CHAPTER 3

Troubleshooting the Cisco IPICS Server

This chapter describes how to resolve problems that you may encounter when you use the Cisco IPICS server and includes the following sections:

Troubleshooting Cisco IPICS Installation Issues

For information about troubleshooting problems that you may experience when you install Cisco IPICS, refer to the "Troubleshooting the Installation" chapter in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*.

Troubleshooting Cisco IPICS Administration Console Issues

This section describes the issues that you may encounter with the Cisco IPICS Administration Console. These problems range from login issues to issues with viewing the information in the Administration Console.

This section includes the following topics:

Resolving Intermittent Browser Problems

Problem Your browser window does not reflect the latest configuration changes, or you experience intermittent problems with the Administration Console.

Solution Cisco IPICS supports only the use of Internet Explorer version 6.0.2. Be aware of the following browser-related guidelines and caveats when you use Cisco IPICS:

- By default, the Administration Console times out after 30 minutes of non use. When a timeout occurs, the system prompts you to log back in.

Note You may configure this session timeout period for a different duration by accessing the **Administration > Options** window and entering a new value in the Cisco IPICS Session Timeout Period field.

- As a best practice, make sure that you update your browser window often and before you perform any server administration tasks to ensure that you are working with the most current information. If you attempt to perform administration updates in a window that does not display the most current data, the update will not succeed and Cisco IPICS will display an error. If this situation occurs, update your browser window and retry the operation.
- To ensure that a current browser window displays the most current information, refresh it by clicking the button or tab that you used to display it. Cisco IPICS does not support the use of the browser Refresh button to refresh a window in the Administration Console.
- The Cisco IPICS Administration Console uses browser pop-up windows for certain functionality. If you have any browser pop-up blocker software installed on your machine, you may be prevented from performing certain actions. To ensure that you are not blocked from performing administration tasks, disable any pop-up blocker software that is installed on your machine before you use the Administration Console.
- Cisco IPICS does not support accessing the Administration Console in more than one browser session at the same time on the same machine. If you use multiple browser sessions to access the Administration Console, you may

experience unexpected results. To ensure proper server operational behavior, do not open more than one browser session at a time on the same machine for Administration Console functions.

- To avoid browser-related memory issues, exit your browser and then restart it after prolonged use of the Cisco IPICS Administration Console.

Resolving Failures to Access the Server With an Administration Console Browser Session

Problem After you install Cisco IPICS, you cannot successfully connect to the Cisco IPICS server by using a browser session.

Solution You may encounter this problem if one of the following issues has occurred:

- You entered the incorrect IP address or DNS name for the Cisco IPICS server
- The tomcat service is not running
- The database server is not running
- A security setting on your computer has caused a required JavaScript add-on to become disabled

To resolve this problem, perform the following procedure:

Procedure

Step 1 Check for the following items to make sure that the URL that you entered is correct:

- Ensure that you are using the secure HTTP URL, **https://** in the URL.
- If you entered the IP address for the server, check that you entered the correct IP address in the Address field in your browser.
- If you entered the DNS name for the server, ensure that the DNS name is correct and that your network is able to resolve the DNS name. If your network is unable to resolve the DNS name, enter the IP address in your browser.

Step 1 If you still cannot access the Administration Console, connect to the Cisco IPICS server via a terminal console by using the root user ID.

Step 2 Enter **root** in the *hostname* **login:** field and press **Enter**.

Cisco IPICS prompts you for the password for the root user ID.

Step 3 Enter the password for the root user ID and press **Enter**.

Step 4 Ensure that the tomcat service is running by entering the following command:

[root]# **service ipics_tomcat status**

Step 5 Perform one of the following actions, depending on the output that you receive:

- If the tomcat service is running, you receive output that is similar to the following example:

```
[root]# service ipics_tomcat status
Tomcat process (pid: 24025) is running on the system
```

  If you receive output that indicates that the tomcat service is running, continue to Step 11.

