



Troubleshooting Cisco ICS 7750 Software

This chapter explains how to identify and to solve problems with the Cisco Integrated Communications Systems (ICS) 7750 software, including ICS System Manager and Cisco CallManager. This chapter includes the following sections:

- [Troubleshooting ICS System Manager, page 5-2](#)
- [Troubleshooting Cisco CallManager, page 5-11](#)
- [Password Recovery, page 5-19](#)



Note

See [Chapter 9, “Solving Voice Problems”](#) for information about problems related to IP Phones, trunks, lines, and voice interface cards (VICs), including information on digital signal processors (DSPs) and packet voice/data modules (PVDMs).



Note

For a description of the features, modifications, and caveats for the Cisco Integrated Communications System 7750 (Cisco ICS 7750) release 2.6.0, refer to the [Release Notes for System Software Release 2.6.0 on the Cisco ICS 7750](#).

Troubleshooting ICS System Manager

The following sections describe how to resolve problems with ICS System Manager:

- [Initial Configuration Problems, page 5-2](#)
- [ICS System Manager Error Codes, page 5-3](#)
- [ICS System Manager Log Files, page 5-4](#)
- [Changing the Host Name of the SPE Running System Manager, page 5-6](#)
- [Launching Visual Switch Manager from SSP Manager, page 5-8](#)
- [Conflicting Credentials When Upgrading ICS System Software, page 5-8](#)
- [ICSConfig Error After Upgrading Cisco CallManager to 3.1\(4a\), page 5-9](#)
- [Error Installing Cisco CallManager 3.3 Subscriber, page 5-11](#)

Initial Configuration Problems

If you use ICSConfig to change the IP address of an analog station interface (ASI) or multiservice route processor (MRP) card that has analog—Foreign Exchange Station (FXS), Foreign Exchange Office (FXO), or ear and mouth (E&M)—ports, you might not be able to place a public switched telephone network (PSTN)-to-IP call or an IP-to-PSTN call over that port. PSTN-to-PSTN and IP-to-IP calls, however, will continue to be placed normally.

To resolve this problem, complete the following steps:

-
- Step 1** Access Cisco CallManager.
 - Step 2** Choose **Device > Gateway**.
The Find and List Gateway screen appears.
 - Step 3** Enter search criteria to locate the gateway (ASI or MRP).
A list of discovered devices appears.
 - Step 4** Click the **Reset** button next to the gateway that you want to reset.
The Reset Device window appears.

Step 5 Click **Restart Device**.



Note

During system discovery, you may see specific error codes if ICSSConfig encounters an error condition; for example, “error code 100—cannot discover SSP.” When such an error occurs, ICSSConfig displays a page that contains a description of the specific error with links to the help pages that provide instructions for correcting the problem. If an error occurs while ICSSConfig is running, click the link(s) on the error code page for instructions on resolving the error condition and then proceed with ICSSConfig.

ICS System Manager Error Codes

Table 5-1 lists some of the error codes that might be displayed through System Manager when an internal error condition is found by any of the ICS System Manager software modules.

Table 5-1 ICS System Manager Error Codes

Error Code	Description
2	Login password was not correct; could not execute any commands on system card
3	Enable password not correct; could not execute any commands on the system card
9	File may not be available in TFTP directory on SPE
13	FTP copy failed
15	Timed out while reading file to deliver to system card
19	System card unreachable; host name truncated; could not establish connection
101	Config file generation failed for system card
102	Config file cannot be parsed by the ICSSM
103	Internal error; could not continue the process
104	Failed to add device record to the inventory database

Table 5-1 ICS System Manager Error Codes (continued)

Error Code	Description
105	Failed to delete device record to the inventory database
106	Failed to update device record from the inventory database
107	ICS System Manager could not create system registry key
108	ICS System Manager could not open system registry key
109	Command cannot be accepted by system card
-65435 to -65429	ICS System Manager failed to set address on the system card; slot number is incremented from -65435 to -65429
-65335 to -65329	ICS System Manager failed to process the copy run start command on the system card; slot number is incremented from -65435 to -65429

ICS System Manager Log Files

The log files used by ICS System Manager are listed below, along with the location of each log file on the system processing engine (SPE) hard disk. You can use these log files to help isolate and resolve ICS System Manager problems.

