ISDS Security Enhancements Instructions

Overview

Introduction

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

Purpose

This document contains information about security features and enhancements, and instructions on changing your security defaults.

Audience

This document is written for system administrators. Our engineers may also find this document to be useful.

Document Version

This is the fourth release of this document. In addition to minor text and graphic changes from the last draft, the following table provides the technical changes to this document.

Description	See Topic
Removed the forced-change password parameter from several topics	■ ***Creating a User Account*** (on page 8) ■ ***Changing Another User's Password*** (on page 27)
Fixed the login procedures in several topics	■ ***Deleting a User Account*** (on page 9) ■ View the ISDS Database Permissions ■ View the RNCS Database Permissions ■ ***Changing the System Password Expiration Period*** (on page 29) ■ ***Changing a User Password Expiration Period*** (on page 29)
Removed a redundant sentence	***Log Into the ISDS Remotely*** (on page 12)
Fixed an incomplete sentence	***Unsuccessful Login Attempts*** (on page 17)
Added topic for changing timeout parameter for current session	***Changing Timeout Defaults for a Session*** (on page 17)
Fixed parameter syntax in several topics	■ ***SSH and SFTP Connections*** (see "SSH, SFTP, and SCP Connections" on page 19) ■ ***Changing the Login Time Limit for SSH and SFTP*** (on page 23)
Amended section for updated default behavior	***Password Expiration Period*** (on page 27)
Removed several outdated topics	■ Changing Timeout Defaults for a User ■ Forcing a User to Change Passwords on Login

Operating System

Operating System Defaults

- **Operating System:** Solaris 10
- **Security Features:**
  - **Secure by Default** - OS is installed with minimal network services
  - **Networking**
    - SSH is the only network listening service 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 UI access using SSH
  - **Restricted Network Resources** - Authorized users have access to all network resources, but the system itself has very little exposure to the network, making unauthorized access very difficult
  - **System Monitoring** - Basic Security Module (BSM) provides monitoring of system events for logging and auditing

Operating system defaults are set up during system installation.

Important: We recommend that you do not change the operating system defaults to retain the highest level of system security.

Role-Based Access Control

Prior to the implementation of the Security Enhancements on the ISDS, the dncs user account was the only account required to accomplish almost any task associated with the ISDS system. These tasks include access to the ISDS GUI suite, the ISDS database, the ISDS file system, diagnostic scripts, logging, and the command line.

We have implemented role-based access control as part of the ISDS operating system. This access control allows system administrators to assign specific administrative control of parts of the system to users.

You can give users permissions to run certain commands or access to certain files. You can also prevent users from running commands or accessing files. Role-based access control allows increased flexibility in the assignment of permissions on the system.

The following table lists the three most important roles and account types available on the ISDS and a description of their permission levels.

Role and Account Privileges for the ISDS Application

	Files		Commands	Database		
Role	**Read**	**Write**	**Execute**	**Read**	**Write**	**Alter**
Root	Y	Y	Y	Y	Y	Y
DNCS Role	Y	Y	Y	Y	Y	N
DNCS Admin Account	Y	N	N	N	N	N

Roles and Accounts Available on the ISDS and RNCS

This section is a more detailed description of the roles and accounts available on the ISDS and RNCS.

root User

The root user is the system administrator account and has all privileges and rights.

- Login access to the system using the root user is limited to direct local access, such as from the local console.
- You can switch to the root user from another account that is logged in locally or remotely.
- You must use the root user to create all customer-specific login accounts.
- The root user has permission to switch to the dncs role.

- The root user is the database administrator.
- You should perform all RNCS application activities (including starting and stopping the RNCS, RNCS application file management, and RNCS diagnostic script execution) as root user.

Note: You can access the RNCS using as the root user. You must use the siteCmd command to access the RNCS from the ISDS as root user.

dncs Role

The dncs role is the ISDS and RNCS application administrator and user.

- You should perform all ISDS application activities (including starting and stopping the ISDS applications, ISDS GUI access, ISDS application file management, ISDS diagnostic script execution, and ISDS log configuration) using the dncs role.
- You must use the dncs role to start the Administrative Console.
- Access to the dncs role is limited to the root user and DNCS Administrator accounts. These are the only accounts with permission to switch to the dncs role.
- You cannot login directly to the ISDS or RNCS using "dncs" and the dncs role password.