- If the tomcat service is not running, you receive output that is similar to the following example:

```
[root]# service ipics_tomcat status
PID_SEARCH_RESULT=
Tomcat is not running on the system.
```

  If you receive output that indicates that the tomcat service is not running, continue with Step 6.

Step 6 Restart the tomcat service and the policy engine by entering the following command:

[root]# **service ipics restart**

Note Be aware that Cisco IPICS cancels any active dial-in or dial-out calls when you enter the **service ipics restart** command.

Step 7 If the tomcat service does not restart, perform the following actions:

a. Check whether Cisco IPICS already installed the crontab file by entering the following command:

[root]# **crontab -l -u ipicsadmin**

Note The crontab file runs a process that checks if the tomcat service and database are running, and starts them if they are not running.

b. If you receive a message that is similar to the following message, the tomcat cron file already exists. Continue to Step 11.

```
[root]# crontab -l -u ipicsadmin
#------------------------------------------------------------------
#
#  Module: ipicsadmin.cron - Cisco IPICS cron file for user
'ipicsadmin'
#
#  Usage: crontab < ipicsadmin.cron
#
#  Environment Variables:
#
#------------------------------------------------------------------
SHELL=/bin/sh
MAILTO=root
HOME=/opt/cisco/ipics/tomcat

*  *  *  *  * /opt/cisco/ipics/bin/check_tomcat >>
/opt/cisco/ipics/tomcat/current/logs/ipicsadmin_cron.log 2>&1
```

c. If you receive a message such as **no crontab for ipicsadmin**, continue with Step 8.

Step 8 Install the crontab file by entering the following command:

[root]# **crontab /opt/cisco/ipics/cron/ipicsadmin.cron**

Cisco IPICS installs the crontab file.

Next, Cisco IPICS starts the tomcat service. You can then log in to the Administration Console by using your browser.

For information about checking the status of the tomcat service, see the "Performing Tomcat Service Procedures" section on page 2-2.

Step 9 To check the status of the database, enter the following command:

[root]# **onstat -**

If the database is online and running, the command returns output that is similar to the following example.

```
IBM Informix Dynamic Server Version 10.00.UC1      -- On-Line -- Up
00:16:14 -- 124036 Kbytes
```

If the database is not running, the command returns output that is similar to the following example.

```
shared memory not initialized for INFORMIXSERVER 'IPICSDBServer'
```

If the command output indicates that the database is not running, continue to Step 10.

Step 10 If the database is not running, manually start the database server by entering the following command:

[root]# **service ipics_db start**

Step 11 To verify network connectivity, enter the following command:

ping <*default gateway IP address*>

where:

<*default gateway IP address*> represents the default gateway address for your network.

Step 12 If the ping command is not successful, unplug the network cable from interface 1 of the server, and connect it to interface 2.

Note Generally, for servers that label their Ethernet interfaces as NIC 1 and NIC 2, you connect the Ethernet cable to the NIC 1 interface; this interface is usually the eth0 interface. For servers that label their Ethernet interfaces as 1 and 2, it is possible that the eth0 interface is mapped to interface 2. Consult your server product documentation to confirm the interface mapping.

Step 13 Retry Step 11 to attempt to verify server network connectivity.

Step 14 If the ping command is successful, log in to another server on the network and attempt to ping the Cisco IPICS server.

If the ping command is not successful, troubleshoot the network connectivity with your network administrator.

Step 15 Check the security settings on the PC that you use to access the Administration Console.

Note For enhanced security, Cisco recommends that you review and follow the recommendations that are included in the Windows XP Security Guide. To find this document, refer to the Microsoft support site at http://support.microsoft.com/ and search for "Windows XP Security Guide."

When you follow the recommendations that are included in the Windows XP Security Guide and deny all add-ons, except those that are specifically allowed in the add-on list, you may encounter a problem where you cannot access the Administration Console. This issue occurs when you use Internet Explorer from a PC that runs Microsoft Windows XP SP2 and have not enabled the JavaScript GUID in the add-on list.