- ICS System Manager module logs under C:\Program Files\Cisco Systems\ics\Program:
 - Multi.log
 - Back.log
 - BBTrace.log
 - BBTrace.bak
- FMM traces under C:\Program Files\Cisco Systems\ics\Program\FMM\Trace
- Replication and SNMP logs under C:\W2KS\System32:
 - repl.log
 - snmpdbg.log
- SQL Server 2000 directory files under C:\Program Files\Microsoft SQL Server\MSSQL\$ICSSM

- Directory for client tools under
C:\Program Files\Microsoft SQL Server\80\Tools\Bin
- Installation log files and/or folders that are created during every ICS System Software installation or upgrade. These logs appear under the C drive root directory with the naming convention of ICSINSTALL-date-time, such as
ICSINSTALL-04-26-2002-16-21-19

where the ICSINSTALL-date-time folder contains the following log files:

- ICSINSTALL.LOG—running log for the installation program
- Summary.html—summary of the installation in html
- Summary.log—summary of the installation

Under the ICSINSTALL-date-time folder, the following log files and/or folders may also be created, depending on the action taken:

- Log files and/or folders that are created when ICS System Manager software is installed on the SPE:
 - ICS System Manager_LOCAL.log
 - Windows 2000 Updates_LOCAL.log
- Upgrade log files and/or folders that are created when the SPE running System Manager is upgraded to a later version of software:
 - ICS System Manager Upgrade_LOCAL.log
 - Windows 2000 Updates_LOCAL.log
- Upgrade log files and/or folders that are created when the SPE running System Manager is upgraded to a later version of software:
 - ICS System Manager Upgrade_LOCAL.log
 - Windows 2000 Updates_LOCAL.log
- Upgrade log files and/or folders that are created when the SPE running ICS Core Software is upgraded to a later version of software:
 - ICS Core Software Upgrade_XXXXXXX-SPE.log
 - Windows 2000 Updates_XXXXXXX-SPE.logwhere XXXXXXX is the host name of the SPE
- Backup log files and/or folders that are created during system backup:
 - ICSBackup_ByICSSetup_ICsver-2.x.x.bkf

- ICSConfigData.xml—created by ICS System Software version 2.4.0 and later
- Uninstallation log files and/or folders that are created when ICS System Software is uninstalled; these files and/or folders appear under the C drive root directory with the naming convention of “SMUninstall date time.”

For example:

```
SMUninstall 5-1-2002 12.19
```

where the SMUninstall date time folder contains the following log files:

- DropTable.sql.log
- ICSSMUninstall.log
- CallManager database migration-related
 - C:\CCMDBSetup.log
 - C:\DBConvert.txt
- CNR logs under C:\Program Files\Network Registrar\logs
- System maintenance module logs in
 - C:\Program Files\Cisco Systems\ics\SysMaint\SysMaint.log
 - C:\Program Files\Cisco Systems\ics\fmm\backup.log
 - C:\Program Files\Cisco systems\ics\fmm\restore.log



Note

See the [“Using Log Files for Troubleshooting” section on page 2-8](#) for additional information on logs used for troubleshooting.

Changing the Host Name of the SPE Running System Manager

The computer name (also known as the *host name*) of an SPE running System Manager can be safely changed only if no applications have been installed on the SPE since it left the factory. For example, if you install Cisco CallManager on the SPE running System Manager, you cannot change the host name of that SPE unless you reimaged the SPE and reinstall the software.

Beginning with ICS System Software release 2.6.0, Microsoft SQL Server 2000 is installed on the SPE as part of the system software and later as part of the Cisco CallManager 3.3 installation. The ICS System Manager installation program installs a named instance, *ICSSM*, of SQL Server 2000 on an SPE running System Manager. The names of the SQL Server 2000 named instance services are *MSSQL\$ICSSM* and *SQLAgent\$ICSSM*.

Because Microsoft SQL Server 2000 is less restrictive with host name changes, you can change the host name on a new, factory-configured SPE running System Manager by following the steps outlined in the “Changing the Host Name of the SPE310 Running System Manager” section in Chapter 5, “Operating the Cisco ICS 7750,” in the *Cisco ICS 7750 Installation and Configuration Guide*, or in the “Setting the Host Name on the Replacement SPE” section in the *Cisco ICS 7750 FRU Installation and Replacement* document.

If you have installed additional applications on the SPE (such as Cisco CallManager 3.3 or Cisco Unity Voice Messaging), changing the host name might not be allowed if those applications restrict it. Refer to the documentation that came with your software for information about limitations and restrictions that might apply.

