-dncsws.log
Impact: None.
```

Define the Web Service Using a Single Web Instance

Use the following procedures to configure the network interface that will be used for the DNCS Web Services.

Important: Prior to starting this procedure, identify the interface on the DNCS currently used for access to the DNCS Web UI. This will be the same network interface that you will use for the web services.

Web Service Interface for HTTP Support

The http web instance should have been configured for HTTP support when remote web UI access was enabled during the initial SR 5.0 installation or upgrade.

See the *DNCS Web UI Configuration* section in *DVD Upgrade Installation Guide for System Release 5.0 with Integrated Application Server* (part number 4035749).

Define the Web Service Interface for HTTPS Support

Complete the following procedure to define the listening interface for HTTPS access to the web services. Skip this procedure if secured (HTTPS) web traffic support is not required.

1 Open an xterm window on the DNCS.

2 Log into the system as root:

a At the prompt, type `su -` and press **Enter**.

b Type the **root password** and press **Enter**.

3 Open the **/etc/apache2/ httpd-dncsws/httpd.conf** file with a text editor.

4 Add `Listen [hostname]:443` to the end of the file.

Notes:

- Replace [hostname] with the IP address or hostname of the network interface that you will use for access to the web services.

- If a hostname is used, the hostname and IP address must be defined in the **/etc/hosts** file.

Example:

```
Listen dncseth:443
```

5 Save and close the httpd.conf file.

Restart the Web Server

Complete the following steps to restart the http web server instance to activate the changes.

1 Complete the following steps to stop and start the http web server instance on the DNCS.

a Open an xterm window on the DNCS.

b Log into the system as root:

i At the prompt, type `su -` and press **Enter**.

ii Type the **root password** and press **Enter**.

c Type the following command and press **Enter** to stop the http instance:

```
svcadm -v disable -st http
```

d Type the following command and press **Enter** to refresh the http instance configuration:

```
svcadm refresh http
```

e Type the following command and press **Enter** to start the http instance:

```
svcadm -v enable -s http
```

2 Type the following command and press **Enter** to verify that the http instance started successfully.

```
svcs -xv http
```

Example: Output should be similar to the following:

```
svc:/network/http:apache2 (Apache 2 HTTP server)
    State: online since Tue Oct 26 17:33:06 2010
      See: man -M /usr/apache2/man -s 8 httpd
      See: /var/svc/log/network-http:apache2.log
   Impact: None.
```

Allow HTTP Access to the Web Services

The BOSS Web Service and STB Staging Web Service must be configured to allow HTTP access to specific service requesters, billing systems, and STB staging clients.

Allowing HTTP Access to the BOSS Web Service

Complete the following procedure to allow a specific billing system to have HTTP access to the BOSS Web Service.

Note: Only an "Allow from" statement is required for HTTP access to the BOSS Web Service. Both an "Allow from" statement and REMOTE_ADDR definition are required for HTTPS access to the BOSS Web Service. The REMOTE_ADDR statement is added later in this document.

1. Open an xterm window on the DNCS.
2. Log into the system as root:
   a. At the prompt, type `su -` and press **Enter**.
   b. Type the **root password** and press **Enter**.
3. Open the **/etc/apache2/user-conf/SAIdncs.bossreq.auth.conf** file using a text editor.
4. Add the following line to the end of the "Allow from" list:

   ```
   Allow from [billing server IP]
   ```

   Notes:

   - Replace [billing server IP] with the IP address or hostname of the billing system.
   - If a hostname is used, the hostname and IP address must be defined in the /etc/hosts file.
   - An entire subnet can be allowed using slash notation.

   Example: The "Allow from" list should look similar to the following example:

   ```
   Order Allow,Deny
   Allow from localhost
   Allow from dncs dncs
   Allow from dncsws
   Allow from 172.16.20.1
   Allow from 172.10.1.0/24
   ```
5. Save and close the file.

6 Follow these instructions to restart the DNCS http process.

   a Type the following command and press **Enter** to stop the http process:

   ```
   svcadm -v disable -st http
   ```

   b Type the following command and press **Enter** to refresh the http process:

   ```
   svcadm refresh http
   ```

   c Type the following command and press **Enter** to restart the http process:

   ```
   svcadm -v enable -s http
   ```

   Result: The system displays the **svc:/network/http:apache2 enabled** message.

7 Follow these instructions to restart the DNCS http-dncsws process.

   a Type the following command and press **Enter** to stop the http-dncsws process:

   ```
   svcadm -v disable -st http-dncsws
   ```

   b Type the following command and press **Enter** to refresh the http-dncsws process:

   ```
   svcadm refresh http-dncsws
   ```

   c Type the following command and press **Enter** to restart the http-dncsws process:

   ```
   svcadm -v enable -s http-dncsws
   ```

   Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

Allowing HTTP Access to the STB Staging Web Service

Complete the following procedure to allow a specific set-top staging client to have HTTP access to the STB Staging Web Service using a separate web instance. Skip this procedure if the STB Staging Web Service is configured on the same web instance as the web UI.

1 Open an xterm window on the DNCS.

2 Log into the system as root:

   a At the prompt, type `su -` and press **Enter**.

   b Type the **root password** and press **Enter**.

3 Open the /etc/apache2/user-conf/SAIdncs.loadPIMS.auth.conf file using a text editor.

4 Add the following line to the end of the "Allow from" list.

```
Allow from [STB Staging Client IP]
```

Notes:

- Replace [STB Staging Client IP] with the IP address or hostname of the STB staging client.
- If a hostname is used, the hostname and IP address must be defined in the /etc/hosts file.
- An entire subnet can be allowed using slash notation.

Example: The "Allow from" list should look similar to the following example:

```
Order Allow,Deny
Allow from localhost
Allow from dncs dncs
Allow from dncsws
Allow from 172.16.30.1
Allow from 172.10.1.0/24
```

5 Will only HTTPS access, rather than HTTP, be allowed for the STB Staging web service?

- If **yes**, verify that the "SSLRequireSSL" line does not have "#" at the beginning of the line. The SSLRequireSSL line disables HTTP access to the STB Staging web service.

  Example:

  ```
  SSLRequireSSL
  ```

- If **no**, HTTP and HTTPS support is required; go to step 6.

6 Save and close the file.

7 Follow these instructions to restart the DNCS http process.

a Type the following command and press **Enter** to stop the http process:

```
svcadm -v disable -st http
```

b Type the following command and press **Enter** to refresh the http process:

```
svcadm refresh http
```

c Type the following command and press **Enter** to restart the http process:

```
svcadm -v enable -s http
```

Result: The system displays the **svc:/network/http:apache2 enabled** message.

8 Follow these instructions to restart the DNCS http-dncsws process.

a Type the following command and press **Enter** to stop the http-dncsws process:

```
svcadm -v disable -st http-dncsws
```

b Type the following command and press **Enter** to refresh the http-dncsws process:

```
svcadm refresh http-dncsws
```

c Type the following command and press **Enter** to restart the http-dncsws process:

```
svcadm -v enable -s http-dncsws
```

Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

Create Client Authorization Username and Password for the STB Staging Web Service

The DNCS STB Staging Web Service does not use basic username and password authentication by default.

When basic username and password authentication is implemented, the STB Staging Web Service requires an accurate username and password from the STB Staging client. If basic username and password authentication is desired for STB Staging transactions, then complete the following steps to create a username and password for the STB Staging Web Service. Skip this section if basic authentication is not required.

Notes:

- We do NOT recommend implementing basic authentication without HTTPS. The credentials (username and password) are transported over HTTP in the clear.
- Groups of usernames can be used to grant access to the STB Staging web service if a large number of usernames will be created. See the /etc/apache2/user-conf/SAIdncs.loadPIMS.auth.conf file on the DNCS for implementation details.

1 Type the following command and press **Enter** to create a new username and password for the STB Staging web service access on the DNCS:

```
/usr/apache2/bin/htpasswd -b /etc/apache2/user-conf/httpd-dncsws.users [username] [password]
```

Notes:

- This is one single command.
- Replace [username] [password] with the username and password.

Example:

```
/usr/apache2/bin/htpasswd -b /etc/apache2/user-conf/httpd-dncsws.users dtaom dtaomPwd
```

2 Did the system return a cannot modify file /etc/apache2/user-conf/httpd-dncsws.users; use '-c' to create it message?

- If **yes**, then no usernames exist on this system in the httpd-dncsws.users file. Type the following command and press **Enter** to create a new username and password in a new file named httpd-dncsws.users:

  ```
  /usr/apache2/bin/htpasswd -c -b /etc/apache2/user-conf/httpd-dncsws.users [username] [password]
  ```

  Notes:

  – This is one single command.

  – Replace [username] [password] with the desired username and password.

  Example:

  ```
  /usr/apache2/bin/htpasswd -c -b /etc/apache2/user-conf/httpd-dncsws.users dtaom dtaomPwd
  ```

- If **no**, the system returned the Adding password for user [username] message. Continue with the next step.

3 Open the /etc/apache2/user-conf/SAIdncs.loadPIMS.auth.conf file with a text editor.

4 Change the **Satisfy** option to **All**.

Note: The "All" option requires that a service requester have an IP Address in the "Allow from" statement AND provide a valid username and password.

Example: The Satisfy line should be:

```
Satisfy All
```

5 Uncomment the following lines (remove the "#" that appears at the beginning of the line):

```
AuthType Basic
AuthName "loadPIMS"
AuthUserFile /etc/apache2/user-conf/httpd-dncsws.users
Require user <user> <user2>
```

Note: These lines might already be uncommented if usernames already exist.

6 Remove `<user> <user2>` from the line **Require user**, if it exists.

Notes:

- Do not delete actual usernames from the file if they exist.
- <user> <user2> will not exist if usernames were added to this system in the past.

7 Add the new **username** to the end of the **Require user** line.

Example:

```
Require user dtaom
```

8 Document the username's password in the /etc/apache2/user-conf/SAIdncs.loadPIMS.auth.conf file as a commented line. Once it is created, it cannot be retrieved. The line must be commented (a **#** must exist at the beginning of the sentence).

Example:

```
# Leave as a comment and document the PASSWORD: dtaomPwd
```

9 Save and close the /etc/apache2/user-conf/SAIdncs.loadPIMS.auth.conf file.

10 Follow these instructions to restart the DNCS http process.

a Type the following command and press **Enter** to stop the http process:

```
svcadm -v disable -st http
```

b Type the following command and press **Enter** to refresh the http process:

```
svcadm refresh http
```

c Type the following command and press **Enter** to restart the http process:

```
svcadm -v enable -s http
```

Result: The system displays the **svc:/network/http:apache2 enabled** message.

11 Follow these instructions to restart the DNCS http-dncsws process.

a Type the following command and press **Enter** to stop the http-dncsws process:

```
svcadm -v disable -st http-dncsws
```

b Type the following command and press **Enter** to refresh the http-dncsws process:

```
svcadm refresh http-dncsws
```

c Type the following command and press **Enter** to restart the http-dncsws process:

```
svcadm -v enable -s http-dncsws
```

Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

Verify HTTP Access to the Web Services

Complete the following procedure to verify HTTP access to the web services. Skip this step if HTTP access was not enabled for the web services.

1 After the DNCS is configured, you can verify that the BOSS web service is accessible using HTTP by completing the following steps:

a Use a web browser to access the following site:

```
http://[ip_address_of_DNCS_host]/dncs/soap/bossreq
```

b If the computer you are using for the test has an IP address that is allowed to access the web service, the browser will return the following error message.

```
HTTP GET method not implemented
```

c If you receive a different error message, review all configuration changes against the previously executed procedures and repeat this step.

2 After the DNCS is configured, you can verify that the STB Staging web service is accessible using HTTP by completing the following steps.

a Use a web browser to access the following site:

```
http://[ip_address_of_DNCS_host]/dncs/soap/loadPIMS
```

b If the STB Staging web service is configured for basic user authentication, a username and password prompt should be displayed. Enter a valid STB Staging username and password.

c If the computer you are using for the test has an IP address that is allowed to access the web service, the browser will return the following error message:

```
HTTP GET method not implemented
```

d If you receive a different error message, review all configuration changes against the previously executed procedures and repeat this step.

Configure Remote Access to the DNCS Web Interface

Complete the following procedure to access the DNCS Web interface remotely.

Important: You must obtain the hostname and IP address for your corporate network-facing interface from your System Administrator to complete these steps. The examples below use *dncs1* as the hostname and *10.90.176.90* as the IP address. These are examples, only.

1. Log on to the DNCS as **root** user.
2. Open the /etc/hosts file with a text editor.
3. Add *dncseth* to your corporate network interface entry in the /etc/hosts file.

   Example: `10.90.176.90 dncs1 dncs1. loghost dncseth`
4. Add *dncsws* to the loopback2 entry in the /etc/hosts file.

   Example: `127.0.0.2  loopback2  dncsws`
5. Save and close the /etc/hosts file.
6. Open the /etc/apache2/user-conf/80.auth.conf file with a text editor.
7. Add *Allow from [machine/subnet IP Address]* before the "ErrorDocument" line.

   Example:

```
#ident "@(#) %full_filespec: 80.auth.conf,4:ascii:Da=1 %"
<Location />
 Order Allow,Deny
 Allow from localhost
 Allow from dncs
 Allow from dncseth
# Access restrictions can be enforced here, so that valid
users can only
# come from allowable hosts/(sub)networks e.g. :
 Allow from 64.100.86.0/24
 ErrorDocument 403 "<html><head><title>Error
403</title></head><body><h2>SECURITY WARNING</h2>Web
connections are not allowed from this location.</body></html>"
</Location>
```

8. Save and close the 80.auth.conf file.
9. Open the /etc/apache2/user-conf/httpd.ports file with a text editor.

10 Add an entry to "Listen to port 80" on the corporate-facing interface line.

Example:

```
#
#ident "@(#) %full_filespec: httpd.ports.dist,2:ascii:Da=2 %"
#
# This configuration file is for DNCS Web UI traffic.
# If $hostname is on a separate interface, it can be enabled
too, but
# we won't do that automatically.
#
# Listen: Allows you to bind Apache to specific IP addresses
and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown
below to
# prevent Apache from glomming onto all bound IP addresses
(0.0.0.0)
#
# This configuration file is for DNCS Web UI traffic.
# If $hostname is on a separate interface, it can be enabled
too, but
# we won't do that automatically.
Listen 0.0.0.0:8045
Listen 127.0.0.1:80
Listen dncseth:80
```

11 Save and close the httpd.ports file.

12 Type the following command and press **Enter** to restart the Apache server process.