Step 16 Change your security settings to ensure proper operation from Internet Explorer by explicitly enabling the following JavaScript GUID add-on on your PC:

GUID: {F414C260-6AC0-11CF-B6D1-00AA00BBBB58} - JavaScript

For detailed information about how to enable this add-on, refer to the Microsoft support site at http://support.microsoft.com/ and search for Article ID 555235.

Step 17 Try to access the server again by entering the IP address or DNS name, as shown below:

https://<*ipaddress*> | <*dnsname*>

where:

<*ipaddress*> or <*dnsname*> represents the IP address or DNS name of the server.

If you still cannot access the server, contact your Cisco technical support representative for assistance.

Enlarging the Text in the Administration Console

Problem You log in to the Administration Console successfully, but the text in the Administration Console is to small to be easily viewed.

Solution Your browser is configured to display text in a font that is smaller than the normal font. To enlarge the text in the Administration Console, perform the following procedure:

Procedure

Step 1 Open a supported version of the Internet Explorer browser.

Step 2 From the menu bar of the browser, select **View > Text Size**.

Step 3 Select **Medium** or **Larger** from the list of options to enlarge the text size.

The text in the browser window displays in a larger font.

Reducing Text in the Administration Console

Problem You log in to the Administration Console successfully, but the text in the Administration Console is too large to be easily viewed.

Solution Your browser is configured to display text in a font that is larger than the normal font. To reduce the text in the Administration Console, perform the following procedure:

Procedure

Step 1 Open a supported version of the Internet Explorer browser.

Step 2 From the menu bar of the browser, select **View > Text Size**.

Step 3 Select **Medium** or **Smaller** from the list of options to make the text size smaller.

The text in the browser window displays in a smaller font.

Analyzing 404 or 500 Error Messages When You Attempt to Access the Administration Console

Problem When you try to access the Cisco IPICS Administration Console after you perform a server software upgrade, the browser displays a 404 and/or 500 error message, as shown in the example below:

```
HTTP Status 404:
type Status report
message /ipics_server/
description: The requested resource (/ipics_server/) is not available.


Error: 500
Location: /ipics_server/
Internal Servlet Error:
```

Solution You may encounter these errors after you upgrade the server software and the system has cached some components that Cisco IPICS used in a previous version. Cached components may interfere with the proper operation of a newer version of the software and result in issues with the web application becoming unavailable and/or the occurrence of a general servlet (500) error, which causes the application to terminate unexpectedly after startup.

When this problem occurs, the system may display a message in the ipics.log file, as shown in the following example:

```
09:10:32,818 ERROR [/ipics_server]:3673 - Exception sending context
initialized event to listener instance of class
com.domain.ipics.server.core.ServerImpl
java.lang.ClassFormatError: Incompatible magic value 16693950 in class
file
```

Without access to the Administration Console **Serviceability > System Logs** window to view these log entries, you must manually access the log files by using CLI commands.

Perform the following procedure to manually access the log entries to look for the applicable error messages:

Procedure

Step 1 Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software).

Step 2 Log in to the server with root user privileges.

Step 3 Change the directory by entering the following command:

[root]# **cd tomcat/current/logs**

Step 4 Read the last 25 lines of the ipics.log file by entering the following command:

Step 5 [root]# **tail -25 ipics.log**

Step 6 Search the log for errors that indicate a problem with the web applications. These messages might contain the domain name (yourdomain.com). Messages relating to a 404 or 500 error also include phrases such as “Incompatible magic value” or “Class not found.”

Step 7 If you determine that the Cisco IPICS web applications have become corrupted, delete one or more copies of the ipics_server folder in the webapps location by entering the following command:

[root]# **rm -rf /opt/cisco/ipics/tomcat/current/webapps/ipics_server**

Note Be careful when you use the **rm** command with the **-rf** argument, because this command deletes files and folders without warning.

Step 8 Delete the ipics_server folder in the work location by entering the following command:

[root]# **rm –rf /opt/cisco/ipics/tomcat/current/work/Catalina/localhost/ipics_server**

Step 9 Restart the tomcat service by entering the following command:

[root]# **service ipics_tomcat restart**

The system displays a message to indicate whether the service has been restarted.