Guidelines for Host Names

The following principles govern the use of host names on SPEs and other devices on the same network as the Cisco ICS 7750:

- Access privileges—You must be logged on as an administrator on the SPE in order to change the SPE host name.
- Naming conventions:
 - The host name must be unique to your network.
 - The host name must not be longer than 15 characters.
 - Host names should contain only the numbers 0 through 9, the letters A through Z and a through z, and hyphens (-). You can use other characters, but using them might prevent other users from finding your device on the network.
 - Host names cannot have a space anywhere in the host name, including leading or trailing spaces. The following characters and symbols are not valid entries in host names: \ " / [] : | < > + = ; , ? .

Launching Visual Switch Manager from SSP Manager

You may encounter a problem launching Visual Switch Manager from SSP Manager in System Manager, if you do not have the required Java plug-in installed on your client PC or workstation.

**Note**

Visual Switch Manager has been renamed as Cisco Cluster Management Suite.

In attempting to launch Visual Switch Manager from the SSP Manager page, the browser may first display an initial page for the Visual Switch Manager and then go blank as the browser tries to load a Java applet. This problem affects both Internet Explorer and Netscape Navigator browsers.

To resolve this problem, install the Java plug-in version 1.3.1 on your client PC or workstation that is being used to launch the browser. The Java plug-in can be downloaded from the [Cisco Software Download](http://www.cisco.com/pcgi-bin/tablebuild.pl/java) page at <http://www.cisco.com/pcgi-bin/tablebuild.pl/java>.

Conflicting Credentials When Upgrading ICS System Software

When running the ICS System Software Setup program on the SPE running System Manager, and at least one of the SPEs (running ICS Core Software) is selected for upgrade, you might encounter a problem in which the upgrade fails on the core software SPE. With this problem, the following error message might appear during the upgrade process:

```
ICS7700-AIFK2M1 / Slot 5 Installation Failed
```

```
System Error: Configuring SNMP Service: Unable to map a network drive to the remote SPE because the credentials being used conflict with an existing set of credentials. Please disconnect all existing connections such as mapped drives and explore sessions from the current SPE to the remote SPE and restart the current SPE before retrying the installation.
```

```
Configuring SNMP Service: Installation Failed
```

This problem occurs when there is an existing authenticated connection between the two SPEs in the chassis. The Windows operating system allows for only one user-authenticated connection between two Windows systems. Multiple

connections between two SPEs are permitted, but only when they are using the same credentials. If an existing connection between the SPE running System Manager and the core software SPE has a credential other than that used by the ICS System Software Setup program, then you will encounter this problem.

To resolve the problem, check to make sure that there are no existing connections between the two SPEs, that you did not explicitly create a connection (by mapping a drive) between the two SPEs, or that an application that is running on your system did not create a connection in the background (such as connection to IPC\$).

To check that there are no existing connections between the two SPEs, at the command prompt of the SPE running System Manager (where the installation program is executed) enter the following command:

```
C:\>net use
```

If there are any existing connections, they will be listed. Remove the existing connections by entering the following command:

```
C:\>net use /delete\\IP_address\c$
```

where *IP_address* is the IP address of the existing connection that you need to remove.

In addition, you should close any existing Windows Explorer sessions that might be open between the two SPEs. You can take these actions before you start the Setup program.

If the problem is still not resolved, then reboot the SPE running System Manager to remove any existing connections.

ICSConfig Error After Upgrading Cisco CallManager to 3.1(4a)

When running ICS System Software release 2.1.0 through 2.5.0, you might encounter a problem proceeding with ICSConfig after upgrading to Cisco CallManager version 3.1(4a). When this problem occurs, ICSConfig reports error code 100—Cannot discover SSP.

If you encounter this problem, you need to install an executable patch file—UpdateICSBeforeCMInstall.exe—on the SPE310.

(UpdateICSBeforeCMInstall.exe contains two batch files, ICSBeforeInstall.bat and ICSAfterInstall.bat). You can download this patch file from CCO. See the [“Downloading ICS System Software” section on page 4-10](#) for information about downloading software from CCO.

Follow these steps to apply the UpdateICSBeforeCMInstall.exe patch on the SPE and to recover your system:

-
- Step 1** From CCO, download the UpdateICSBeforeInstall.exe file to the root directory (C:\) of the SPE running System Manager.
- Step 2** On the SPE, navigate to C:\UpdateICSBeforeInstall.exe, and double-click the file to execute it.
- Two batch files appear on the display—ICSBeforeInstall.bat and ICSAfterInstall.bat.
- Step 3** Open up a command line prompt (**Start > Run > cmd**) on the SPE to access the root (C:\) directory.
- Step 4** At the command line prompt, enter **ICSBeforeInstall.bat**:
- ```
c:\ICSBeforeInstall.bat
```
- Press **Enter**.
- Step 5** Return to the command line prompt, and enter **ICSAfterInstall.bat**:
- ```
c:\ICSAfterInstall.bat
```
- Press **Enter**.
- Step 6** Close the command line prompt by typing exit:
- ```
c:\exit
```
- 



**Note**

If you reimage an SPE310 that is running ICS System Software release 2.1.0 through 2.5.0, you will need to reapply this patch. You can apply this patch before upgrading to Cisco CallManager 3.1(4a), in which case you should not encounter the problem with ICSCfg. You do not need to apply this patch if you are running ICS System Software release 2.6.0.