DNCS Administrator

DNCS Administrator accounts are the only system accounts (other than root) that have permission to switch to the dncs role.

- These accounts are created when needed by the ISDS or RNCS system administrator using the create_users script.
- These accounts can be used on the ISDS or RNCS only to view logs and other application files.

DNCS Operator

DNCS Operator accounts can be used on the ISDS or RNCS only to view logs and other application files.

- These accounts are created when needed by the ISDS or RNCS system administrator using the create_users script.
- These accounts do not have permission to switch to the dncs role.

Regular Users

Regular User accounts do not have permission to view ISDS or RNCS logs or other application files.

- These accounts are created when needed by the ISDS or RNCS system administrator using the create_users script.
- These accounts do not have permission to switch to the dncs role.

User Accounts

This section describes how to create and delete user accounts.

User Account Defaults

Regular User

- Can log into the ISDS operating system (Solaris)
- Cannot read or write ISDS files
- Cannot execute ISDS applications
- Cannot switch to the dncs role

Operator

- Can log into the ISDS operating system (Solaris)
- Can read but cannot write ISDS files
- Cannot execute ISDS applications
- Cannot switch to the dncs role

Administrator

- Can log into the ISDS operating system (Solaris)
- Can read but cannot write ISDS files
- Cannot execute ISDS applications
- Can switch to the dncs role

Creating a User Account

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

1. Open an xterm window on the ISDS.
2. Log into the ISDS as root.
3. Type **cd /dvs/dncs/etc** and press **Enter**.
4. Type **create_users** and press **Enter**.
5. Select one of the following user types:
   - Add Regular User
   - Add Operator
   - Add Administrator

   Note: See ***User Account Defaults*** (on page 7) for more information on the user types.
6. Type the name of the new user account and press **Enter**.

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

   Result: The **Do you wish to continue adding this user (Y/N)?** message appears.
7. Type **y** (for yes) and press **Enter**.
8. Type the **password** for the user and press **Enter**.
9. Re-type the **password** for the user and press **Enter**. The create_users program exits.
10. Type **cd /export/home/[username]** and press **Enter**. The user's home directory becomes the active directory.
11. Open the user's **.profile** file in a UNIX text editor.
12. Add the following lines to the .profile file:

    export PATH=$PATH:/usr/ucb

    export PS1='$LOGNAME'@'hostname':'$PWD>'

    set -o vi
13. Save and close the user's .profile file.

Deleting a User Account

Use this procedure to delete users that were added using the create_users script.

1. Log into the ISDS as root.
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**, you are finished with this procedure.

Important: Even when you delete a user, the user name 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.

ISDS and RNCS Database Access

The following permissions are set up by default on the ISDS and RNCS databases:

- root user: DBA, connect, resources
- dncs role: Connect and only insert, delete, select, and update on tables

Who Am I?

To determine who is logged into a session, you can type one of the following from the ISDS command line and press **Enter**:

- **id**
- **/usr/ucb/whoami**

  Note: If you add /usr/ucb to your default path, you only need to type **whoami** and press **Enter**.

The system returns the user ID of the user currently logged into the session.

Log On

Log into the ISDS

This section contains the procedures you need to log into the ISDS at the server terminal. If you need to log into the system remotely using a PC, go to ***Log into the ISDS Remotely*** (on page 12).

Logging into the ISDS

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

1. At the ISDS terminal, type your **user name** and press **Enter**.
2. At the prompt, type your **password** and press **Enter**. A ISDS prompt should appear on the screen.
3. Before you execute any ISDS commands (such as dncsStart or dncsStop), type **su - dncs** and press **Enter**.
4. Before you launch any ISDS user interface windows (such as the Administrative Console), type the following commands:

   export DISPLAY= : 0.0 and press **Enter**

   xhost + and press **Enter**

Restrictions on Multiple Logins

You can only have one active session for SSH, SFTP, or CDE login for any single user name.

Note: This does not apply to the dncs role or to the root user.

This restriction can be changed for a user by modifying the project file entry for that user.

1. Log into the ISDS as root.
2. Type the following command and press **Enter**:

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

   Notes:

   - The **x** in (priv,x,deny) is the number of active sessions the user is allowed to have open at a time.
   - Substitute the user name for **[username]**. Do not type the brackets **[ ]** in the command.