```
svcadm restart http
```

Introduction to DNCS HTTPS Certificates

This section describes the files required and options available to implement TLS/SSL on the DNCS.

Certificate File Overview

Implementation of the SSL/TLS protocol to secure the connection between a DNCS and an external client, such as billing systems and STB staging clients, requires certificates.

The following is a high-level overview of the certificate files required on an HTTP-S server and client, and how they are created:

- **Private Key —** A private key file must be created for the HTTP-S server. This file must be well guarded and should never leave the HTTP-S server. It is preferable to generate the private key file on the HTTP-S server itself. The private key file is typically identified by the .key extension.
- **Certificate Signing Request (CSR) —** A CSR file must be created for the HTTP-S server for the certification authority (CA) to sign. This file includes the HTTP-S server identity information and a public key. The CSR is digitally signed (encrypted hash) with the private key. The CSR file is sent to the CA to sign. The CSR file is typically identified by the .csr extension.
- **HTTP-S Server Certificate —** The CA receives the CSR file and, if necessary, verifies that the originator of the CSR is genuine; that is, the sender of the CSR is who they say they are. The CA will then digitally sign the CSR with the private key of the CA. This creates the certificate file for the HTTP-S server. The certificate file is typically identified by the .crt extension.
- **HTTP-S Client Certificate —** If Client Authentication is required by the HTTP-S server, then a client certificate must be created. The same steps outlined in the previous three items can be used to create the client certificate. Note that you can use the one certificate for both the server certificate and client certificate.
- **Certification Authority Certificates —** The certification authority, also known as the Certificate Authority (CA), will have one or more self-signed certificates, the root certificates, and possibly intermediate certificates, which are CA certificates signed using a root certificate or another intermediate certificate. These certificates contain information about the CA, including the CA's common name, the CA's public key, and are digitally signed with the appropriate CA private key. The CA can be you, someone in your company, or can be a commercial CA such as VeriSign.

- **Certificate Chain —** The succession of certificates starting from the server or client certificate to the root certificate makes up a certificate chain. The shortest possible certificate chain is two: the server or client certificate and a root CA certificate. This occurs when the server or client certificate is signed by the root CA private key. To decrease the risk of compromising the root CA's private key, some Certification Authorities only use an intermediate certification authority to sign server or client certificates. It is also possible to use an intermediate CA to sign another intermediate CA certificate, thus the certificate chain becomes longer. The certificate chain is the entire certification path from the signed certificate to the root CA certificate.
- **CA Certificate Chain —** A CA certificate chain is the succession of intermediate CA certificates to the root certificate. If a server or client certificate is signed by the root CA, then the CA certificate chain contains only the root certificate. If a server or client certificate is signed by an intermediate CA, then the CA certificate chain contains all intermediate CA certificates and the root certificate. For example, if the client or server certificate was signed by intermediate CA 2 and the intermediate CA 2 certificate was signed by intermediate CA 1 which was signed by the root CA, then intermediate CA 2, intermediate CA 1, and the root certificate make up the CA certificate chain. The cachain.crt file on the DNCS must contain the entire CA certificate chain for the DNCS server certificate. The cacert.pem file on the DNCS must contain the entire CA certificate chain for the DNCS client certificate.
- **Trusted Certificate Authorities —** For an HTTP-S client to trust an HTTP-S server's certificate, the HTTP-S client must trust the server's root CA certificate. If client authentication is required on the HTTP-S server, the server must trust the client's root CA certificate. Web browsers, a type of HTTP-S client, typically include a set of trusted root CA certificates for companies such as VeriSign. The cacert.pem file on the DNCS must contain all of the trusted root CA certificates.

Certificate Files Required on the DNCS

A common set of certificate files are used for both web server instances on the DNCS. Two lists of certificate files for the DNCS follow.

- The first list contains the certificate files required when the DNCS acts as an HTTP-S server.
- The second list contains the certificate files required when the DNCS acts as an HTTP-S client, which is only applicable to the BOSS billing web service.

Note: All of the following files exist in the /etc/opt/certs directory on the DNCS.

- DNCS HTTPS Server
  - server key — The server private key.
  - server.crt — The server signed certificate.
  - cachain.crt — The server certificate CA certificate chain. This file must contain the entire CA certificate chain used to sign the server certificate.
  - cacert.pem — A collection of all trusted root certificates for remote clients. If client authentication is implemented, then this file must contain the root CA certificate for the remote client certificate.
- DNCS HTTPS Client
  - bossclient.key — A concatenation of the private key, certificate, and CA certificate chain used to sign the client certificate in the following order:
    - client private key
    - client certificate
    - intermediate CA certificates, if applicable
    - root CA certificate

    Important: The order of the CA certificate chain must follow the certification path starting with the intermediate CA certificate (if applicable) used to sign the client certificate and ending with the root CA certificate.
  - cacert.pem — A collection of all trusted root certificates for remote billing servers. This file must contain the root CA certificate for the billing system server certificate.

    Note: It is possible to define a different file than the cacert.pem file using the BOSS_SSL_CACERTS environment variable. This variable is not used in the steps within this guide. If you use this environmental variable, you must define it in the /export/home/dncs/.profile file. Additionally, the file referenced by the environment variable must be readable by the dncs role.

Certificate Deployment Options

The Open Source toolkit from the OpenSSL Project collaborative is included with the DNCS. This tool can be used to create the private key and the CSR file. It can also be used to create a CA on the DNCS, allowing you to sign and install your own CA certificates. This tool also includes testing functions.

For more information on the Open Source toolkit and for documentation on toolkit commands, go to: http://www.openssl.org.

The DNCS also includes a custom certificate creation and signing tool called gen_crt_dncs. The provided instructions direct you to use the appropriate tool. There are several different methods for creating and signing certificates. Instructions for these methods are detailed in the following sections:

- ***Generating and Deploying Self-Signed Certificates*** (on page 117)
- ***Generating and Deploying SSL Certificates Signed by a CA on a DNCS*** (on page 80)
- ***Deploying SSL Certificates Signed by an External CA*** (on page 93)

Notes:

- Use the root user to execute all commands in these sections. The following commands log the user on as root user:
  - **a** If necessary, open an xterm window on the DNCS.
  - **b** At the prompt, type `su -` and press **Enter**.
  - **c** Type the **root password** and press **Enter**.
- To implement SSL/TLS for the DNCS web server instances, it is helpful to have an understanding of SSL/TLS, the certificate generation process, and HTTP message flows. The following is a list of websites that can be used as references:
  - http://www.ietf.org/rfc/rfc2246.txt
  - http://www.freesoft.org/CIE/Topics/121.htm
  - http://en.wikipedia.org/wiki/Secure_Sockets_Layer
- Be sure to carefully plan for the implementation of SSL/TLS for the DNCS web services. Implementation of SSL/TLS should not be attempted during the upgrade maintenance window unless you have thoroughly planned and are well-prepared.
- Certificate expiration dates must be closely managed to ensure stability of the DNCS web services.

The gen_cert _dncs Utility

The DNCS gen_crt_dncs SSL Configuration Utility includes options to execute several of the steps necessary to generate and deploy certificates. The following is an overview of the utility options:

- **Option 1 —** The DNCS gen_crt_dncs SSL Configuration Utility creates a self-signed certificate (server.crt), private key (server.key), cachain.crt, and cacert.pem files and then enables HTTPS. This option is used as part of the ***Generating and Deploying Self-Signed Certificates*** (on page 117) method.
- **Option 2 —** The DNCS gen_crt_dncs SSL Configuration Utility generates a private key (server.key) and a Certificate Signing Request (CSR) file (server.csr) in the /etc/opt/certs directory. The CSR must be signed by a CA on a DNCS external CA.
- **Option 3 —** Not used.
- **Option 4 —** This option allows you to check that the necessary files are available and, if so, enables HTTPS.
  - If all needed files are available, HTTPS is enabled.
  - If any required files are not available, the output from this option includes detailed information about missing files.
- **Option 5 —** Exits the utility.

Enable HTTPS Access and Installing Certificates

Allowing HTTPS Access to the BOSS Web Service

Complete the following procedure to allow a specific billing system to have HTTPS access to the BOSS Web Service.

Note: Only an "Allow from" state is required for HTTPS access to the BOSS Web Service. Both an "Allow from" statement and a *REMOTE_ADDR* definition are required for HTTPS access to the BOSS Web Service. The *REMOTE_ADDR* statement is added later in this document.

1. Open an xterm window on the DNCS.
2. Log into the system as root:
   a. At the prompt, type `su -` and press **Enter**.
   b. Type the **root password** and press **Enter**.
3. Open the /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf file using a text editor.
4. Add the following line to the end of the "Allow from" list:

   ```
   Allow from [billing server IP]
   ```

   Notes:

   - Replace [billing server IP] with the IP address or hostname of the billing system.
   - If a hostname is used, the hostname and IP address must be defined in the /etc/hosts file.
   - An entire subnet can be allowed using slash notation.

   Example: The "Allow from" list should look similar to the following example:

   ```
   Order Allow,Deny
   Allow from localhost
   Allow from dncs dncs
   Allow from dncsws
   Allow from 172.16.20.1
   Allow from 172.10.1.0/24
   ```

5. Add the following line after the "SSLRequire" line.

   ```
   %{REMOTE_ADDR} eq "[billing server IP]" or \
   ```

   Notes:

   - Replace [billing server IP] with the IP address or hostname of the billing system.
   - A hostname cannot be used in place of an IP address.

- An entire subnet can be allowed using a regular expression. The *172.10.1.0/24* subnet would be represented as follows:

  ```
  m/^172\.10\.1\.[0-254]/
  ```

  Example: The "SSLRequire" statement should look similar to the following example:

  ```
  SSLRequire ( %{REMOTE_ADDR} eq "127.0.0.1" or \
               %{REMOTE_ADDR} eq "172.16.20.1" or \
               %{REMOTE_ADDR} =~ m/^172\.10\.1\.[0-254]/ or \
               %{SSL_CLIENT_VERIFY} eq "SUCCESS" )
  ```

6 Will only HTTPS access, not HTTP, be allowed for the BOSS web service?

- If **yes**, add the "SSLRequireSSL" line after the "SSLVerifyDepth" line.

  Note: The SSLRequireSSL line disables HTTP access to the STB Staging web.

  Example:

  ```
  SSLVerifyDepth  10
  SSLRequireSSL
  ```

- If **no**, HTTP and HTTPS support is required; skip to step 7.

7 Save and close the file.

8 Follow these instructions to restart the DNCS http process.

a Type the following command and press **Enter** to stop the http process:

```
svcadm -v disable -st http
```

b Type the following command and press **Enter** to refresh the http process:

```
svcadm refresh http
```

c Type the following command and press **Enter** to restart the http process:

```
svcadm -v enable -s http
```

Result: The system displays the **svc:/network/http:apache2 enabled** message.

9 Follow these instructions to restart the DNCS http-dncsws process.

a Type the following command and press **Enter** to stop the http-dncsws process:

```
svcadm -v disable -st http-dncsws
```

b Type the following command and press **Enter** to refresh the http-dncsws process:

```
svcadm refresh http-dncsws
```

c Type the following command and press **Enter** to restart the http-dncsws process:

```
svcadm -v enable -s http-dncsws
```

Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

Allowing HTTPS Access to the STB Staging Web Service

Complete the following procedure to allow a specific set-top staging client to have HTTPS access to the STB Staging Web Service.

1. Open an xterm window on the DNCS.
2. Log into the system as root:
   a. At the prompt, type `su -` and press **Enter**.
   b. Type the **root password** and press **Enter**.
3. Open the **/etc/apache2/user-conf/SAIdncs.loadPIMS.auth.conf** file using a text editor.
4. Add the following line to the end of the "Allow from" list.

   ```
   Allow from [STB Staging Client IP]
   ```

   Notes:

   - Replace [STB Staging Client IP] with the IP address or hostname of the STB staging client.
   - If a hostname is used, the hostname and IP address must be defined in the /etc/hosts file.
   - An entire subnet can be allowed using slash notation.

   Example: The "Allow from" list should look similar to the following example:

   ```
   Order Allow,Deny
   Allow from localhost
   Allow from dncs dncs
   Allow from dncsws
   Allow from 172.16.30.1
   Allow from 172.10.1.0/24
   ```

5. Will only HTTPS access, not HTTP, be allowed for the STB Staging web service?
   - If **yes**, verify that the `SSLRequireSSL` line is not commented out (it does not have a "**#**" at the beginning of the line). The SSLRequiresSSL line disables HTTP access to the STB Staging web service.
   - If **no**, HTTP and HTTPS support is required. Go to the next step.
6. Save and close the file.

7 Follow these instructions to restart the DNCS http process.

a Type the following command and press **Enter** to stop the http process:

```
svcadm -v disable -st http
```

b Type the following command and press **Enter** to refresh the http process:

```
svcadm refresh http
```

c Type the following command and press **Enter** to restart the http process:

```
svcadm -v enable -s http
```

Result: The system displays the **svc:/network/http:apache2 enabled** message.

8 Follow these instructions to restart the DNCS http-dncsws process.

a Type the following command and press **Enter** to stop the http-dncsws process:

```
svcadm -v disable -st http-dncsws
```

b Type the following command and press **Enter** to refresh the http-dncsws process:

```
svcadm refresh http-dncsws
```

c Type the following command and press **Enter** to restart the http-dncsws process:

```
svcadm -v enable -s http-dncsws
```

Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

Generating and Deploying SSL Certificates Signed by a CA on a DNCS

This section provides step-by-step instructions for generating the DNCS Web Service private key and (CSR) file, creating the DNCS certificate by signing the CSR file using a CA on a DNCS, and deploying the signed certificate.

The gen_crt_dncs utility is used to create the private key and CSR file, as well as deploying the signed certificate (server.crt) on the DNCS. The openssl tool is used to create the CA on a DNCS and sign the DNCS certificate. Please note that these instructions implement one certificate for the DNCS Web Service; that is, the same certificate is used for the DNCS HTTP-S server and HTTP-S client.

Notes:

- In these instructions, DNCS refers to the system that needs a certificate. DNCS CA refers to the DNCS that was chosen to be the CA. The DNCS and DNCS CA can be the same system.
- If a CA has not been created on the chosen DNCS, then follow the steps in ***Create Your Own Certification Authority*** (on page 105).

Create the DNCS Certificate Using a DNCS CA

To create, and deploy SSL certificates using a DNCS CA, complete the following steps.

1 From an xterm window on the DNCS, type the following command and press **Enter:**

```
/etc/apache2/gen_crt_dncs
```

Result: The system displays a message similar to the following:

```
Prepare SSL certificate for HTTPS service. HTTPS will not be
supported on
this host without an SSL certificate in place. Choose from
following options:
1. Generate a self-signed SSL certificate and deploy now. You
will need to manually deploy the certificate to those clients
connecting to this server.
2. Generate a certificate signing request for the server
certificate and proceed. No SSL certificate will be deployed,
you will need to sign the generated CSR file externally and
manually deploy it.
3. Import a server certificate for use by openssl and apache.
4. Check dependencies and enable apache SSL.
5. Exit - Skip this step now and manually deploy SSL
certificate later.
```

```
Refer to the system User's Guide for instructions.
Please enter your choice: [1|2|3|4|5]
```

2 Select choice **2** to create a certificate signing request and then press **Enter**. The system prompts you for the **Distinguished Name** attributes of the certificate.

3 Use these guidelines to answer the prompt displayed in step 2.

Note: We recommended that you provide valid input for the Distinguished Name information. Use a period (.) to indicate blank input.

- **Country Name —** The country where your company resides. Use the two-letter country code without punctuation for country (for example, US or FR).
- **State or Province —** The state or province where your company resides. Spell out the state completely (for example, California). Do not abbreviate the state or province name.
- **Locality or City —** The city or town where your company resides (for example, Berkeley).
- **Organization Name —** Your company's name (for example, XYZ Corporation). If your company or department name has an **&**, **@**, or any other symbol that requires using the **Shift** key in its name, you must spell out the symbol or omit it.
- **Organizational Unit —** The organization within the company. This field is optional but can be used to help identify certificates registered to an organization. The Organizational Unit (OU) field is the name of the department or organization unit making the request. To skip the OU field, press **Enter**.
- **Common Name —** The Common Name is the host plus the domain name (for example, **www.company.com** or ***.company.com**). For the DNCS, use the IP address of the interface that will be used for the DNCS Web Services.
- **Email Address —** E-mail address of the certificate requester.
- **Challenge Password —** Type **.** and then press **Enter**.
- **Optional Company Name —** Type **.** and then press **Enter**.

Result: The DNCS creates the CSR file (server.csr) and private key file (server.key) in the /etc/opt/certs directory.

4 Type the following command and press **Enter** to set the file permissions to *read-only* for the **root** user:

```
chmod 400 /etc/opt/certs/server.key
```

5 Copy the /etc/opt/certs/server.csr file from the DNCS to the DNCS CA /export/home/dncs/dncsCA/ directory.

6 Follow these steps to create the certificate file by signing the CSR on the DNCS CA.

   a If necessary, open an xterm window on the DNCS CA.

   b Type the following command and press **Enter:**

   ```
   cd /export/home/dncs/dncsCA
   ```

   c Type the following command and press **Enter:**

   ```
   /dvs/tools/openssl/bin/openssl x509 -req -days [days] -in
   server.csr -CA ca.crt -CAkey ca.key -set_serial [SN] -out
   server.crt
   ```

   Notes:

   – This is a single command.

   – Replace [days] with the number of days that the DNCS certificate will be valid.

   – Replace [SN] with a unique serial number for this certificate. This can be a decimal number or hexadecimal value if preceded by 0x (e.g. 0xDEADFACE).

   d When prompted, enter the ca.key pass phrase. The openssl x509 command saves the new certificate file, server.crt, in the current working directory, /export/home/dncs/dncsCA.

   e Copy the newly created /export/home/dncs/ncsCA/server.crt file from the DNCS CA to the DNCS /etc/opt/certs/ directory.

   f Copy the DNCS CA certificate file, /export/home/dncs/dncsCA/ca.crt, to the DNCS /etc/opt/certs/ directory.

   g Type the following command and press **Enter** to delete the server.crt file from the DNCS CA:

   ```
   rm  /export/home/dncs/dncsCA/server.crt
   ```

   h Type `exit` and then press **Enter** to exit from the DNCS CA.

7 If necessary, return to the /etc/opt/certs directory on the DNCS by typing the following command and pressing **Enter** in the xterm window:

```
cd /etc/opt/certs
```

8 Type the following command and press **Enter** to ensure that the certificate is globally readable:

```
chmod 444 /etc/opt/certs/server.crt
```

9 Follow these instructions to copy the DNCS CA certificate into the cachain.crt file and to ensure that the file is globally readable.

   a Type the following command and press **Enter:**

   ```
   cp /etc/opt/certs/ca.crt  /etc/opt/certs/cachain.crt
   ```

   b Type the following command and press **Enter:**

   ```
   chmod 444 /etc/opt/certs/cachain.crt
   ```

Add Trusted Root CA Certificates for the BOSS Web Service

Follow these instructions to copy the billing system's HTTP-S server root CA certificate to the list of trusted certificate authorities.

1 Obtain a copy of the root CA certificate in the CA certificate chain used to sign the billing system's HTTP-S server certificate and place it in the /etc/opt/certs directory of the DNCS. The root CA certificate must be in privacy-enhanced mail format (PEM) format.

Note: The text file must contain the entire root CA certificate starting with **BEGIN CERTIFICATE** and ending with **END CERTIFICATE**.

Example:

```
-----BEGIN CERTIFICATE-----
MIICWjCCAcMCAgGlMA0GCSqGSIb3DQEBBAUAMHUxCzAJBgNVBAYTAlVTMRgwFg
VQQKEw9HVEUgQ29ycG9yYXRpb24xJzAlBgNVBAsTHkdURSBDeWJlclRydXN0IF
bHV0aW9ucywgSW5jLjEjMCEGA1UEAxMaR1RFIEN5YmVyVHJ1c3QgR2xvYmFsIF
b3QwHhcNOTgwODEzMDAyOTAwWhcNMTgwODEzMjM1OTAwWjB1MQswCQYDVQQGEw
UzEYMBYGA1UEChMPR1RFIENvcnBvcmF0aW9uMScwJQYDVQQLEx5HVEUgQ3liZX
cnVzdCBTb2x1dGlvbnMsIEluYy4xIzAhBgNVBAMTGkdURSBDeWJlclRydXN0IE
b2JhbCBSb290MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCVD6C28FCc6H
iM3dFw4usJTQGz0O9pTAipTHBsiQl8i4ZBp6fmw8U+E3KHNgf7KXUwefU/ltWJ
r41tiGeA5u2ylc9yMcqlHHK6XALnZELn+aks1joNrI1CqiQBOeacPwGFVw1Yh0
04Wqk2kmhXBIgD8SFcd5tB8FLztimQIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAG
GwnpXtlR22ciYaQqPEh346B8pt5zohQDhT37qw4wxYMWM4ETCJ57NE7fQMh017
3PR2VX2bY1QY6fDq81yx2YtCHrnAlU66+tXifPVoYb+O7AWXX1uw16OFNMQkpw
lZPvy5TYnh+dXIVtx6quTx8itc2VrbqnzPmrC3p/
   -----END CERTIFICATE-----
```

2 Type the following command and press **Enter** to create the cacert.pem file:

```
cat /etc/opt/certs/[billing server Root CA Crt] >>
/etc/opt/certs/cacert.pem
```

Note: Replace [Billing Server Root CA Crt] with the root CA certificate of the CA chain used to sign the billing system's HTTPS server certificate.

Important: Do not attempt to append the root CA certificate to the cacert.pem file using a text editor.

Configure Client Authentication for the BOSS Web Service

Client authentication is optional for the DNCS BOSS web service. The BOSS web service does not require client authentication by default.

When client authentication is required by an HTTP-S Server, the HTTP-S client must provide a valid client certificate. When client authentication is optional for an HTTP-S Server, the server requests a valid client certificate but the client is not required to return one. If the client does return a certificate, it must be trusted by the server.

Complete the following steps to define client authentication on the DNCS.

1 Is client authentication required for the BOSS web service?

- If **yes**, go to step 2.
- If **no**, complete the following steps to disable client authentication.
  - **a** Use a text editor to open the /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf file.
  - **b** Change "optional" to "none" in the SSLVerifyClient line.

    Example:

    ```
    SSLVerifyClient none
    ```
  - **c** Save and close the file.
  - **d** Type the following command and press **Enter** to verify that the file was updated successfully:

    ```
    grep SSLVerifyClient /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf
    ```

    Result: Output should look similar to the following example:

    ```
    SSLVerifyClient none
    ```
  - **e** Is the BOSS web service configured to operate on the same web instance as the web UI?
    - If **yes**, complete the following steps to disable client authentication on the single web instance:
      1) Use a text editor to open the /etc/apache2/user-conf/443.auth.conf file.
      2) Change "optional" to "none" in the SSLVerifyClient optional line.
      3) Save and close the file.
    - If **no**, go to step f.
  - **f** Go to step 17.

2 Complete the following steps to concatenate the DNCS client private key and client certificate into the bossclient.key file.

Note: Unless a separate client certificate is required, the server certificate should be used. If a unique client certificate is required, then temporarily move the server.key, server.csr, server.crt, and ca.crt files to alternate names, and repeat steps 1 through 8 of the ***Create the DNCS Certificate using a DNCS CA*** (on page 80). Complete the following steps a through e. Provide a copy of the new server.crt file to the billing system administrator for use as the trusted root CA certificate for client authentication. Finally, move the original server.key, server.csr, server.crt and ca.crt files back after the completion of this step.

a Type the following command and press **Enter:**

```
cd /etc/opt/certs
```

b Type the following command and press **Enter** to create the necessary file for the BOSS client to return a client certificate when requested by the billing server:

```
cat server.key server.crt >> bossclient.key
```

c Type the following command and press **Enter** to set the ownership to the *dncs role* and *dncs group:*

```
chown dncs:dncs bossclient.key
```

d Type the following command and press **Enter** to set the necessary file permissions:

```
chmod 400 bossclient.key
```

e Type the following command and press **Enter** to add the CA certificate chain to the bossclient.key file:

```
cat ca.crt >> bossclient.key
```

3 Use a text editor to open the **/etc/apache2/user-conf/SAIdncs.bossreq.auth.conf** file.

4 Change "*optional*" to "*require*" in the SSLVerifyClient optional line.

Example:

```
SSLVerifyClient require
```

5 Save and close the file.

6 Type the following command and press **Enter** to verify that the file was updated successfully:

```
grep SSLVerifyClient /etc/apache2/user-
conf/SAIdncs.bossreq.auth.conf
```

Example: Output should look similar to the following example:

```
SSLVerifyClient require
```

7 Open the /export/home/dncs/.profile file with a text editor.

8 Add the following lines to the end of the file to enable the return of a client certificate from the BOSS for billing response messages:

```
# Enable BOSS client certificate return
BOSS_CLIENT_SSL_SETTINGS=7
export BOSS_CLIENT_SSL_SETTINGS
```

9 Save and close the file.

10 Type the following command and press **Enter** to switch to the **dncs** role:

```
su - dncs
```

11 If prompted, type the **dncs** role password and press **Enter**.

12 Type the following command and press **Enter** to source in the dncs .profile file:

```
. ./.profile
```

13 Type the following command and press **Enter** to stop the BOSS Server process:

```
dncsControl -stop bossServer
```

Note: The system displays **stopped(1)** when the bossServer process is stopped.

14 Type the following command and press **Enter** to restart the BOSS Server process.