When the tomcat service restarts, the system creates new ipics_server folders.

Step 10 Open a supported version of the Internet Explorer browser.

Step 11 In the Location or Address field, enter the URL in the following format:

https://<*ipaddress*> | <*dnsname*>

where:

<*ipaddress*> is the IP address of the server and <*dnsname*> is the host name that you configured for the server.

You should be able to access the Administration Console.

Troubleshooting Browser Timeout Issues When You Configure an RMS with Twelve or More Loopback Interfaces

Problem When using a high latency, low bandwidth connection, you may encounter browser timeout errors when you try to update the RMS configuration for any RMS that is configured with twelve or more loopback interfaces.

Solution To resolve this issue, you must modify the Internet Explorer settings on your PC to adjust the timeout duration. This configuration modifies the ReceiveTimeout data value to allow for the additional delay.

Caution Please use extreme caution when you modify the registry. If you are not familiar with editing the registry, you should seek technical support assistance before you perform this procedure. If you modify the registry incorrectly, you may need to reinstall the operating system. Therefore, make sure that you back up the registry before you modify it and are aware of how to restore the registry, if a problem occurs.

Tip For more information about how to back up, restore, and modify the registry, access the Microsoft Support site at http://support.microsoft.com and search the Microsoft Knowledge Base for a description of the Microsoft Windows registry.

To modify the ReceiveTimeout data value, perform the following procedure on the PC that you use to access the Cisco IPICS Administration Console:

Procedure

Step 1 On the PC that you use to access the Administration Console, choose **Start > Run**.

Step 2 In the Open dialog box, enter **regedit**.

The Registry Editor displays.

Step 3 Click the **+** sign that displays next to the **HKEY_CURRENT_USER** entry.

The folders that contain root configuration information for the user who is currently logged in display.

Step 4 Click the **+** signs that display next to each of the folder names to navigate to the **Software\Microsoft\Windows\CurrentVersion** folder.

Step 5 Click the **+** sign that displays next to the **Internet Settings** folder.

At this point, you have navigated to the following folder: **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings**.

Step 6 In the Internet Settings folder, look for the **ReceiveTimeout** name.

Step 7 To modify this setting, right-click the **ReceiveTimeout** name; then, click **Modify**.

The Edit DWORD Value dialog box displays. The current DWORD value displays in hexadecimal format.

Alternatively, you can choose to delete the ReceiveTimeout name altogether by clicking **Delete**. If you choose to take this action, be aware that you could wait indefinitely for the server to respond.

Step 8 Click the **Decimal** radio button to display this value in decimal format.

Step 9 To configure this value to the recommended setting to accommodate high latency, low bandwidth links, enter **480000** in the Value data field.

This modification configures the timeout value to 8 minutes.

Step 10 Click **OK** to save your change.

Step 11 To exit the Registry Editor, choose **Registry > Exit**.

Step 12 Restart your PC for the change to become effective.

Performing Database Procedures To Resolve Login Problems and Failure To Complete Tasks in the Administration Console

Problem Users who are currently logged in to the system encounter errors when they try to perform tasks and new users cannot log in to the Administration Console. Existing VTGs and channel connections function normally.

Solution You may encounter this problem under the following conditions:

- The database has stopped.
- The database has entered into quiescent mode. This mode occurs when a restore operation or database maintenance is being performed.

If the database has stopped or gone into quiescent mode, you can perform procedures to restart the database.