Notes on the Middle Mouse Button

The middle mouse button on the CDE provides a menu of options such as launching the Administrative Console, Starting and Stopping the ISDS, and launching an xterm window.

If you are logged in as a DNCS Administrator, you will be prompted for a password if you select any of the menu options using the middle mouse button; however, the root user does not require a password.

If you are logged in as a DNCS Operator or as a Regular Solaris user, you cannot execute any of the menu options using the middle mouse button.

Do not close any console window that automatically opens if you select any of the following UIs:

- Administrative Console
- DNCS Monitor
- App Serve Monitor

Closing these console windows will cause the UI to also close. After you close the UI, you can close its associated console window.

Log into the ISDS Remotely

Set Up Your xterm Terminal Emulator

To access your ISDS network 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

Configure PuTTY

This section contains the information you need to configure PuTTY for use with the ISDS.

PuTTY Settings

Use the following settings when you configure PuTTY.

Category	Field	Description
Session	Host Name (or IP Address)	IP address of the ISDS.
	Connection Type	Select the **SSH** option.
	Saved Sessions	Enter a host and user name. **Example:** Type **ISDS - Fred Flintstone**.
Connection > Data	Auto-login username	Enter your ISDS user name. **Note:** This is not mandatory, but it prevents you from having to enter your user name each time you log into the ISDS.
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**.
3. In **Host Name (or IP Address)**, type the IP address of the ISDS.
4. Under **Connection Type**, select the **SSH** option.
5. Under **Saved Sessions**, enter a host name and user name.

   Example: Enter **ISDS - FredFlintstone**.
6. In the **Category** list, click **Connection > Data**.
7. In **Auto-login username**, type your ISDS user name.

   Note: This is not mandatory, but it prevents you from having to enter your user name each time you log into the ISDS.
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**.

Configure Exceed

This section contains the information you need to configure Exceed for use with the ISDS.

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 ISDS.

Configure Reflection X

There is no configuration necessary to use Reflection X with the ISDS.

Logging into the ISDS Remotely

This section describes how to use Exceed and a terminal emulation program to login remotely to the ISDS.

1. Make sure you have set up your terminal emulation program correctly on your local PC. See ***Set Up Your xterm Terminal Emulator*** (on page 12) 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 ISDS you want to log into.
5. Click **Load**.
6. Click **Open**. A keyboard authentication screen opens.
7. Did you configure PuTTY with your user name 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 ISDS 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, continue with step 10.

10 Maximize the program you launched in step 2. You should see a prompt in the window.

11 To launch the ISDS Administration Console, type **admincon** and press **Enter**.

Logging Into the ISDS Using an Apple Mac

To login into the ISDS remotely using a Mac using SSH with x11 forwarding, follow these directions.

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

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 Administration Console (admincon), the DNCS Control Panel (dncsControl), and other UI applications.

Session Security Enhancements

Session Timeout Defaults

The ISDS will close a user 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

Notes:

- 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.

Changing the Session Timeout Default for a User

1. Open an xterm window on the ISDS.
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 Timeout Defaults for a Session

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

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

1. Log into the ISDS using the dncs role.
2. Open an xterm window on the ISDS.
3. Type **export TMOUT=0** and press **Enter**.
4. Close the xterm window.

Unsuccessful Login Attempts

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

- 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

1. Open an xterm window on the ISDS.
2. Type **cd /etc/default** and press **Enter**.
3. Open the login file in a UNIX text editor.
4. Locate the following line in the login file:

   #RETRIES=5
5. 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.
6. Save the login file and close the text editor.
7. Type **exit** and press **Enter** to close the xterm window.
8. Log out of the system and log back in to make the changes effective.

Unlocking a User Account

1. Open an xterm window on the ISDS.
2. Log into the ISDS as root.
3. Type one of the following:
   - **If you know the username**, type

     cat /etc/shadow | grep [username] and press **Enter**. The user account opens in the window.
   - **If you do not know the username**, type

     cat /etc/shadow | grep LK and press **Enter**. The list of locked user accounts opens in the window.

   Note: Locked user accounts display with *LK* in front of the user name.

   Examples:
   - **Locked user account:** dncs:*LK*WY6sdlkjWU:14090:::::::::15
   - **Unlocked user account:** dncs:WY6sdlkjWU:14090:::::::::15
4. Find the user account that you need to unlock in the list.
5. Type **passwd -r files -u [username]** and press **Enter**.