---

## Error Installing Cisco CallManager 3.3 Subscriber

When installing Cisco CallManager subscriber on an SPE, the installation might fail with error code 5—Access is denied.

When you log in to an SPE that is running the Windows 2000 operating system, a security context is created with the user and the user's password. This security context is used for all network calls. If the password is changed, the security context is not updated unless you log off and then log in to the SPE. (Any network calls made before you log off the SPE will continue to use the old security context.)

You might encounter this error if the Cisco CallManager subscriber cannot connect to the Cisco CallManager publisher because the passwords configured on the subscriber and the publisher are not the same.

To resolve this problem, take the following actions:

- Before you install the Cisco CallManager subscriber, make sure that the Windows 2000 administrator password that you configure on the SPE running the Cisco CallManager subscriber is the same as the password that you configured on the SPE running the Cisco CallManager publisher.
- Using ICSCConfig to change the Windows 2000 administrator password on the SPE, make sure that you log off the SPE and then log in again to successfully complete the installation of the Cisco CallManager subscriber. To log off the SPE, choose **Start > Shut Down > Log Off Administrator**. To log in, press **Ctrl-Alt-Del** and enter the administrator password.

## Troubleshooting Cisco CallManager

Use [Table 5-2](#) to find the likely cause of some of the problems associated with Cisco CallManager. The problems are described in detail in the sections that follow.

**Table 5-2 Cisco CallManager Problems and Possible Causes**

| Problem                                                                                                    | Possible Cause                                                                              |
|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Attempting to view a Cisco CallManager web page results in an error.                                       | See the <a href="#">“Access Denied”</a> section on page 5-12.                               |
| Attempting to view Cisco CallManager 3.1 CCMUser or CCMAAdmin web pages with Netscape results in an error. | See the <a href="#">“Browser Access Limitations”</a> section on page 5-12.                  |
| Calls cannot be placed, or other voice applications close unexpectedly.                                    | See the <a href="#">“Cisco CallManager Shutdown”</a> section on page 5-13.                  |
| Cisco CallManager services are disabled after Cisco CallManager 3.3 is installed.                          | See the <a href="#">“Cisco CallManager 3.3 Services Are Disabled”</a> section on page 5-13. |

## Access Denied

When attempting to access Cisco CallManager, you may see the following message:

```
Unable to start a DCOM Server... Access is Denied...
```

This message means that the system does not have read permission on the Cisco CallManager directory or that there is a Cisco CallManager database error. Contact technical support to resolve this problem.

## Browser Access Limitations

When Cisco CallManager 3.1 is accessed with Netscape 6.1, the CCMUser web pages will not be displayed, and you will see an error message indicating the following:

```
Failed to create ASP object for: _RemoteScripts/rs_logon.asp
```

This message results from the use of an unsupported browser. The workaround is to use Netscape 4.7 or Internet Explorer 5.5 or later. This problem is scheduled to be resolved in Cisco CallManager 3.2.

You may also encounter problems in attempting to use Netscape 6.1 to access the Cisco CallManager 3.1 CCMAAdmin web pages. In this situation, the CCMAAdmin web pages will appear, but the top menu will not be functional, and the CCMAAdmin pages will be inaccessible. The workaround is to use Netscape 4.7 or Internet Explorer 5.5 or later.

**Note**

---

Web browser support requires Netscape Communicator 4.7 or later, or Internet Explorer 5.5 or later, with Java plug-in version 1.3.1 or later (refer to the [Cisco Software Download](http://www.cisco.com/pcgi-bin/tablebuild.pl/java) page at <http://www.cisco.com/pcgi-bin/tablebuild.pl/java>).

---

## Cisco CallManager Shutdown

After a Cisco CallManager shutdown or restart, any calls that are being placed through Cisco CallManager are disconnected.