To troubleshoot this issue, perform the following procedure:

Procedure

Step 1 Check to make sure that the database is running by following these steps:

a. Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software).

b. Log in to the server with the root user ID.

c. Check to see if the database is running by entering the following command:

[root]# **onstat -**

– If the database is online and running, the command returns the following response; continue to Step 5.

```
IBM Informix Dynamic Server Version 10.00.UC1     -- On-Line --
Up 00:16:14 -- 124036 Kbytes
```

– If the database is in quiescent mode, the command returns the following response; continue to Step d.

```
IBM Informix Dynamic Server Version 10.00.UC1     -- Quiescent
-- Up 00:00:42 -- 124036 Kbytes
```

– If the database is not running, the command returns the following response; continue to Step 2.

```
shared memory not initialized for INFORMIXSERVER
'IPICSDBServer'
```

d. If the database is in quiescent mode and a restore operation is in progress, wait for the operation to complete.

e. If you are not currently restoring the database, move the database from maintenance mode to online mode by entering the following command:

[root]# **onmode –m**

Step 2 If the database is stopped, you can start it by entering the following command:

[root]# **service ipics_db start**

If the database successfully starts, the Cisco IPICS operating system displays the message `[OK]`.

Step 3 If the database does not successfully start, check the diagnostics.log file by entering the following command:

[root]# more /opt/cisco/ipics/database/logs/diagnostics.log

Step 4 Press the **Spacebar** to view all the messages in the log file. To close the message log file, press **q**.

If you cannot resolve the problem by using the information that appears in the diagnostics.log file, contact your Cisco support personnel.

Step 5 If the database is running properly and you cannot use the Administration Console, contact your Cisco technical support representative for assistance.

VTG Activates Without Dispatcher Action

Problem From the **VTG Management > VTG Workgroups** window in the Administration Console, you see that a VTG is active, even though you did not activate it.

Solution You may encounter this situation if one of the following instances have occurred:

- The VTG was triggered by a policy. To check if Cisco IPICS recently activated any policies that contained the VTG, navigate to the **Policy Management > Execution Status > Executing/Executed Policy** tab.

- Another dispatcher is logged in to your Cisco IPICS system and activated that VTG.

Note As a best practice, make sure that you refresh your browser window often and before you perform any server administrative functions to ensure that you are working with the most current information. If you attempt to perform an administrative refresh in a window that does not display the most current data, the refresh will not succeed and Cisco IPICS will display an error. If this situation occurs, refresh your browser window and retry the operation.

Troubleshooting VTG Activation Problems

Problem You activate a policy, but one of the VTGs in the policy does not activate.

Solution The system may have insufficient resources, such as unavailable multicast addresses, to activate the entire policy. In such cases, Cisco IPICS attempts to activate as much of the policy as it can (for example, activating two of the three VTGs in a policy, if the system has only two available multicast addresses). To attempt to fix the problem, perform the following procedure:

Procedure

Step 1 Navigate to the **Policy Management > Execution Status > Executing/Executed Policy** tab.

Step 2 Locate the policy that you activated.

Step 3 Click **+** next to the policy name to expand it.

Step 4 Check the Status field in any rows that contain **ActivateVTG** in the Action Type field.

Step 5 If the status displays as Failed, click **Details** in the Message field.

The Message popup window displays with detailed information about the activation failure.

Step 6 If you can determine the cause of the problem from the information in the Message window, perform appropriate actions to fix the problem.

For example, the following message might indicate that the problem may be due to an insufficient number of available multicast addresses:

```
Activate VTG:vtgname has FAILED.Failed to activate talkgroup
```

VTG Does Not Appear on User PMC

Problem The dispatcher adds a user to a VTG, but the user does not see the VTG appear on the PMC. The user may also not see channels that the operator associates to the user profile.

Solution This problem occurs when a user is logged in to the database under two different user IDs. The user may log in with one user ID, while the operator or dispatcher uses another ID for the user.

Check the **User Management > Users** window for users that have multiple user IDs and delete the extra IDs.

Troubleshooting an Ops View Save Failure

Problem When you try to save an ops view that you added, the following error message displays:

```
Cisco IPICS could not save ops view <opsview name>
```

where:

<*opsview name*> is the name of the ops view that was being saved.

Solution Cisco IPICS may display this error message because of various situations, such as a database problem or an issue with another system component. If you encounter this error, take the following action:

Procedure

Step 1 Log in to the Cisco IPICS Administration Console by using the ipics user ID.

Step 2 Navigate to the **Serviceability > System Logs** window.

Step 3 Review the logs in the **Recent System Log Entries** pane. Check for any errors that display in red or blue text and which appear to be related to ops views.