   Notes:
   - 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 a User Account Password*** (on page 26).
6. Type **exit** and press **Enter** to close the xterm window.

SSH, SFTP, and SCP Connections

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.

Changing the SSH and SFTP Connection Retries Parameters

1. Change the system session locking default the the number you prefer by following the procedure in ***Changing the Session Lock Number*** (on page 17).
2. In an xterm window on the ISDS 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 ISDS where you are logged in as root, type **svcadm restart ssh** and press **Enter**. The ssh process restarts and uses the new MaxAuthTries parameter.

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 ISDS, 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.

To open a session for SFTP:

1. On a UNIX machine, open an xterm window.
2. Type **sftp [username]@[IP address of the ISDS]** and press **Enter**.
3. Navigate to your target directory by typing cd /[target directory] and pressing Enter.
   - **To transfer a file from the ISDS to your computer,** type **get [target file]** and press **Enter**.
   - **To transfer a file from your computer to the ISDS,** 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:

     2 root root 512 Aug 24 14:49 [target directory]

   - If the directory is owned by the dncs role:

     2 dncs dncs 512 Aug 24 14:49 [target directory]

   - If the file is owned by the root user:

     1 root root 2568 Aug 24 14:49 [target directory]

   - If the file is owned by the dncs role:

1 dncs dncs 2568 Aug 24 14:49 [target directory]

Enable FTP for the EAS

The EAS equipment uses the easftp user to deliver EAS files to the ISDS. We have enhanced the sftp process for the easftp user in the following ways:

- The easftp user is now confined to the directories under **/export/home/secure/easftp**.
- The easftp user is placed in the custom root directory when they login via sftp (/export/home/secure/<username>/).
- To ensure a smooth transition to sftp for the easftp user, the /export/home/easftp/ directory is linked to /export/home/secure/easftp/export/home/easftp.

  Important: EAS equipment vendors must understand that the path **/export/home/easftp** must be specified when putting or getting files using sftp or scp.

To enable FTP for EAS on the ISDS

1. Open an xterm window on the ISDS.
2. Log into the ISDS as root user.
3. Type **inetadm -e svc:/network/ftp:default** and press **Enter**.
4. Open the **/export/home/dncs/.profile** file in a UNIX text editor.
5. Add the following lines to the .profile file:

   # Source the Local EAS Server IP Address

   LOCAL_EAS_IP=<EAS Server IP>; export LOCAL_EAS_IP

   Note: Replace <EAS Server IP> with the IP address of the local EAS server.
6. Save and close the file.
7. Type **usermod -s /bin/sh easftp** and press **Enter**. The default shell changes to /bin/sh (Bourne shell) for the easftp user.
8. Did the system display a message that indicated that the easftp user did not exist?
   - If **yes** (the easftp user does not exist), follow these instructions.
     a. Type **useradd -m -c "EAS FTP Account" -d /export/home/easftp -u 800 -g dncs -s /bin/sh easftp** and press **Enter**.
     b. Type **chmod 775 /export/home/easftp** and press **Enter**.

c Type **passwd easftp** and press **Enter** to set the password.

- If **no** (the easftp user exists), continue with step 10.

9 Type **grep easftp /etc/passwd** and press **Enter**.

10 Confirm that the last item in the output string from step 10 is **/bin/sh**.

SSH Security File

The ISDS is configured for strict RSA key checks, ensuring the highest level of security for the ISDS.

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

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.

Time Limit to Login

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

- 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

1. Open an xterm window on the ISDS.
2. Type **cd /etc/ssh** and press **Enter**.
3. Open the **sshd_config** file in a UNIX text editor.
4. Locate the following line in the login file:

   LoginGraceTime 600
5. 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.
6. Save the sshd_config file and close the text editor.
7. In the xterm window, type **svcadm restart ssh** and press **Enter**. The system restarts the SSH process.
8. Type **exit** and press **Enter** to close the xterm window.

CDE Screen Lock

The ISDS is set up by default to lock the CDS screen after 30 minutes of inactivity. You can modify the inactivity lock time by following this procedure.

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**.

Kill a Session

There might be times when a user closes a 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.

Killing a Session

1 Open an xterm window on the ISDS.

2 Log into the ISDS as root.

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 | 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**.