Determine whether the Cisco CallManager outage is planned (scheduled by an administrator) or unplanned:

- **Planned**—Coordinate with the administrator to ensure that an orderly Cisco CallManager shutdown takes place by first verifying that there are no active caller sessions and by shutting down plug-ins and other applications associated with Cisco CallManager, in accordance with the instructions in the Cisco CallManager documentation.
- **Unplanned**—Verify that there are no environmental or power problems affecting the Cisco ICS 7750 (see [Chapter 2, “System Troubleshooting Guidelines”](#)) and that the SPE on which Cisco CallManager is installed is functioning properly (see [Chapter 3, “Solving Hardware Problems”](#)).

## Cisco CallManager 3.3 Services Are Disabled

After you install ICS System Software 2.6.0 and Cisco CallManager 3.3, the Cisco CallManager services might be in a disabled state. To activate the Cisco CallManager services, you must explicitly enable them.

Follow these steps to activate the Cisco CallManager services on the target SPE:

- 
- Step 1** Access the SPE310 Windows user interface, and connect your peripherals as described in the “[Accessing the SPE310 Windows Interface Through Directly Connected Peripherals](#)” section on page 4-4.
- Step 2** Log in as an administrator (user ID *administrator*), and enter the default password (*changeme*).
- Step 3** On the target SPE running the Cisco CallManager 3.3 Publisher, use Windows Explorer to access the Cisco CallManager administration services by entering the IP address of the Cisco CallManager.
- For example:
- ```
http://IP_Address\CCMAdmin
```
- where *IP_Address* is the IP address of the Cisco CallManager 3.3 Publisher.
- Step 4** On the Cisco CallManager administration page menu, choose **Application > Cisco CallManager Serviceability**.
- Step 5** Choose **Tools > Service Activation**.
- Step 6** Select the Cisco CallManager server and enable the required services.
-

Cisco CallManager Traces

Traces are a valuable tool used for monitoring system performance and troubleshooting problems. Made up of user mask flags (bits) and trace levels, traces can add a load to the Cisco ICS 7750 SPE processor that may degrade call-processing performance.

Therefore, it is important to consider both the amount of trace information needed and the load on the system before you decide to turn on traces. It is equally important to ensure that trace parameters are configured properly so as not to generate large amounts of information, which can hinder problem isolation and resolution.

Because of the above considerations, tracing is turned off by default on Cisco CallManager.

Setting Up Cisco CallManager Traces for the Cisco TAC

To set up CallManager Traces, perform these steps:

-
- Step 1** In Cisco CallManager, choose **Service > Trace**.
 - Step 2** Click **CallManager Name** or **IP Address**.
 - Step 3** Click **Cisco CallManager**.
 - Step 4** If you have not visited the page before, click the **SetDefault** button, which will populate most of the fields automatically and make any needed minor adjustments.
 - Step 5** Click **Update** to save these values.

These values are used for all the services. Most of the details are specific to the Cisco CallManager Service, but the other services can be examined as well.
 - Step 6** Note where the files are being logged. For Cisco CallManager, trace files are logged in the C:\Program Files\Cisco\Trace\CCM\ directory.
 - Step 7** Collect the correct trace files by navigating in Windows Explorer to the CCM directory (C:\Program Files\Cisco\Trace\CCM\), and then selecting **View > Details** from the menu bar to view dates and times.

Files will be overwritten after a period of time, so the only way to know which file is being logged to is to click **View > Refresh** on the menu bar and look at the dates and times on the files.

**Note**

If you are reproducing a problem, make sure to select the file for the timeframe when you reproduced it. The best way to collect accurate trace files is to reproduce a problem and then quickly locate the most recent file and copy it from Cisco CallManager.

SDL Traces

SDL traces are useful in finding the cause of a particular error (such as dropped calls) by displaying a series of events that have occurred. Once enabled, SDL trace files can be saved to local directories, the Windows NT Event Viewer, and CiscoWorks2000. To avoid system performance degradation, SDL tracing should be turned off after the trace data has been captured.

To enable SDL traces, perform the following steps:

-
- Step 1** In Cisco CallManager, choose **Service > Service Parameters**.
 - Step 2** Click **CallManager Name** or **IP Address**.
 - Step 3** In the Param field, select **SdlTraceFlag**.
 - Step 4** In the Value field, select **T**.

The following parameters should be configured with the recommended settings:

- SdlTraceFlag—To turn SDL traces on and off.
 - To turn SDL traces on—set to T.
 - SdlTraceMaxLines—Maximum number of lines in each file before starting the next file. Can be any numeric value.
 - Set to 200 as a starting point.
 - SdlTraceTotalNumFiles—Maximum number of files before restarting file count and overwriting old files.
 - Set to 10 as a starting point.
 - SdlTraceTypeFlags—Values determine the type of debugging (layer 1,2,3, TCP, interface, gateway, etc.).
 - Change the default value (0x00004B05) to 0x00004B15 to see the errors logged.
-

Once the SDL traces are enabled and collected, they can be retrieved from the SPE in the C:\program files\cisco\trace\sdl subdirectory.