```
dncsControl -start bossServer
```

Note: The system displays **running(2)** when the bossServer process has restarted.

15 Type `exit` and press **Enter** to log out of the dncs role.

16 Select one of the following options:

- If the billing system uses Client Authentication and utilizes the same certificate for both the server and the client, then skip to step 18.
- If the billing system uses two separate root CAs (one to sign the server certificate and one to sign the client certificate), then follow these instructions.
  - **a** Obtain a copy of the root CA certificate in the CA certificate chain used to sign the billing system's client certificate and place it in the **/etc/opt/certs** directory of the DNCS.
  - **b** Type the following command and press **Enter** to append the CA certificate to the cacert.pem file.

    ```
    cat /etc/opt/certs/[Billing Client Root CA Crt] >>
    /etc/opt/certs/cacert.pem
    ```

    Note: Replace [Billing Client Root CA Crt] with the root CA certificate of the CA chain used to sign the billing system's HTTPS client certificate. Do not attempt to append the second CA Certificate to the cacert.pem file using a text editor.

17 Follow these instructions to restart the DNCS http process.

a Type the following command and press **Enter** to stop the http process:

```
svcadm -v disable -st http
```

b Type the following command and press **Enter** to refresh the http process:

```
svcadm refresh http
```

c Type the following command and press **Enter** to restart the http process:

```
svcadm -v enable -s http
```

Result: The system displays the **svc:/network/http:apache2 enabled** message.

18 Follow these instructions to restart the DNCS http-dncsws process.

a Type the following command and press **Enter** to stop the http-dncsws process:

```
svcadm -v disable -st http-dncsws
```

b Type the following command and press **Enter** to refresh the http-dncsws process:

```
svcadm refresh http-dncsws
```

c Type the following command and press **Enter** to restart the http-dncsws process:

```
svcadm -v enable -s http-dncsws
```

Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

Prepare the DNCS Web Instance Trust Store

The cacert.pem file on the DNCS must contain all of the trusted root CA certificates. This file must exist with a minimum of one trusted certificate for the web instances to start. At this point, this file will either contain the trusted root CA certificates for the BOSS Web Service or not exist if the DNCS has only been configured for the STB Staging Web Service.

1 Type the following command and press **Enter:**

```
cat /etc/opt/certs/cacert.pem
```

2 Did the output from step 1 display certificate text?

- If **yes**, continue with step 3.
- If **no** (a **cannot open /etc/opt/certs/cacert.pem** message appears), then the cacert.pem file does not exist. Type the following command and press **Enter** to copy the cachain.crt file to cacert.pem.

```
cp /etc/opt/certs/cachain.crt /etc/opt/certs/cacert.pem
```

3 Type the following command and press **Enter** to set the file permissions:

```
chmod 444 /etc/opt/certs/cacert.pem
```

4 Follow these instructions to restart the DNCS http process.

a Type the following command and press **Enter** to stop the http process:

```
svcadm -v disable -st http
```

b Type the following command and press **Enter** to refresh the http process:

```
svcadm refresh http
```

c Type the following command and press **Enter** to restart the http process:

```
svcadm -v enable -s http
```

Result: The system displays the **svc:/network/http:apache2 enabled** message.

5 Follow these instructions to restart the DNCS http-dncsws process.

a Type the following command and press **Enter** to stop the http-dncsws process:

```
svcadm -v disable -st http-dncsws
```

b Type the following command and press **Enter** to refresh the http-dncsws process:

```
svcadm refresh http-dncsws
```

c Type the following command and press **Enter** to restart the http-dncsws process:

```
svcadm -v enable -s http-dncsws
```

Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

Verify the Running Status of the Web Server Instances

Complete the following steps to verify that the web server instances are running properly.

Note: Both web instances are checked even if you configured only one instance to support the web UI and the web services.

1 Type the following command and press **Enter** to verify the configuration and to enable HTTP-S.

```
/etc/apache2/gen_crt_dncs
```

Result: Output should look similar to the following example:

```
Prepare SSL certificate for HTTPS service. HTTPS will not be
supported on this host without an SSL certificate in place.
Choose from following options:

1. Generate a self-signed SSL certificate and deploy now. You
will need to manually deploy the certificate to those clients
connecting to this server.

2. Generate a certificate signing request for the server
certificate and proceed. No SSL certificate will be deployed,
you will need to sign the generated CSR file externally and
manually deploy it.
```

```
3. Import a server certificate for use by openssl and apache.
4. Check dependencies and enable apache SSL.
5. Exit - Skip this step now and manually deploy SSL
certificate later.
   Refer to the system User's Guide for instructions.
Please enter your choice: [1|2|3|4|5]
```

2 Select choice **4** and press **Enter**.

3 Type the following command and press **Enter:**

```
ps -ef | grep httpd
```

Example: Output should look similar to the following example:

```
root 21610     1   0 14:10:09 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
dncs 21614 21610   0 14:10:10 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
dncs 21615 21610   0 14:10:10 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
nobody 21594 21589   0 14:09:59 ?   0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-dncsws/httpd.conf
-k start -DSSL
root 21589     1   0 14:09:58 ?     0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-dncsws/httpd.conf
-k start -DSSL
root 27663 19973   0 14:28:06 pts/2 0:00 grep httpd
nobody 21593 21589   0 14:09:59 ?   0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-dncsws/httpd.conf
-k start -DSSL
```

4 Type the following command and press **Enter:**

```
lsof -i :443
```

Example: Output should look similar to the following example, but the **Name** column will vary, based on your specific configuration:

```
COMMAND   PID   USER   FD   TYPE        DEVICE SIZE/OFF NODE
NAME
httpd   21589   root  257u  IPv4 0x60019fa8340      0t0  TCP
ossbss:443 (LISTEN)
httpd   21593 nobody  257u  IPv4 0x60019fa8340      0t0  TCP
ossbss:443 (LISTEN)
httpd   21594 nobody  257u  IPv4 0x60019fa8340      0t0  TCP
ossbss:443 (LISTEN)
httpd   21610   root  259u  IPv4 0x60019f6d540      0t0  TCP
localhost:443 (LISTEN)
httpd   21614   dncs  259u  IPv4 0x60019f6d540      0t0  TCP
localhost:443 (LISTEN)
httpd   21615   dncs  259u  IPv4 0x60019f6d540      0t0  TCP
localhost:443 (LISTEN)
```

5 Did the output in step 3 include "**-DSSL**", AND did the output from step 4 include listen entries for the interface used in the ***Define the Web Service Interface for HTTPS Support Only*** (on page 59)?

- If **yes**, go to step 4.
- If **no**, complete the following steps.
  - **a** Type the following command and press **Enter** to stop the http process:
    ```
    svcadm -v disable -st http
    ```
  - **b** Type the following command and press **Enter** to refresh the http process:
    ```
    svcadm refresh http
    ```
  - **c** Type the following command and press **Enter** to restart the http process:
    ```
    svcadm -v enable -s http
    ```
    Result: The system displays the **svc:/network/http:apache2 enabled** message.
  - **d** Type the following command and press **Enter** to stop the http process:
    ```
    svcadm -v disable -st http-dncsws
    ```
  - **e** Type the following command and press **Enter** to refresh the http-dncsws process:
    ```
    svcadm refresh http-dncsws
    ```
  - **f** Type the following command and press **Enter** to restart the http-dncsws process:
    ```
    svcadm -v enable -s http-dncsws
    ```
    Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.
  - **g** Repeat steps 3 through 5.

6 Copy the **/export/home/dncs/dncsCA/ca.crt** file from the DNCS CA used to sign the DNCS HTTP-S certificate(s) to the appropriate location on the billing system and/or STB Staging Client for use as the trusted root CA certificate(s).

7 After the DNCS is configured, you can verify that the DNCS HTTP-S server certificates are deployed correctly and that the BOSS web service is accessible by completing the following steps.

a Use a web browser to access the following site:

```
https://[ip_address_of_DNCS_host]/dncs/soap/bossreq
```

Result: The web browser should prompt you to accept the certificate but warn that the certificate was issued by a company that you have not chosen to trust, similar to this example:

b Select the appropriate confirmation buttons to allow the web service to continue.

c Is client authorization enabled on this system?

– If **yes**, the web browser will either return a prompt for a client certificate or a connection failure message.

– If **no**, if the computer you are using for the test has an IP address that is allowed to access to the web service, the browser will return a **HTTP GET method not implemented** error message.

d To verify that the billing system HTTP-S server is accessible from the DNCS, use Firefox on the DNCS and enter the following address:

```
https://[ip_address_of_Billing_System_host]
```

8 After the DNCS is configured, you can verify that the DNCS HTTP-S server certificates are deployed correctly and the STB Staging web service is accessible by completing the following steps.

a Use a web browser to access the following site:

```
https://[ip_address_of_DNCS_host]/dncs/soap/loadPIMS
```

Result: The web browser should prompt you to accept the certificate but warn that the certificate was issued by a company that you have not chosen to trust, similar to this example:

b Select the necessary confirmation buttons to allow the web connection to continue.

c If the STB Staging web service is configured for basic user authentication, a username and password prompt should display. Enter a valid STB Staging username and password.

d If the computer you are using for the test has an IP address that is allowed to access the web service, the browser will return a **HTTP GET method not implemented** error message.

9 If you receive a different error message, review all configuration changes against the previously executed procedures and repeat this procedure.

Deploying SSL Certificates Signed by an External CA

This section provides step-by-step instructions for generating the DNCS Web Service private key and CSR files, and then deploying the Certificate signed by the external CA.

The gen_crt_dncs utility is used to create the private key and CSR file, as well as deploying the signed certificate (server.crt) on the DNCS. Note that these instructions implement one certificate for the DNCS Web Instance; that is, the same certificate is used for the DNCS HTTP-S server and HTTP-S client.

The Certification Authority can be someone or some group within your company or a commercial CA, such as VeriSign.

Create the DNCS Certificate Using an External CA

To create, and deploy SSL certificates using an External CA, complete the following steps.

1 From an xterm window on the DNCS, type the following command and press **Enter:**

```
/etc/apache2/gen_crt_dncs
```

Result: The system displays a message similar to the following.

```
Prepare SSL certificate for HTTPS service. HTTPS will not be
supported on
this host without an SSL certificate in place. Choose from
following options:
1. Generate a self-signed SSL certificate and deploy now. You
will need to manually deploy the certificate to those clients
connecting to this server.
2. Generate a certificate signing request for the server
certificate and proceed. No SSL certificate will be deployed,
you will need to sign the generated CSR file externally and
manually deploy it.
3. Import a server certificate for use by openssl and apache.
4. Check dependencies and enable apache SSL.
5. Exit - Skip this step now and manually deploy SSL
certificate later.
Refer to the system User's Guide for instructions.
Please enter your choice: [1|2|3|4|5]
```

2 Select choice **2** to create a certificate signing request and press **Enter**. The command prompts you for the **Distinguished Name** attributes of the certificate.

3 Use these guidelines to answer the prompt displayed in step 2.

Note: We recommended that you provide valid input for the Distinguished Name information. Use a period (.) to indicate blank input.

- **Country Name —** The country where your company resides. Use the two-letter country code without punctuation for country (for example, US or FR).
- **State or Province —** The state or province where your company resides. Spell out the state completely (for example, California). Do not abbreviate the state or province name.
- **Locality or City —** The city or town where your company resides (for example, Berkeley).
- **Organization Name —** Your company's name (for example, XYZ Corporation). If your company or department name has an **&**, **@**, or any other symbol that requires using the **Shift** key in its name, you must spell out the symbol or omit it.
- **Organizational Unit —** The organization within the company. This field is optional but can be used to help identify certificates registered to an organization. The Organizational Unit (OU) field is the name of the department or organization unit making the request. To skip the OU field, press **Enter**.
- **Common Name —** The Common Name is the host plus the domain name (for example, **www.company.com** or ***.company.com**). For the DNCS, use the IP address of the interface that will be used for the DNCS Web Services.
- **Email Address —** E-mail address of the certificate requester.
- **Challenge Password —** Type **.** and then press **Enter**.
- **Optional Company Name —** Type **.** and then press **Enter**.

Result: The DNCS creates the CSR file (server.csr) and private key file (server.key) in the /etc/opt/certs directory.

4 Type the following command and press **Enter** to set the file permissions to read-only for the root user:

```
chmod 400 /etc/opt/certs/server.key
```

5 Send a copy of the /etc/opt/certs/server.csr file from the DNCS to the external CA for signing.

6 After the signed DNCS certificate is returned, copy the certificate into the /etc/opt/certs/ directory.

7 From an xterm window on the DNCS, type the following command and press **Enter:**

```
cd /etc/opt/certs
```

8 Type the following command and press **Enter:**

```
mv [certificate] /etc/opt/certs/server.crt
```

Note: Replace [certificate] with the name of the signed certificate file from the external CA.

9 Type the following command and press **Enter** to ensure that the certificate is globally readable:

```
chmod 444 /etc/opt/certs/server.crt
```

10 Obtain a copy of the external CA's certificate chain, (the root CA certificate, and any intermediate CA certificates,) that was used to sign the DNCS Web Server HTTP-S server certificate. Then, place it in the /etc/op/certs/ directory.

11 Type the following command and press **Enter** to create the cachain.crt file on the DNCS:

```
cat [caCertificateChain] >> /etc/opt/certs/cachain.crt
```

12 Type the following command and press **Enter** to set the cachain.crt file permissions to read for all:

```
chmod 444 cachain.crt
```

Add Trusted Root CA Certificates for the BOSS Web Service

Follow these instructions to copy the billing system's HTTP-S server root CA certificate to the list of trusted certificate authorities.

1 Obtain a copy of the root CA certificate in the CA certificate chain used to sign the billing system's HTTP-S server certificate and place it in the /etc/opt/certs directory of the DNCS. The root CA certificate must be in privacy-enhanced mail format (PEM) format.

Note: The text file must contain the entire root CA certificate starting with **BEGIN CERTIFICATE** and ending with **END CERTIFICATE**.

Example:

```
-----BEGIN CERTIFICATE-----
MIICWjCCAcMCAgGlMA0GCSqGSIb3DQEBBAUAMHUxCzAJBgNVBAYTAlVTMRgwFg
VQQKEw9HVEUgQ29ycG9yYXRpb24xJzAlBgNVBAsTHkdURSBDeWJlclRydXN0IF
bHV0aW9ucywgSW5jLjEjMCEGA1UEAxMaR1RFIEN5YmVyVHJ1c3QgR2xvYmFsIF
b3QwHhcNOTgwODEzMDAyOTAwWhcNMTgwODEzMjM1OTAwWjB1MQswCQYDVQQGEw
UzEYMBYGA1UEChMPR1RFIENvcnBvcmF0aW9uMScwJQYDVQQLEx5HVEUgQ3liZX
cnVzdCBTb2x1dGlvbnMsIEluYy4xIzAhBgNVBAMTGkdURSBDeWJlclRydXN0IE
b2JhbCBSb290MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCVD6C28FCc6H
iM3dFw4usJTQGz0O9pTAipTHBsiQl8i4ZBp6fmw8U+E3KHNgf7KXUwefU/ltWJ
r41tiGeA5u2ylc9yMcqlHHK6XALnZELn+aks1joNrI1CqiQBOeacPwGFVw1Yh0
04Wqk2kmhXBIgD8SFcd5tB8FLztimQIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAG
GwnpXtlR22ciYaQqPEh346B8pt5zohQDhT37qw4wxYMWM4ETCJ57NE7fQMh017
3PR2VX2bY1QY6fDq81yx2YtCHrnAlU66+tXifPVoYb+O7AWXX1uw16OFNMQkpw
```

```
lZPvy5TYnh+dXIVtx6quTx8itc2VrbqnzPmrC3p/
   -----END CERTIFICATE-----
```

2 Type the following command and press **Enter** to create the cacert.pem file:

```
cat /etc/opt/certs/[billing server Root CA Crt] >>
/etc/opt/certs/cacert.pem
```

Note: Replace [Billing Server Root CA Crt] with the root CA certificate of the CA chain used to sign the billing system's HTTPS server certificate.

Important: Do not attempt to append the root CA certificate to the cacert.pem file using a text editor.

Configure Client Authentication for the BOSS Web Service

Client authentication is optional for the DNCS BOSS web service. The BOSS web service does not require client authentication by default. When client authentication is required by an HTTP-S Server, the HTTP-S client must provide a valid client certificate.

When client authentication is optional for an HTTP-S Server, the server requests a valid client certificate but the client is not required to return one. If the client does return a certificate, it must be trusted by the server.

Complete the following steps to define client authentication on the DNCS.

1 Is client authentication required for the BOSS web service?

- If **yes**, go to step 2.
- If **no**, complete the following steps to disable client authentication.

a Use a text editor to open the /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf file.

b Change "optional" to "none" in the SSLVerifyClient line.

Example:

```
SSLVerifyClient none
```

c Save and close the file.

d Type the following command and press **Enter** to verify that the file was updated successfully:

```
grep SSLVerifyClient /etc/apache2/user-
conf/SAIdncs.bossreq.auth.conf
```

Result: Output should look similar to the following example:

```
SSLVerifyClient none
```

e Is the BOSS web service configured to operate on the same web instance as the web UI?

– If **yes**, complete the following steps to disable client authentication on the single web instance:

i Use a text editor to open the /etc/apache2/user-conf/443.auth.conf file.

ii Change "optional" to "none" in the SSLVerifyClient optional line.

Example:

```
SSLVerifyClient none
```

iii Save and close the file.

– If **no**, go to step f.

f Go to step 17.

2 Complete the following steps to concatenate the DNCS client private key and client certificate into the bossclient.key file.

Note: Unless a separate client certificate is required, the server certificate should be used. If a unique client certificate is required, then temporarily move the server.key and server.crt files to alternate names, repeat steps 1 through 6 of ***Create the DNCS Certificate Using an External CA*** (on page 93). Complete the following steps a through d. Provide a copy of the new server.crt file to the billing system administrator for use as the trusted root CA certificate for client authentication. Finally, move the original server.key and server.crt files back after the completion of these steps.

a Type the following command and press **Enter:**

```
cd /etc/opt/certs
```

b Type the following command and press **Enter** to create the necessary file for the BOSS client to return a client certificate when requested by the billing server:

```
cat server.key server.crt >> bossclient.key
```

c Type the following command and press **Enter** to set the ownership to the *dncs role* and *dncs group:*

```
chown dncs:dncs bossclient.key
```

d Type the following command and press **Enter** to set the necessary file permissions:

```
chmod 400 bossclient.key
```

3 Use a text editor to open the /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf file.

4 Change "*optional*" to "*require*" in the SSLVerifyClient optional line.

Example:

```
SSLVerifyClient require
```

5 Save and close the file.

6 Type the following command and press **Enter** to verify that the file was updated successfully.

```
grep SSLVerifyClient /etc/apache2/user-
conf/SAIdncs.bossreq.auth.conf
```

Example: Output should look similar to the following example:

```
SSLVerifyClient require
```

7 Open the /export/home/dncs/.profile file with a text editor.

8 Add the following lines to the end of the file to enable the return of a client certificate from the BOSS for billing response messages.

```
# Enable BOSS client certificate return
BOSS_CLIENT_SSL_SETTINGS=7
export BOSS_CLIENT_SSL_SETTINGS
```

9 Save and close the file.

10 Type the following command and press **Enter** to switch to the **dncs** role:

```
su - dncs
```

11 If prompted, type the dncs role password and press **Enter**.

12 Type the following command and press **Enter** to source in the dncs .profile file:

```
. ./.profile
```

13 Type the following command and press **Enter** to stop the BOSS Server process:

```
dncsControl -stop bossServer
```

Note: The system displays **stopped(1)** when the bossServer process is stopped.

14 Type the following command and press **Enter** to restart the BOSS Server process:

```
dncsControl -start bossServer
```

Note: The system displays **running(2)** when the bossServer process has restarted.

15 Type `exit` and press **Enter** to log out of the dncs role.

16 Select one of the following options:

- If the billing system uses Client Authentication and utilizes the same certificate for both the server and the client, then go to the next step.
- If the billing system uses two separate root CAs (one to sign the server certificate and one to sign the client certificate), then follow these instructions.
  - **a** Obtain a copy of the root CA certificate in the CA certificate chain used to sign the billing system's client certificate and place it in the /etc/opt/certs directory of the DNCS.
  - **b** Type the following command and press **Enter** to append the CA certificate to the cacert.pem file:

    ```
    cat /etc/opt/certs/[Billing Client Root CA Crt] >>
    /etc/opt/certs/cacert.pem
    ```

    Note: Replace [Billing Client Root CA Crt] with the root CA certificate of the CA chain used to sign the billing system's HTTPS client certificate. Do not attempt to append the second CA Certificate to the cacert.pem file using a text editor.

17 Follow these instructions to restart the DNCS http process.

- **a** Type the following command and press **Enter** to stop the http process:

  ```
  svcadm -v disable -st http
  ```

- **b** Type the following command and press **Enter** to refresh the http process:

  ```
  svcadm refresh http
  ```

- **c** Type the following command and press **Enter** to restart the http process:

  ```
  svcadm -v enable -s http
  ```

  Result: The system displays the **svc:/network/http:apache2 enabled** message.

18 Follow these instructions to restart the DNCS http-dncsws process.

- **a** Type the following command and press **Enter** to stop the http-dncsws process:

  ```
  svcadm -v disable -st http-dncsws
  ```

- **b** Type the following command and press **Enter** to refresh the http-dncsws process:

  ```
  svcadm refresh http-dncsws
  ```

- **c** Type the following command and press **Enter** to restart the http-dncsws process:

  ```
  svcadm -v enable -s http-dncsws
  ```

  Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

Prepare the DNCS Web Instance Trust Store

The cacert.pem file on the DNCS must contain all of the trusted root CA certificates. This file must exist with a minimum of one trusted certificate for the web instances to start. At this point, this file will either contain the trusted root CA certificates for the BOSS Web Service or not exist if the DNCS has only been configured for the STB Staging Web Service.

1 Type the following command and press **Enter:**

```
cat /etc/opt/certs/cacert.pem
```

2 Did the output from step 1 display certificate text?

- If **yes**, continue with step 3.
- If **no** (a **cannot open /etc/opt/certs/cacert.pem** message appears), then the cacert.pem file does not exist. Type the following command and press **Enter** to copy the cachain.crt file to cacert.pem.

  ```
  cp /etc/opt/certs/cachain.crt /etc/opt/certs/cacert.pem
  ```

3 Type the following command and press **Enter** to set the file permissions:

```
chmod 444 /etc/opt/certs/cacert.pem
```

4 Follow these instructions to restart the DNCS http process.

a Type the following command and press **Enter** to stop the http process:

```
svcadm -v disable -st http
```

b Type the following command and press **Enter** to refresh the http process:

```
svcadm refresh http
```

c Type the following command and press **Enter** to restart the http process:

```
svcadm -v enable -s http
```

Result: The system displays the **svc:/network/http:apache2 enabled** message.

5 Follow these instructions to restart the DNCS http-dncsws process.

a Type the following command and press **Enter** to stop the http-dncsws process:

```
svcadm -v disable -st http-dncsws
```

b Type the following command and press **Enter** to refresh the http-dncsws process:

```
svcadm refresh http-dncsws
```

c Type the following command and press **Enter** to restart the http-dncsws process:

```
svcadm -v enable -s http-dncsws
```

Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

Verify the Running Status of the http Web Server Instance

Complete the following steps to verify that the web server instances are running properly.

Note: Both web instances are checked even if you configured only one instance to support the web UI and the web services.

1 Type the following command and press **Enter** to verify the configuration and to enable HTTP-S.

```
/etc/apache2/gen_crt_dncs
```

Result: Output should look similar to the following:

```
Prepare SSL certificate for HTTPS service. HTTPS will not be
supported on
this host without an SSL certificate in place. Choose from
following options:
1. Generate a self-signed SSL certificate and deploy now. You
will need to
manually deploy the certificate to those clients connecting to
this server.
2. Generate a certificate signing request for the server
certificate and
proceed. No SSL certificate will be deployed, you will need to
sign the
generated CSR file externally and manually deploy it.
3. Import a server certificate for use by openssl and apache.
4. Check dependencies and enable apache SSL.
5. Exit - Skip this step now and manually deploy SSL
certificate later.
   Refer to the system User's Guide for instructions.
Please enter your choice: [1|2|3|4|5]
```

2 Select choice **4** and press **Enter**.

3 Type the following command and press **Enter**.

```
ps -ef | grep httpd
```

Example: Output should look similar to the following example:

```
root 21610     1   0 14:10:09 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
dncs 21614 21610   0 14:10:10 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
dncs 21615 21610   0 14:10:10 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
nobody 21594 21589 0 14:09:59 ?     0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-dncsws/httpd.conf
-k start -DSSL
```

```
root 21589     1   0 14:09:58 ?     0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-dncsws/httpd.conf
-k start -DSSL
root 27663 19973   0 14:28:06 pts/2 0:00 grep httpd
nobody 21593 21589   0 14:09:59 ?   0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-dncsws/httpd.conf
-k start -DSSL
```

4 Type the following command and press **Enter**.