Password Management

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

Password Guidelines

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

- Contain 8 or more characters
- Contain at least 2 alphanumeric characters and at least one numeric or special character
- Do **not** consist of only one character type (**aaaaaaa** or **11111111**)
- Do **not** contain any aspects of a date
- Are **not** proper names
- Are **not** telephone numbers or similar numeric groups
- Are **not** user IDs, user names, group IDs, 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**)

System Password Retention

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 a User Account Password

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 ISDS. Our recommendations for other account passwords are as follows:

- **informix account:** Changing the informix account password is not necessary since this account is locked by default.
- **dncsSSH account:** Changing the dncsSSH account password is not necessary since this user is not directly used by an operator, and the default password is either not known or documented.
- **easftp and dncdftp accounts:** These account passwords should be done only in coordination with the administrator of the EAS and the VOD systems.
- **pcgrequest** and **pcgscp accounts**: Changing these account passwords is not absolutely necessary since these accounts are not used directly by an operator and do not support normal login shells.

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

Changing Your Own Password

Note: Users can change their own account password. Only administrators can change other users' account passwords.

1. Open an xterm window on the ISDS.
2. At the login prompt, 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 ISDS.
8. Login to the ISDS with your new password.

Changing Another User's Password

Note: Users can change their own account password. Only administrators can change other users' account passwords.

1. Open an xterm window on the ISDS.
2. Log into the ISDS as root.
3. Type **passwd -r files [username]** and press **Enter**.

   Example: Type **passwd -r files jonesx** and press **Enter**.
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 ISDS.
8. Have the user login to the ISDS with the new password. If you used the **-f** option, the user must enter the one-time password you created. Then, the system prompts the user to create a new password.

Changing the Root Password

Note: Users can change their own account password. Only administrators can change other users' account passwords.

1. Open an xterm window on the ISDS.
2. Log into the ISDS as root.
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

By default, the system requires that user accounts change their passwords after 13 weeks. The system also displays a warning 2 weeks before the deadline. After that time, if the user has not changed their account password, the user account is locked. We recommend that, at a minimum, you change the default password for root and the dncs role to increase the level of security on the ISDS.

You should not change the informix and dncsSSH passwords as these accounts are locked by default. Additionally, changing the pcgrequest and pcgscp user passwords is not absolutely necessary because these accounts are not used directly by an operator and do not support normal login shells. Changing the easftp and dncsftp passwords should be done only in coordination with the administrator of the EAS and the ISDS, respectively.

The root, dncsftp, easftp, and any custom accounts, as well as the dncs role, all have the password expiration period set by default. You can modify or remove the expiration period if you do not want to manage password expiration on the ISDS. The informix, dncsSSH, pcgrequest, and pcgscp users have the password expiration period disabled, by default.

WARNING:

The ISDS (or components within the ISDS) will become unstable if any of the default user passwords expire (root, dncs, dncsSSH, Informix, dncsftp, or easftp). The ISDS system administrator MUST ensure that these passwords do NOT expire. It is imperative that you disable the password expiration period UNLESS the ISDS system administrator can ensure that the passwords for these accounts do not expire.

- Default number of weeks a password is valid: 13
- Default time period from password expiration the user receives a warning message to change passwords: 2
- Recovery: Administrator must reset the user account by changing the password

You can change or disable the password expiration period applied when adding new users or changing passwords, and change or disable an individual user's password expiration period.

Change the Password Expiration Period

You can change the password expiration period applied when creating new users or changing passwords.

Important:

- New users added to the ISDS after the password expiration period has changed automatically inherit the new password expiration period.
- Existing users' individual expiration periods remain in force until the the user's password is changed (either by an administrator or by the user).
- Unless the system password expiration period is disabled, all user accounts will inherit the system password expiration period each time they change their passwords, even if the user's expiration period has been disabled.
- If you set the value of MAXWEEKS to -1, you disable password expiration.

Changing the System Password Expiration Period

Use this procedure to change the password expiration period for the entire system.