Sniffer Trace

A sniffer trace may be used in conjunction with an SDL trace. A sniffer is a software application that monitors IP traffic on a network and provides information about the quantity and type of network traffic, in the form of a trace. Sniffer traces can also help to identify high levels of broadcast traffic that could result in voice audio problems or dropped calls.

Common sniffer applications include Network Associates SnifferPro, and W&G Domino (sniffing hardware/software, and a network analyzer). With Domino, the recommendation is to use the analysis software to evaluate a captured sniffer file (such as from the SnifferPro application). Any sniffer application will work with Cisco CallManager.

Refer to the following websites for additional information on sniffer trace applications:

- [Network Associates SnifferPro](http://www.sniffer.com/), which is available at <http://www.sniffer.com/>
- [W&G Domino Analyzer](http://www.acterna.com/products/index.html), which is available at <http://www.acterna.com/products/index.html>



Note

For detailed information about traces and about other monitoring tools and utilities in Cisco CallManager, refer to the “Troubleshooting Tools” section of the *Cisco CallManager Troubleshooting Guide*, available at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_3/trouble/index.htm.

Troubleshooting Tips for Cisco CallManager

The following tips may be helpful in troubleshooting problems with Cisco CallManager:

- Know where your devices are registered.

Each Cisco CallManager log traces files locally. If a Cisco IP Phone or gateway is registered to a particular CallManager, then the call processing is done on that CallManager if the call is initiated there. You will need to capture traces on that CallManager to debug a problem.

A common mistake is to have devices registered on a Subscriber, while capturing traces on the Publisher. These trace files will be nearly empty (and most definitely will not have the trace information you need in them).

Another common problem is having Device 1 registered to “CM1” and Device 2 registered to “CM2.” If Device 1 calls Device 2, the call trace is in CM1; if Device 2 calls Device 1, the trace is in CM2. If you are troubleshooting a two-way calling issue, you need traces from both CallManagers in order to collect all the information needed.

- Include DNs (phone numbers) or IP addresses (if gateways) for all devices in the path of the problem. Also, collect software package version information for the associated ASIs or MRPs, including any available configurations.

This will enable the TAC engineer to quickly locate the phones and other devices involved in the problem call(s).

- Know the approximate time of the problem in the traces.

Multiple calls may have been made; therefore, knowing the approximate time of the call can help TAC isolate the problem more quickly and efficiently.

Additional resources that are available to help you troubleshoot Cisco CallManager include the following:

- *Cisco CallManager Troubleshooting Guide*
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_3/trouble/index.htm
- *AVVID (Architecture for Voice, Video, and Integrated Data)*
<http://www.cisco.com/warp/customer/788/AVVID/avvid.shtml>

CallManager and Problems with DC Directory

If you cannot add a user or view the Global Directory, you may have a problem with the Data Connection (DC) Directory. The DC Directory Service may have halted, or the DC Directory Service running on the CallManager Subscriber and the CallManager Publisher may not be synchronized.

For additional information on DC Directory, refer to *Fixing Problems with DC Directory*.

Password Recovery

This section describes how to recover password information.

Password Recovery Scenarios

The following situations might require you to recover passwords:

- Forgotten or lost password—Password recovery is required if the person who configured the system forgets the password or is unavailable.
- Unsupported Cisco IOS CLI modification—Password recovery is required if a password on one or more system cards is changed using the command-line interface (CLI), instead of using ICSCfg. See the [“Best Practices for Using the Cisco IOS CLI” section on page 2-14](#) for a list of unsupported Cisco IOS CLI commands.
- System interruption or system malfunction—Password recovery might be required if any of the following occurs while the system is writing data to the SPE310:
 - Power loss—The system does not have uninterruptible power supply (UPS) backup, and a commercial power outage occurs.
 - User intervention—The SPE310 card is rebooted, or the ICS System Manager session is terminated by the user.
 - System malfunction—The system malfunctions as a result of a hardware or software problem.

How Passwords Are Stored on the Cisco ICS 7750

ICS System Manager stores password information for each of the cards in the system, as follows:

- SPE310 cards—Windows 2000 user IDs and passwords (including passwords associated with the *admin* [Super Administrator] and *Administrator* [Administrator] user IDs)
- ASI and MRP cards—Cisco IOS login and enable passwords
- System switch processor (SSP) card—Cisco IOS login and enable passwords

- System alarm processor (SAP) card—Serial line protocol (SLP) enable password

**Note**

MRP200, ASI81, and ASI160 cards do not have Flash memory; this means that these cards do not have permanent local storage of configuration data—they obtain this information from the SPE running System Manager.