```
lsof -i :443
```

Example: Output should look similar to the following example, but the Name column will vary, based on your specific configuration:

```
COMMAND   PID   USER   FD   TYPE        DEVICE SIZE/OFF NODE
NAME
httpd   21589   root  257u  IPv4 0x60019fa8340      0t0  TCP
ossbss:443 (LISTEN)
httpd   21593 nobody  257u  IPv4 0x60019fa8340      0t0  TCP
ossbss:443 (LISTEN)
httpd   21594 nobody  257u  IPv4 0x60019fa8340      0t0  TCP
ossbss:443 (LISTEN)
httpd   21610   root  259u  IPv4 0x60019f6d540      0t0  TCP
localhost:443 (LISTEN)
httpd   21614   dncs  259u  IPv4 0x60019f6d540      0t0  TCP
localhost:443 (LISTEN)
httpd   21615   dncs  259u  IPv4 0x60019f6d540      0t0  TCP
localhost:443 (LISTEN)
```

5 Did the output in step 3 include "-DSSL", AND did the output from step 4 include listen entries for the interface used in the ***Define the Web Service Interface for HTTPS Support Only*** (on page 59) ?

- If **yes**, go to step 6.
- If **no**, complete these steps.
  - **a** Type the following command and press **Enter** to stop the http process:
    ```
    svcadm -v disable -st http
    ```
  - **b** Type the following command and press **Enter** to refresh the http process:
    ```
    svcadm refresh http
    ```
  - **c** Type the following command and press **Enter** to restart the http process:
    ```
    svcadm -v enable -s http
    ```
    Result: The system displays the svc:/network/http:apache2 enabled message.
  - **d** Type the following command and press **Enter** to stop the http-dncsws process:
    ```
    svcadm -v disable -st http-dncsws
    ```

e Type the following command and press **Enter** to refresh the http-dncsws process:

```
svcadm refresh http-dncsws
```

f Type the following command and press **Enter** to restart the http-dncsws process:

```
svcadm -v enable -s http-dncsws
```

Result: The system displays the svc:/network/http-dncsws:apache2-dncsws enabled message.

g Repeat steps 3 through 5.

6 Copy the root CA certificate file from the CA certificate chain used to sign the DNCS HTTP-S certificate(s) to the appropriate location on the billing system and/or STB Staging Client for use as the trusted root CA certificate(s).

7 After the DNCS is configured, you can verify that the DNCS HTTP-S server certificates are deployed correctly and that the BOSS web service is accessible by completing the following steps.

a Use a web browser to access the following site:

```
https://[ip_address_of_DNCS_host]/dncs/soap/bossreq
```

Result: The web browser should prompt you to accept the certificate but warn that the certificate was issued by a company that you have not chosen to trust, similar to this example:

b Select the appropriate confirmation buttons to allow the web service to continue.

c Is client authorization enabled on this system?

– If **yes**, the web browser will either return a prompt for a client certificate or a connection failure message.

– If **no**, if the computer you are using for the test has an IP address that is allowed to access to the web service, the browser will return a **HTTP GET method not implemented** error message.

d To verify that the billing system HTTP-S server is accessible from the DNCS, use Firefox on the DNCS and enter the following address:

```
https://[ip_address_of_Billing_System_host]
```

8 After the DNCS is configured, you can verify that the DNCS HTTP-S server certificates are deployed correctly and the STB Staging web service is accessible by completing the following steps.

a Use a web browser to access the following site:

`https://[ip_address_of_DNCS_host]/dncs/soap/loadPIMS`

Result: The web browser should prompt you to accept the certificate but warn that the certificate was issued by a company that you have not chosen to trust, similar to this example:

b Select the necessary confirmation buttons to allow the web connection to continue.

c If the STB Staging web service is configured for basic user authentication then a username and password prompt should display. Enter a valid STB Staging username and password.

d If the computer you are using for the test has an IP address that is allowed to access the web service, the browser will return a **HTTP GET method not implemented** error message.

9 If you receive a different error message, review all configuration changes against the previously executed procedures and repeat this procedure.

Create Your Own Certification Authority

A Certification Authority (CA) is an entity that signs certificate files for web servers and web clients.

A CA can exist within a company or on your own computer. There are also commercial CAs, such as VeriSign, that create certificates for a fee.

This section includes instructions for creating a CA on a DNCS. We recommend that you create one CA on only one DNCS within your company. This one CA can be used to sign certificates for all other DNCS servers. This is the preferred method so that only one CA certificate is required for distribution to all other DNCS servers and web systems or billing systems and STB Staging Clients.

The CA key file will be used every time you sign a certificate and must NEVER leave the DNCS that is acting as the CA. The CA Certificate must be copied to all HTTP-S clients and HTTP-S servers that use Client Authentication and all HTTP-S clients that will receive certificates signed by this CA. In other words, the ca.crt file should be propagated to all DNCS servers and associated web or billing systems and STB Staging Clients.

Creating Your Own Certification Authority

Follow these steps to create a CA key file (ca.key) and a CA certificate (ca.crt) on the selected DNCS.

1. Log onto the DNCS that will be the CA and open an xterm window as **root** user.
2. Type the following command and press **Enter** to create a directory for all of the necessary CA files:

   ```
   mkdir /export/home/dncs/dncsCA
   ```

3. Type the following command and press **Enter:**

   ```
   cd /export/home/dncs/dncsCA
   ```

   Important: Ensure that you include this directory in the list of key files that must be backed up and restored for every upgrade.

4. Type the following command and press **Enter**. The system prompts you to enter a ca.key pass phrase:

   ```
   /dvs/tools/openssl/bin/openssl genrsa -des3 -out ca.key 4096
   ```

   Notes:

   - This pass phrase is needed every time this CA signs a certificate request.
   - Keep this pass phrase very secure. To ensure the highest level of security, never move or copy the key file to any other system.

- The `openssl genrsa` command saves the ca.key file in your current working directory.
- The generated key is a 4096-bit RSA key, which is encrypted using Triple DES and stored in PEM format so that it is readable as ASCII text.

5 Type the following command and press **Enter** to change the ca.key file permissions to *read only*, for the **root** user:

```
chmod 400 ca.key
```

Important: Keep this key file safely guarded. Any breach of this file will compromise the root CA certificate trust.

6 Type the following command and press **Enter** to generate the CA certificate. A prompt for a pass phrase appears:

```
/dvs/tools/openssl/bin/openssl req -new -x509 -days [days] -
key ca.key -out ca.crt
```

Notes:

- This is a single command.
- Replace `[days]` with the number of days the root CA certificate is valid. We suggested that this value be as long as possible to reduce the impact of re-deploying signed certificates. Do not type the brackets (**[ ]**) in the command.

7 Type the ca.key pass phrase that was just created and then press **Enter**. You are prompted for the following **Distinguished Name** attributes of the certificate. We recommended that you provide valid input for all Distinguished Name information. Use a period (.) to indicate blank input.

- **Country Name —** The country where your company resides. Use the two-letter country code without punctuation for country (for example, US or FR).
- **State or Province —** The state or province where your company resides. Spell out the state completely (for example, California). Do not abbreviate the state or province name.
- **Locality or City —** The city or town where your company resides (for example, Berkeley).
- **Organization Name —** Your company's name (for example, XYZ Corporation). If your company or department name has an **&**, **@**, or any other symbol that requires using the **Shift** key in its name, you must spell out the symbol or omit it.
- **Organizational Unit —** The organization within the company. This field is optional but can be used to help identify certificates registered to an organization. The Organizational Unit (OU) field is the name of the department or organization unit making the request. To skip the OU field, press **Enter**.

- **Common Name —** The Common Name is the host plus the domain name (for example, **www.company.com** or ***.company.com**). For the DNCS, use the IP address of the interface that will be used for the DNCS web services.
- **Email Address —** E-mail address of the certificate requester.

8 Type `ls -l` and then press **Enter** to verify that the ca.key and ca.crt files were created successfully. Output should look similar to the following:

```
-rw-r-----   1 root     root        2358 Oct 24 17:30 ca.crt
-r--------   1 root     root        3311 Oct 24 16:28 ca.key
```

Note: The `-l` in the command is a lowercase L, not the number 1 (one).

Troubleshooting SSL/TLS on the DNCS

DNCS Web Service Process Check

Complete the following steps to verify that the DNCS Web Service http processes are running properly.

1 Type the following command and press **Enter**.

```
ps -ef | grep httpd
```

Result: Output should look similar to the following example:

```
root   21610  1     0 14:10:09 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
dncs   21614  21610 0 14:10:10 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
dncs   21615  21610 0 14:10:10 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
nobody 21594  21589 0 14:09:59 ?     0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-dncsws/httpd.conf
-k start -DSSL
root   21589  1     0 14:09:58 ?     0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-dncsws/httpd.conf
-k start -DSSL
root   27663  19973 0 14:28:06 pts/2 0:00 grep httpd
nobody 21593  21589 0 14:09:59 ?     0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-dncsws/httpd.conf
-k start -DSSL
```

Note: If SSL/TLS is not enabled, "**-DSSL**" will not appear at the end of each line.

2 Type the following command and press **Enter**.

```
lsof -i :443
```

Result: Output should look similar to the following example, but the Name column will vary, based on your specific configuration:

```
COMMAND PID   USER   FD   TYPE DEVICE        SIZE/OFF NODE
NAME
httpd   21589 root   257u IPv4 0x60019fa8340 0t0      TCP
ossbss:443 (LISTEN)
httpd   21593 nobody 257u IPv4 0x60019fa8340 0t0      TCP
ossbss:443 (LISTEN)
httpd   21594 nobody 257u IPv4 0x60019fa8340 0t0      TCP
ossbss:443 (LISTEN)
httpd   21610 root   259u IPv4 0x60019f6d540 0t0      TCP
localhost:443 (LISTEN)
httpd   21614 dncs   259u IPv4 0x60019f6d540 0t0      TCP
localhost:443 (LISTEN)
```

```
httpd   21615 dncs   259u IPv4 0x60019f6d540 0t0      TCP
localhost:443 (LISTEN)
```

Note: If TLS/SSL is not enabled, no data is displayed.

3 If your output does not match what is displayed in steps 1 and 2, complete the following steps to stop and restart the DNCS web service instances.

a Type the following command and press **Enter** to stop the http process:

```
svcadm -v disable -st http
```

b Type the following command and press **Enter** to refresh the http process:

```
svcadm refresh http
```

c Type the following command and press **Enter** to restart the http process:

```
svcadm -v enable -s http
```

Result: The system displays the **svc:/network/http:apache2 enabled** message.

d Type the following command and press **Enter** to stop the http-dncsws process:

```
svcadm -v disable -st http-dncsws
```

e Type the following command and press **Enter** to refresh the http-dncsws process:

```
svcadm refresh http-dncsws
```

f Type the following command and press **Enter** to restart the http-dncsws process:

```
svcadm -v enable -s http-dncsws
```

Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

g Repeat steps 1 and 2.

4 If TLS/SSL has been implemented, you can verify that the DNCS HTTP-S server certificates are deployed correctly and the BOSS web service is accessible by completing the following steps.

a Use a web browser to access the following site:

```
https://[ip_address_of_DNCS_host]/dncs/soap/bossreq
```

Result: The web browser should prompt you to accept the certificate but warn that the certificate was issued by a company that you have not chosen to trust, similar to this example:

b Select the necessary confirmation buttons to allow the web connection to continue.

c Is client authentication enabled on this system?

– If **yes**, the web browser will either return a prompt for a client certificate or a connection failure message.

– If **no**, if the computer you are using for the test has an IP address that is allowed to access the web service, the browser will return a **HTTP GET method not implemented** error message.

d To verify that the billing system HTTP-S server is accessible from the DNCS, use Firefox on the DNCS and enter the following address:

```
https://[ip_address_of_Billing_System_host]
```

5 If TLS/SSL has been implemented, you can verify that the DNCS HTTP-S server certificates are deployed correctly and the STB Staging web service is accessible by completing the following steps.

a Use a web browser to access the following site:

`https://[ip_address_of_DNCS_host]/dncs/soap/loadPIMS`

Result: The web browser should prompt you to accept the certificate but warn that the certificate was issued by a company that you have not chosen to trust, similar to this example:

b Select the necessary confirmation buttons to allow the web connection to continue.

c If the STB Staging web service is configured for basic user authentication then a username and password prompt should be displayed. Enter a valid STB Staging username and password.

d If the computer you are using for the test has an IP address that is allowed to access the web service, the browser will return a **HTTP GET method not implemented** error message.

6 After the DNCS is configured, you can verify that the BOSS web service is accessible using HTTP by completing the following steps.

a Use a web browser to access the following site:

`http://[ip_address_of_DNCS_host]/dncs/soap/bossreq`

b If the computer you are using for the test has an IP address that is allowed to access the web service, the browser will return a **HTTP GET method not implemented** error message.

7 After the DNCS is configured, you can verify that the STB Staging web service is accessible using HTTP by completing the following steps.

a Use a web browser to access the following site:

`http://[ip_address_of_DNCS_host]/dncs/soap/loadPIMS`

b If the STB Staging web service is configured for basic user authentication, then a username and password prompt should be displayed. Enter a valid STB Staging username and password.

c If the computer you are using for the test has an IP address that is allowed to access the web service then the browser will return a **HTTP GET method not implemented** error message.

8 If you receive a different error message, review all configuration changes against the previously executed procedures and repeat this procedure.

Log Files to Monitor

The following is a list of several log files that can be monitored for errors related to HTTPS sessions:

- /dvs/dncs/tmp/bossServer.x
  - Type the following command and press **Enter** to increase the log level for the bossServer process.

    ```
    logLvl bossServer +DEBUG
    ```

  - Type the following command and press **Enter** to reduce the log level for the bossServer process once troubleshooting is complete.

    ```
    logLvl bossServer -DEBUG
    ```

  - Type the following command and press **Enter** to increase the log level for the bossServer SOAP process.

    ```
    logLvl bossServer.soap +DEBUG
    ```

  - Type the following command and press **Enter** to reduce the log level for the bossServer SOAP process once troubleshooting is complete.

    ```
    logLvl bossServer.soap -DEBUG
    ```

- Files in the /var/apache2/logs directory

Files and Directory Permissions

File and directory permissions are critical for the operation of the web servers on the DNCS. The following is a sample error message from the bossServer log when permissions are incorrect for the /etc/opt/certs/cacert.pem file:

```
|ERROR|bossServer:BossResponseClientSoap.C(99)|SOAP FAULT: SOAP-
ENV:Server SOAP-ENV:Server SSL error Can't read CA file and
directory  initializing context
```

The following is a list of the required permissions for the required files and directory:

- `drwxr-xr-x 7 root sys  1024 Jul 16 19:41 /etc/opt/certs`
- `-r-------- 1 root root 887  Jul 16 18:43 server.key`
- `-r--r--r-- 1 root root 1419 Jul 16 18:43 server.crt`
- `-r--r--r-- 1 root root 4716 Jul 16 13:53 cachain.crt`

- `-r-------- 1 dncs dncs 2294 Jul 16 18:39 bossclient.key`
- `-r--r--r-- 1 root root 9456 Jul 16 19:43 cacert.pem`

View Certificate Files

You can use the following command to view certificate files. Viewing the contents of certificate files can be helpful if the file name is generic.

```
/dvs/tools/openssl/bin/openssl x509 -text -in [certificate]
```

Note: Replace `[certificate]` with the name of the certificate file that you would like to view. Do not type the brackets (**[ ]**) in the command.

Add Trusted Root CA Certificates

Complete the following procedure to add a trusted root CA certificate to the list of trusted certificate authorities.

1 Obtain a text copy of the root CA certificate and place it in the /etc/opt/certs directory on the DNCS.

Note: The text file must contain the entire certificate starting with **-----BEGIN CERTIFICATE-----** and ending with **-----END CERTIFICATE-----**.

Example:

```
-----BEGIN CERTIFICATE-----
MIICWjCCAcMCAgGlMA0GCSqGSIb3DQEBBAUAMHUxCzAJBgNVBAYTAlVTMRgwFg
VQQKEw9HVEUgQ29ycG9yYXRpb24xJzAlBgNVBAsTHkdURSBDeWJlclRydXN0IF
bHV0aW9ucywgSW5jLjEjMCEGA1UEAxMaR1RFIEN5YmVyVHJ1c3QgR2xvYmFsIF
b3QwHhcNOTgwODEzMDAyOTAwWhcNMTgwODEzMjM1OTAwWjB1MQswCQYDVQQGEw
UzEYMBYGA1UEChMPR1RFIENvcnBvcmF0aW9uMScwJQYDVQQLEx5HVEUgQ3liZX
cnVzdCBTb2x1dGlvbnMsIEluYy4xIzAhBgNVBAMTGkdURSBDeWJlclRydXN0IE
b2JhbCBSb290MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCVD6C28FCc6H
iM3dFw4usJTQGz0O9pTAipTHBsiQl8i4ZBp6fmw8U+E3KHNgf7KXUwefU/ltWJ
r41tiGeA5u2ylc9yMcqlHHK6XALnZELn+aks1joNrI1CqiQBOeacPwGFVw1Yh0
04Wqk2kmhXBIgD8SFcd5tB8FLztimQIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAG
GwnpXtlR22ciYaQqPEh346B8pt5zohQDhT37qw4wxYMWM4ETCJ57NE7fQMh017
3PR2VX2bY1QY6fDq81yx2YtCHrnAlU66+tXifPVoYb+O7AWXX1uw16OFNMQkpw
lZPvy5TYnh+dXIVtx6quTx8itc2VrbqnzPmrC3p/
-----END CERTIFICATE-----
```

2 Open an xterm window on the DNCS as **root**.

3 Type the following command and press **Enter:**

```
cd /etc/opt/certs
```

4 Type the following command and press **Enter** to create a backup copy of the existing cacert.pem file:

```
cp cacert.pem  cacert.pem.orig
```

5 Type the following command and then press **Enter** to copy the contents of the root CA certificate to the cacert.pem file:

```
cat [root CA File] >> cacert.pem
```

Note: Replace [root CA File] with the file name of the root CA certificate obtained in step 1.

6 Follow these instructions to stop and restart the web server instances.

a Type the following command and press **Enter** to stop the http process:

```
svcadm -v disable -st http
```

b Type the following command and press **Enter** to refresh the http process:

```
svcadm refresh http
```

c Type the following command and press **Enter** to restart the http process:

```
svcadm -v enable -s http
```

Result: The system displays the **svc:/network/http:apache2 enabled** message.

d Type the following command and press **Enter** to stop the http-dncsws process:

```
svcadm -v disable -st http-dncsws
```

e Type the following command and press **Enter** to refresh the http-dncsws process:

```
svcadm refresh http-dncsws
```

f Type the following command and press **Enter** to restart the http-dncsws process:

```
svcadm -v enable -s http-dncsws
```

Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

7 Follow these instructions to stop and restart the bossServer process.

a Type the following command and press **Enter** to stop the bossServer process:

```
dncsControl -stop bossServer
```

b Type the following command and press **Enter** to start the bossServer process:

```
dncsControl -start bossServer
```

8 Follow these instructions to verify that the http service started properly.

a Type the following command and press **Enter:**

```
ps -ef | grep httpd
```

Result: Output should look similar to the following example:

```
root 21610     1   0 14:10:09 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
dncs 21614 21610   0 14:10:10 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
dncs 21615 21610   0 14:10:10 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
nobody 21594 21589   0 14:09:59 ?   0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-
dncsws/httpd.conf -k start -DSSL
root 21589     1   0 14:09:58 ?     0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-
dncsws/httpd.conf -k start -DSSL
root 27663 19973   0 14:28:06 pts/2 0:00 grep httpd
```

```
nobody 21593 21589   0 14:09:59 ?   0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-
dncsws/httpd.conf -k start -DSSL
```

b Type the following command and press **Enter**.

```
lsof -i :443
```

Result: Output should look similar to the following example, but the Name column will vary, based on your specific configuration:

```
COMMAND PID   USER   FD   TYPE DEVICE        SIZE/OFF NODE
NAME
httpd   21589 root   257u IPv4 0x60019fa8340 0t0      TCP
ossbss:443 (LISTEN)
httpd   21593 nobody 257u IPv4 0x60019fa8340 0t0      TCP
ossbss:443 (LISTEN)
httpd   21594 nobody 257u IPv4 0x60019fa8340 0t0      TCP
ossbss:443 (LISTEN)
httpd   21610 root   259u IPv4 0x60019f6d540 0t0      TCP
localhost:443 (LISTEN)
httpd   21614 dncs   259u IPv4 0x60019f6d540 0t0      TCP
localhost:443 (LISTEN)
httpd   21615 dncs   259u IPv4 0x60019f6d540 0t0      TCP
localhost:443 (LISTEN)
```

9 Log out of the DNCS.

Generating and Deploying Self-Signed Certificates

Important: Cisco recommends that you do **not** generate and deploy self-signed certificates on a production network.

This section provides step-by-step instructions for generating and deploying self-signed certificates. The gen_crt_dncs utility is used to create and deploy a self-signed certificate (server.crt) and private key (server.key) on the DNCS.

Note: The self-signed certificate expiration date will be set to the year 2036.

Generating and Deploying Self-Signed Certificates

Complete the following steps to use the gen_crt_dncs SSL Configuration Utility to create and deploy self-signed certificates.

1 From an xterm window on the DNCS, type the following command and press **Enter:**

```
/etc/apache2/gen_crt_dncs
```

Result: The system displays a message similar to the following:

```
Prepare SSL certificate for HTTPS service. HTTPS will not be
supported on this host without an SSL certificate in place.
Choose from following options:

1. Generate a self-signed SSL certificate and deploy now. You
will need to manually deploy the certificate to those clients
connecting to this server.

2. Generate a certificate signing request for the server
certificate and proceed. No SSL certificate will be deployed,
you will need to sign the generated CSR file externally and
manually deploy it.

3. Import a server certificate for use by openssl and apache.

4. Check dependencies and enable apache SSL.

5. Exit - Skip this step now and manually deploy SSL
certificate later.

Refer to the system User's Guide for instructions.

Please enter your choice: [1|2|3|4|5]
```

2 Select choice **1** and then press **Enter** to create and deploy a self-signed certificate. The command prompts you for the **Distinguished Name** information for the certificate.

3 Use these guidelines to answer the prompt displayed in step 2.

Note: We recommended that you provide valid input for the Distinguished Name information. Use a period (.) to indicate blank input.

- **Country Name —** The country where your company resides. Use the two-letter country code without punctuation for country (for example, US or FR).
- **State or Province —** The state or province where your company resides. Spell out the state completely (for example, California). Do not abbreviate the state or province name.
- **Locality or City —** The city or town where your company resides (for example, Berkeley).
- **Organization Name —** Your company's name (for example, XYZ Corporation). If your company or department name has an **&**, **@**, or any other symbol that requires using the **Shift** key in its name, you must spell out the symbol or omit it.
- **Organizational Unit —** The organization within the company. This field is optional but can be used to help identify certificates registered to an organization. The **Organizational Unit** (OU) field is the name of the department or organization unit making the request. To skip the OU field, press **Enter**.
- **Common Name —** The **Common Name** is the host plus the domain name (for example, **www.company.com** or ***.company.com**). For the DNCS, use the IP address of the interface that will be used for the DNCS Web Services.
- **Email Address —** E-mail address of the certificate requester.

Result: The DNCS creates the server.key, server.crt, cachain.crt, and cacert.pem files in the /etc/opt/certs directory.

4 Type the following command and press **Enter** to set the file permissions to *read-only* for the root user:

```
chmod 400 /etc/opt/certs/server.key
```

5 Type the following command and press **Enter** to ensure that the file is globally readable:

```
chmod 444 /etc/opt/certs/server.crt
```

6 Type the following command and press **Enter** to remove the symbolic link to the cachain.crt file:

```
rm /etc/opt/certs/cacert.pem
```

Note: This file will be recreated later with the appropriate contents and permissions.

Add Trusted Root CA Certificates for the BOSS Web Service

Follow these instructions to copy the billing system's HTTP-S server root CA certificate to the list of trusted certificate authorities.

1 Obtain a copy of the root CA certificate in the CA certificate chain used to sign the billing system's HTTP-S server certificate and place it in the /etc/opt/certs directory of the DNCS. The root CA certificate must be in privacy-enhanced mail format (PEM) format.

Note: The text file must contain the entire root CA certificate starting with **BEGIN CERTIFICATE** and ending with **END CERTIFICATE**.

Example:

```
-----BEGIN CERTIFICATE-----
MIICWjCCAcMCAgGlMA0GCSqGSIb3DQEBBAUAMHUxCzAJBgNVBAYTAlVTMRgwFg
VQQKEw9HVEUgQ29ycG9yYXRpb24xJzAlBgNVBAsTHkdURSBDeWJlclRydXN0IF
bHV0aW9ucywgSW5jLjEjMCEGA1UEAxMaR1RFIEN5YmVyVHJ1c3QgR2xvYmFsIF
b3QwHhcNOTgwODEzMDAyOTAwWhcNMTgwODEzMjM1OTAwWjB1MQswCQYDVQQGEw
UzEYMBYGA1UEChMPR1RFIENvcnBvcmF0aW9uMScwJQYDVQQLEx5HVEUgQ3liZX
cnVzdCBTb2x1dGlvbnMsIEluYy4xIzAhBgNVBAMTGkdURSBDeWJlclRydXN0IE
b2JhbCBSb290MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCVD6C28FCc6H
iM3dFw4usJTQGz0O9pTAipTHBsiQl8i4ZBp6fmw8U+E3KHNgf7KXUwefU/ltWJ
r41tiGeA5u2ylc9yMcqlHHK6XALnZELn+aks1joNrI1CqiQBOeacPwGFVw1Yh0
04Wqk2kmhXBIgD8SFcd5tB8FLztimQIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAG
GwnpXtlR22ciYaQqPEh346B8pt5zohQDhT37qw4wxYMWM4ETCJ57NE7fQMh017
3PR2VX2bY1QY6fDq81yx2YtCHrnAlU66+tXifPVoYb+O7AWXX1uw16OFNMQkpw
lZPvy5TYnh+dXIVtx6quTx8itc2VrbqnzPmrC3p/
   -----END CERTIFICATE-----
```

2 Type the following command and press **Enter** to create the cacert.pem file:

```
cat /etc/opt/certs/[billing server Root CA Crt] >>
/etc/opt/certs/cacert.pem
```

Note: Replace [Billing Server Root CA Crt] with the root CA certificate of the CA chain used to sign the billing system's HTTPS server certificate.

Important: Do not attempt to append the root CA certificate to the cacert.pem file using a text editor.

Configure Client Authentication for the BOSS Web Service

Client authentication is optional for the DNCS BOSS web service. The BOSS web service does not require client authentication by default. When client authentication is required by an HTTP-S Server, the HTTP-S client must provide a valid client certificate.

When client authentication is optional for an HTTP-S Server, the server requests a valid client certificate but the client is not required to return one. If the client does return a certificate, it must be trusted by the server.

Complete the following steps to define client authentication on the DNCS.

1 Is client authentication required for the BOSS web service?

- If **yes**, go to step 2.
- If **no**, complete the following steps to disable client authentication.

a Use a text editor to open the /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf file.

b Change "optional" to "none" in the SSLVerifyClient line.

Example:

```
SSLVerifyClient none
```

c Save and close the file.

d Type the following command and press **Enter** to verify that the file was updated successfully:

```
grep SSLVerifyClient /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf
```

Result: Output should look similar to the following example:

```
SSLVerifyClient none
```

e Is the BOSS web service configured to operate on the same web instance as the web UI?

– If **yes**, complete the following steps to disable client authentication on the single web instance:

i Use a text editor to open the /etc/apache2/user-conf/443.auth.conf file.

ii Change "optional" to "none" in the SSLVerifyClient optional line.

Example:

```
SSLVerifyClient none
```

iii Save and close the file.

– If **no**, go to step f.

f Go to step 17.

2 Complete the following steps to concatenate the DNCS client private key and client certificate into the bossclient.key file.

Note: Unless a separate client certificate is required, the server certificate should be used. If a unique client certificate is required, then temporarily move the server.key and server.crt files to alternate names, repeat steps 1 through 6 of ***Generating and Deploying Self-Signed Certificates*** (on page 117). Complete the following steps a through d. Provide a copy of the new server.crt file to the billing system administrator for use as the trusted root CA certificate for client authentication. Finally, move the original server.key and server.crt files back after the completion of these steps.

a Type the following command and press **Enter:**

```
cd /etc/opt/certs
```

b Type the following command and press **Enter** to create the necessary file for the BOSS client to return a client certificate when requested by the billing server:

```
cat server.key server.crt >> bossclient.key
```

c Type the following command and press **Enter** to set the ownership to the *dncs role* and *dncs group:*

```
chown dncs:dncs bossclient.key
```

d Type the following command and press **Enter** to set the necessary file permissions:

```
chmod 400 bossclient.key
```

3 Use a text editor to open the /etc/apache2/user-conf/SAIdncs.bossreq.auth.conf file.

4 Change "*optional*" to "*require*" in the SSLVerifyClient optional line.

Example:

```
SSLVerifyClient require
```

5 Save and close the file.

6 Type the following command and press **Enter** to verify that the file was updated successfully.

```
grep SSLVerifyClient /etc/apache2/user-
conf/SAIdncs.bossreq.auth.conf
```

Example: Output should look similar to the following example:

```
SSLVerifyClient require
```

7 Open the /export/home/dncs/.profile file with a text editor.

8 Add the following lines to the end of the file to enable the return of a client certificate from the BOSS for billing response messages.

```
# Enable BOSS client certificate return
BOSS_CLIENT_SSL_SETTINGS=7
export BOSS_CLIENT_SSL_SETTINGS
```

9 Save and close the file.

10 Type the following command and press **Enter** to switch to the **dncs** role:

```
su - dncs
```

11 If prompted, type the dncs role password and press **Enter**.

12 Type the following command and press **Enter** to source in the dncs .profile file:

```
. ./.profile
```

13 Type the following command and press **Enter** to stop the BOSS Server process:

```
dncsControl -stop bossServer
```

Note: The system displays **stopped(1)** when the bossServer process is stopped.

14 Type the following command and press **Enter** to restart the BOSS Server process:

```
dncsControl -start bossServer
```

Note: The system displays **running(2)** when the bossServer process has restarted.

15 Type `exit` and press **Enter** to log out of the dncs role.

16 Select one of the following options:

- If the billing system uses Client Authentication and utilizes the same certificate for both the server and the client, then go to the next step.
- If the billing system uses two separate root CAs (one to sign the server certificate and one to sign the client certificate), then follow these instructions.
  - **a** Obtain a copy of the root CA certificate in the CA certificate chain used to sign the billing system's client certificate and place it in the /etc/opt/certs directory of the DNCS.
  - **b** Type the following command and press **Enter** to append the CA certificate to the cacert.pem file:

    ```
    cat /etc/opt/certs/[Billing Client Root CA Crt] >>
    /etc/opt/certs/cacert.pem
    ```

    Note: Replace [Billing Client Root CA Crt] with the root CA certificate of the CA chain used to sign the billing system's HTTPS client certificate. Do not attempt to append the second CA Certificate to the cacert.pem file using a text editor.

17 Follow these instructions to restart the DNCS http process.

- **a** Type the following command and press **Enter** to stop the http process:

  ```
  svcadm -v disable -st http
  ```

- **b** Type the following command and press **Enter** to refresh the http process:

  ```
  svcadm refresh http
  ```

- **c** Type the following command and press **Enter** to restart the http process:

  ```
  svcadm -v enable -s http
  ```

  Result: The system displays the **svc:/network/http:apache2 enabled** message.

18 Follow these instructions to restart the DNCS http-dncsws process.

- **a** Type the following command and press **Enter** to stop the http-dncsws process:

```
svcadm -v disable -st http-dncsws
```

b Type the following command and press **Enter** to refresh the http-dncsws process:

```
svcadm refresh http-dncsws
```

c Type the following command and press **Enter** to restart the http-dncsws process:

```
svcadm -v enable -s http-dncsws
```

Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

Prepare the DNCS Web Instance Trust Store

The cacert.pem file on the DNCS must contain all of the trusted root CA certificates. This file must exist with a minimum of one trusted certificate for the web instances to start. At this point, this file will either contain the trusted root CA certificates for the BOSS Web Service or not exist if the DNCS has only been configured for the STB Staging Web Service.

1 Type the following command and press **Enter:**

```
cat /etc/opt/certs/cacert.pem
```

2 Did the output from step 1 display certificate text?

- If **yes**, continue with step 3.
- If **no** (a **cannot open /etc/opt/certs/cacert.pem** message appears), then the cacert.pem file does not exist. Type the following command and press **Enter** to copy the cachain.crt file to cacert.pem.

  ```
  cp /etc/opt/certs/cachain.crt /etc/opt/certs/cacert.pem
  ```

3 Type the following command and press **Enter** to set the file permissions:

```
chmod 444 /etc/opt/certs/cacert.pem
```

4 Follow these instructions to restart the DNCS http process.

a Type the following command and press **Enter** to stop the http process:

```
svcadm -v disable -st http
```

b Type the following command and press **Enter** to refresh the http process:

```
svcadm refresh http
```

c Type the following command and press **Enter** to restart the http process:

```
svcadm -v enable -s http
```

Result: The system displays the **svc:/network/http:apache2 enabled** message.

5 Follow these instructions to restart the DNCS http-dncsws process.

a Type the following command and press **Enter** to stop the http-dncsws process:

```
svcadm -v disable -st http-dncsws
```

b Type the following command and press **Enter** to refresh the http-dncsws process:

```
svcadm refresh http-dncsws
```

c Type the following command and press **Enter** to restart the http-dncsws process:

```
svcadm -v enable -s http-dncsws
```

Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

Verify the Running Status of the Web Server Instances

Complete the following steps to verify that the web server instances are running properly.

Note: Both web instances are checked even if you configured only one instance to support the web UI and the web services.

1 Type the following command and press **Enter:**

```
ps -ef | grep httpd
```

Example: Output should look similar to the following example:

```
DSSLroot 21610 1     0 14:10:09 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
dncs     21614 21610 0 14:10:10 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
dncs     21615 21610 0 14:10:10 ?     0:00
/usr/apache2/bin/httpd -k start -DSSL
nobody   21594 21589 0 14:09:59 ?     0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-dncsws/httpd.conf
-k start -DSSL
root     21589 1     0 14:09:58 ?     0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-dncsws/httpd.conf
-k start -DSSL
root     27663 19973 0 14:28:06 pts/2 0:00 grep httpd
nobody   21593 21589 0 14:09:59 ?     0:00
/usr/apache2/bin/httpd -f /etc/apache2/httpd-dncsws/httpd.conf
-k start -DSSL
```

2 Type the following command and press **Enter:**

```
lsof -i :443
```

Example: Output should look similar to the following example, but the Name column will vary, based on your specific configuration:

```
COMMAND   PID   USER   FD   TYPE        DEVICE SIZE/OFF NODE
NAME
httpd   21589   root  257u  IPv4 0x60019fa8340      0t0  TCP
ossbss:443 (LISTEN)
httpd   21593 nobody  257u  IPv4 0x60019fa8340      0t0  TCP
ossbss:443 (LISTEN)
httpd   21594 nobody  257u  IPv4 0x60019fa8340      0t0  TCP
ossbss:443 (LISTEN)
httpd   21610   root  259u  IPv4 0x60019f6d540      0t0  TCP
localhost:443 (LISTEN)
httpd   21614   dncs  259u  IPv4 0x60019f6d540      0t0  TCP
localhost:443 (LISTEN)
httpd   21615   dncs  259u  IPv4 0x60019f6d540      0t0  TCP
localhost:443 (LISTEN)
```

3 Did the output in step 1 include "**-DSSL**", AND did the output from step 2 include *listen* entries for the interface used in the ***Define the Web Service Interface for HTTPS Support Only*** (on page 59)?

- If **yes**, go to the next step.
- If **no**, complete the following steps.

a Type the following command and press **Enter** to stop the http process:

```
svcadm -v disable -st http
```

b Type the following command and press **Enter** to refresh the http process:

```
svcadm refresh http
```

c Type the following command and press **Enter** to restart the http process:

```
svcadm -v enable -s http
```

Result: The system displays the **svc:/network/http:apache2 enabled** message.

d Type the following command and press **Enter** to stop the http process:

```
svcadm -v disable -st http-dncsws
```

e Type the following command and press **Enter** to refresh the http-dncsws process:

```
svcadm refresh http-dncsws
```

f Type the following command and press **Enter** to restart the http-dncsws process:

```
svcadm -v enable -s http-dncsws
```

Result: The system displays the **svc:/network/http-dncsws:apache2-dncsws enabled** message.

g Repeat steps 1 through 3.

4 Copy the /etc/opt/certs/server.crt file from the DNCS host to the appropriate location on the billing system and/or STB Staging Client for use as the root CA certificate. The server.crt file is used for the DNCS Web Service root CA certificate because the server certificate is self-signed.

5 After the DNCS is configured, you can verify that the DNCS HTTP-S server certificates are deployed correctly and that the BOSS web service is accessible by completing the following steps.

a Use a web browser to access the following site:

```
https://[ip_address_of_DNCS_host]/dncs/soap/bossreq
```

Result: The web browser should prompt you to accept the certificate but warn that the certificate was issued by a company that you have not chosen to trust, similar to this example:

b Select the appropriate confirmation buttons to allow the web service to continue.

c Is client authorization enabled on this system?

– If **yes**, the web browser will either return a prompt for a client certificate or a connection failure message.

– If **no**, if the computer you are using for the test has an IP address that is allowed to access to the web service, the browser will return a **HTTP GET method not implemented** error message.

d To verify that the billing system HTTP-S server is accessible from the DNCS, use Firefox on the DNCS and enter the following address:

```
https://[ip_address_of_Billing_System_host]
```

6 After the DNCS is configured, you can verify that the DNCS HTTP-S server certificates are deployed correctly and the STB Staging web service is accessible by completing the following steps.

a Use a web browser to access the following site:

`https://[ip_address_of_DNCS_host]/dncs/soap/loadPIMS`

Result: The web browser should prompt you to accept the certificate but warn that the certificate was issued by a company that you have not chosen to trust, similar to this example:

b Select the necessary confirmation buttons to allow the web connection to continue.

c If the STB Staging web service is configured for basic user authentication, a username and password prompt should display. Enter a valid STB Staging username and password.

d If the computer you are using for the test has an IP address that is allowed to access the web service, the browser will return a **HTTP GET method not implemented** error message.

7 If you receive a different error message, review all configuration changes against the previously executed procedures and repeat this procedure.

8

Error Messages

Introduction

This section contains some common error messages and their possible causes. You can use this information to start troubleshooting errors that you may receive.

In This Chapter

Error Messages and Possible Causes

Use the following table to find a possible cause for an error message that you receive.

Error Message	Possible Cause
Authorized Users Only	Occurs when a user tries to sign into a role for which they are not authorized.
Resource control limit has been reached	Occurs when the login session number for a user account has been met (the number of concurrent sessions limit has been met).

9

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

Index

P

R

S

T

U

W

X

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

March 2012 Printed in USA

Part Number 4034689 Rev A