> **WARNING:**
>
> **The ISDS (or components within the ISDS) will become unstable if any of the default user passwords expire (root, dncs, dncsSSH, Informix, dncsftp, or easftp). The ISDS system administrator MUST ensure that these passwords do NOT expire. It is imperative that you disable the password expiration period UNLESS the ISDS system administrator can ensure that the passwords for these accounts do not expire.**

1. Open an xterm window on the ISDS.
2. Log into the ISDS as root.
3. Type **cd /etc/default** and press **Enter**.
4. Open the **passwd** file in a UNIX text editor.
5. Locate the following line in the passwd file:

   export MAXWEEKS=13
6. Change the expiration period to the number of weeks that you prefer.

   Note: We recommend that you keep the expiration period as short as possible. This helps prevent unauthorized use of your system.
7. Locate the following line in the passwd file:

   export WARNWEEKS=2
8. Change the warning period to the number of weeks that you prefer.
9. Save the passwd file and close the text editor.
10. Type **exit** and press **Enter** to close the xterm window.

Changing a User Password Expiration Period

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

> **WARNING:**
>
> **The ISDS (or components within the ISDS) will become unstable if any of the default user passwords expire (root, dncs, dncsSSH, Informix, dncsftp, or easftp). The ISDS system administrator MUST ensure that these passwords do NOT expire. It is imperative that you disable the password expiration period UNLESS the ISDS system administrator can ensure that the passwords for these accounts do not expire.**

1. Open an xterm window on the ISDS.
2. Log into the ISDS as root.
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.

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

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

```
dncs      PS         09/02/09              91      14
user      pw_status  date        MIN       MAX     WARN
```

- The **date** (09/02/08) is the date the password was set by the user (dncs).
- The **MIN** (blank) 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** (91) 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.

Disable the Password Expiration Period

You can disable the password expiration period that is applied when creating new users or when changing passwords or for an individual user.

Important:

- New users added to the ISDS after the password expiration period has changed automatically inherit the new password expiration period.
- Existing users' individual expiration periods remain in force until the the user's password is changed (either by an administrator or by the user).
- Unless the system password expiration period is disabled, all user accounts will inherit the system password expiration period each time they change their passwords, even if the user's expiration period has been disabled.
- If you set the value of MAXWEEKS to -1, you disable password expiration.

Disabling the System Password Expiration Period

Use this procedure to disable the password expiration period for the entire system.

1 Open an xterm window on the ISDS.

2 Log into the ISDS as root.

3 Type **cd /etc/default** and press **Enter**.

4 Open the **passwd** file in a UNIX text editor.

5 Locate the following line in the passwd file:

export MAXWEEKS=13

6 Change the expiration period to **–1** (negative one).

7 Locate the following line in the passwd file:

export WARNWEEKS=2

8 Change the warning period to **–1** (negative one).

9 Save the passwd file and close the text editor.

10 In the xterm window, type **source . ./passwd** and press **Enter**. The system will use the updated passwd file.

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

Important: Existing users' individual expiration periods remain in force until the the user's password is changed (either by an administrator or by the user).

Disabling a User Password Expiration Period

Use this procedure to change the password expiration period for an individual user account. We recommend that you follow this procedure for the following user accounts at a minimum:

- root
- dncs
- informix
- dncsSSH
- dncsftp
- easftp
- pcgrequest
- pcgscp

1 Open an xterm window on the ISDS.

2 Log into the ISDS as root.

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: Type **passwd –r files –s dncs** and press **Enter**. The system displays a message similar to the following:

```
dncs        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 4.

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

Important: Unless the system password expiration period is disabled, all user accounts will inherit the system password expiration period each time they change their passwords, even if the user's expiration period has been disabled.

Security Event Logs and System Auditing

The ISDS automatically captures some security event logs and includes tools to audit system security events.

Security Event Logs

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

- SSH
- SFTP
- su login attempts

Login events (su login events) are also captured in the **/var/adm/sulog**.

System Auditing

You can audit system security on the ISDS using BSM.

Using BSM

The BSM utility is installed on the ISDS and logs a significant amount of event information, including 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 ISDS as root.
2. To determine the name and location of the current BSM log file, type **cat /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 **[path and name of file] | praudit** and press **Enter.**
4. To monitor the audit data in real time type **tail -0f [path and name of file] | praudit** and press **Enter**. This results in a significant amount of information.
5. 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]** — Displaysinformation 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 only a 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 only a particular user.
- **[files]** — Specify the BSM binary file(s) to search.

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

For 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.

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

August 2012 Printed in USA Part Number 4027701 Rev B