Recovering Passwords or Resetting Cards to Reset Passwords

This section tells how to recover passwords and how to reset cards so that you can reset the passwords on those cards. This section includes the following topics:

- [SPE310 Cards](#)
- [ASI and MRP Cards Without Flash Memory](#)
- [SSP Card](#)

SPE310 Cards

Password recovery is not supported on SPE310 cards.

If the *admin* and *administrator* passwords have been set to anything other than the defaults (*admin* and *changeme*, respectively), and if you do not remember what the passwords have been changed to, you must reimage the SPE310. Refer to [Appendix B, “Reimaging Cisco ICS 7750 SPEs”](#) for details on how to reimage the SPE310.

ASI and MRP Cards Without Flash Memory

Complete the following steps to reset ASI and MRP cards that do not have Flash memory (MRP200, ASI81, and ASI160). Resetting the cards enables them to obtain their passwords from the SPE310 running System Manager as long as their enable passwords were configured through, and known to, ICSCConfig.

If the MRP200, ASI81, or ASI160 cards have been configured with a different enable password than the password that is known to ICSCConfig, and if the enable password is not set to the default *changeme*, then ICSCConfig will not be able to discover the cards. In that case, you would not be able to restart the cards through the Shutdown/Restart page in System Manager.

Ensure that you use ICSCConfig for all system card configurations. See the [“Best Practices for Using the Cisco IOS CLI”](#) section on page 2-14 for additional information on configuring system cards.

-
- Step 1** On a PC that is connected to or networked with the Cisco ICS 7750 chassis, or using a monitor, keyboard and mouse directly connected to the SPE, access ICSCConfig.
- The system discovers the cards that are currently installed in the chassis. After the discovery process is complete, the ICS 7700 System Configuration page displays.
- Step 2** Click **Shutdown/Restart**.
- The Restart/Shutdown System Cards page appears.
- Step 3** On the Restart/Shutdown System Cards page, click the **Restart** button next to the card that you intend to restart.
- Step 4** Click **OK**.
- The ASI or MRP reboots and obtains its current password settings from the SPE310 running System Manager.
-

SSP Card

Complete the following steps to reset the SSP and change its passwords to their original values:

-
- Step 1** Press the **SHTDN** button on the SSP.
- The STATUS LED on the card starts blinking; after several minutes, it turns off. Wait for the STATUS LED to turn off before continuing to Step 2.
- Step 2** Put on an ESD-preventive wrist strap, and attach it to an unpainted chassis surface.



Caution To prevent ESD damage, handle cards by the edges only, and use an ESD-preventive wrist strap or other grounding device.

- Step 3** Completely loosen the card captive screws.

- Step 4** Press the upper and lower ejector levers outward at the same time to disengage the card from the backplane.



Caution Always use the ejector levers to disengage or seat cards. Failure to use the ejector levers can cause erroneous system error messages that indicate a card failure. Do not use the ejector levers to lift or support the weight of the cards.

- Step 5** Grasp the ejector levers, and gently pull the card partially out of the chassis slot until you can grasp the card front panel with one hand. Pull the card out approximately 1 inch (2.5 cm).
- Step 6** Make sure that the SSP card is still aligned with the upper and lower card guides in slot 7 of the chassis, and make sure that the ejector levers are in the open position (pointing outward).
- Step 7** With the top and bottom edges of the card in the card guides, gently slide the card into the chassis until you feel resistance. Because there are grounding clips near the front and rear of the card guides, you might need to increase the force that you use to get the card past the grounding clips. If you encounter extreme resistance, pull the card out slightly, and push it back in again.
- Step 8** Press the upper and lower ejector levers inward at the same time until they lock into their slots. This step firmly seats the SSP card into the chassis.
- Step 9** While the SSP is booting, use a stylus to press and hold the **SHTDN** button on the SSP front panel.
- Step 10** On a PC, open a HyperTerminal session with the SAP card.
- Step 11** Press **Ctrl-backslash** (\), and use the SAP card menu to switch to the SSP.
- Step 12** Enter the following command:

```
switch:flash_init
```

Text similar to the following is displayed:

```
switch: flash_init
Initializing Flash...
flashfs[0]: 109 files, 2 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 3612672
flashfs[0]: Bytes used: 2672128
flashfs[0]: Bytes available: 940544
flashfs[0]: flashfs fsck took 6 seconds.
...done Initializing Flash.
```

Step 13 Enter the following command to copy the SSP startup configuration file:

```
switch:copy flash:/config.text flash:/configsv.text
```

Text similar to the following is displayed:

```
File "flash:/config.text" successfully copied to  
"flash:/configsv.text"
```

Step 14 Enter the following command to delete the SSP startup configuration file:

```
switch:delete flash:/config.text
```

Step 15 Confirm that you want to delete the SSP startup configuration file:

```
Are you sure you want to delete "flash:/config.text" (y/n)?y
```

Text similar to the following is displayed:

```
File "flash:/config.text" deleted
```

Step 16 Enter the following command to enable the SSP to continue booting:

```
switch:boot
```

The SSP reboots. Text similar to the following is displayed:

```
Loading  
"flash:c2900XL-c3h2s-mz-120-5.WC5.bin".....#####  
#
```

```
File "flash:c2900XL-c3h2s-mz-120-5.WC5.bin" uncompressed and  
installed, entry point: 0x3000 executing...
```

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco Internetwork Operating System Software

```

IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version
12.0(5)WC5, MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Mon 17-Jul-00 17:35 by ayounes
Image text-base: 0x00003000, data-base: 0x00301F3C

Initializing C2900XL flash...
flashfs[1]: 109 files, 2 directories
flashfs[1]: 0 orphaned files, 0 orphaned directories
flashfs[1]: Total bytes: 3612672
flashfs[1]: Bytes used: 2672128
flashfs[1]: Bytes available: 940544
flashfs[1]: flashfs fsck took 7 seconds.
flashfs[1]: Initialization complete.
...done Initializing C2900XL flash.
C2900XL POST: System Board Test: Passed
C2900XL POST: Daughter Card Test: Passed
C2900XL POST: CPU Buffer Test: Passed
C2900XL POST: CPU Notify RAM Test: Passed
C2900XL POST: CPU Interface Test: Passed
C2900XL POST: Testing Switch Core: Passed
C2900XL POST: Testing Buffer Table: Passed
C2900XL POST: Data Buffer Test: Passed
C2900XL POST: Configuring Switch Parameters: Passed
C2900XL POST: Ethernet Controller Test: Passed
C2900XL POST: MII Test: Passed
Cisco ICS7750-SSP80 (PowerPC403GA) processor (revision 0x11) with
8192K/1024K bytes of memory.
Processor board ID JAD04120G73, with hardware revision 0x00
Last reset from warm-reset

Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
8 FastEthernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:01:96:5E:02:C0
Model revision number: B
Model number: SSP-7750
System serial number: JAD04120G73
C2900XL INIT: Complete

00:00:18: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5)WC5,
MAINTENANCE INTERIM SOFTWARE

```

Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Mon 17-Jul-00 17:35 by ayounes

When rebooting is complete, the SSP STATUS LED should be green, and the SSP ALARM LED should be off.

- Step 17** When prompted whether you want to continue with the configuration dialog box, enter **no**:

```
Continue with configuration dialog? [yes/no]:no
```

- Step 18** Enter privileged EXEC mode by entering the following command:

```
switch>enable
```

- Step 19** Display the contents of the SSP Flash memory by entering the following command:

```
switch#sh flash
```

Text similar to the following is displayed:

```
Directory of flash:/

 3  -rwx          108   Mar 01 2000 00:59:37  info
 4  -rwx       1645810   Mar 01 2000 01:00:37
c2900XL-c3h2s-mz-120-5.WC5.bin
 5  drwx          6720   Mar 01 2000 01:01:16  html
111 -rwx          108   Mar 01 2000 01:01:16  info.ver
112 -rwx          998   Jan 01 2001 00:01:50  configsv.text

3612672 bytes total (940544 bytes free)
```

- Step 20** Copy the SSP startup configuration file from Flash memory by entering the following commands:

```
switch#copy flash run
Source filename []?configsv.text
Destination filename [running-config]?<Enter>
998 bytes copied in 1.69 secs (998 bytes/sec)
```

- Step 21** Enter global configuration mode by entering the following command:

```
switch#config t
```

- Step 22** Enter the following commands to change and save your SSP passwords:

```
switch(config)#line con 0
switch(config)#password your login password
switch(config)#enable password your enable password
```

```
switch(config)#  
switch(config)#copy run start  
Building configuration...
```

**Note**

For additional information on password recovery procedures, refer to the [*Recovery Password Procedure for the Catalyst 2900XL, 3500XL, 2950, and 3550 Series Switches*](#).