Step 4 If you cannot find any errors that are related to ops views in the Recent System Log Entries pane, click **Download** to download the activity logs to your computer.

Step 5 Unzip the **ipics.zip** file and save the ipics.log file to your computer.

Step 6 Open the **ipics.log** file as a text file.

Note To view the log file, you must use a text file viewer that can understand UNIX newline characters, such as Wordpad. If you use Notepad, the file will not display properly.

Step 7 Search for the word "ERROR" in the ipics.log file.

The ipics.log may help you to determine the cause of the failure so that you can resolve the problem.

If you are not able to determine the specific error that has occurred or find information in the ipics.log file that may help you to isolate the problem, proceed to Step 8.

Step 8 Check to determine if the database is running by logging in to the Cisco IPICS server by using the root user ID and entering the following command:

[root]# **onstat -**

Step 9 Perform one of the following actions, depending on the output that displays:

- If the database is not running, the command displays text that is similar to the following example.

```
shared memory not initialized for INFORMIXSERVER 'IPICSDBServer'
```

  If you determine that the database is not running, proceed to Step 10.

- If the database is online and running, the command displays text that is similar to the following example.

```
IBM Informix Dynamic Server Version 10.00.UC1     -- On-Line -- Up
00:16:14 -- 124036 Kbytes
```

If you determine that the database is running, contact your Cisco technical support representative for assistance.

Step 10 If the database has stopped, you can start it by entering the following command:

[root]# **service ipics_db start**

If the database successfully starts, the system displays the message `[OK]`.

If the database does not successfully start, check the diagnostics.log file by entering the following command:

[root]# **more /opt/cisco/ipics/database/logs/diagnostics.log**

Step 11 Press the **Spacebar** to view all the messages in the log file. To close the message log file, press **q**.

If you cannot resolve the problem by using the information that appears in the diagnostics.log file, contact your Cisco support personnel.

Resolving Administration Console Undefined Errors

Problem Administration Console users cannot view any windows that display data in a table format, and receive errors that indicate that elements in the Administration Console are undefined.

Solution This problem occurs when the browser JavaScript engine cannot process advanced dynamic features because of installation of third party software or other setup issues. You can resolve this problem by reinstalling the JavaScript engine. To download the installation script to your PC, go to http://www.microsoft.com and search for Windows Script 5.6 for Windows Server 2003.

Commands Fail Intermittently

Problem An intermittent "command failed" error displays when a dispatcher activates or deactivates a VTG or when a user logs in or logs out of the PMC application.

Solution Retry the command or action. For more information about the nature of the error, navigate to the **Serviceability > System Logs** window in the Administration Console and view the logs in the **Recent System Log Entries** window. The log content should provide you with additional details about the command failure.

Adding Fonts to Internet Explorer to Fix Language Character Display Problems

Problem Some data, such as user names and channel names, displays with incorrect characters in some languages.

Solution The Internet Explorer browser on some PCs may be unable to display characters from several languages on the same page. When the browser displays English, Hebrew, and Arabic, characters from some of the languages may display incorrectly. The problem occurs when Internet Explorer selects a font that supports only some languages.

To resolve this problem, in Internet Explorer, choose a font that supports all unicode character sets. Such fonts include Arial Unicode MS (which is included with Microsoft Office).

To choose a new font for Internet Explorer, perform the following procedure:

Procedure

Step 1 Open a supported version of the Internet Explorer browser.

Step 2 From the Internet Explorer menu, choose **Tools > Internet Options**.

The Internet Options window displays.

Step 3 Click **Fonts**.

The Fonts dialog box displays.

Step 4 From the Web page font pane, select Arial Unicode MS.

Step 5 To accept the font choice, click **OK**.

Step 6 Click **OK** to save your changes and close the Internet Options window.

Internet Explorer now displays the languages correctly.

PMC Users Receive Error Messages During Login After a Database Restore Operation

Problem After a database restore procedure completes, PMC users receive an "unknown response" error message when they try to launch the PMC. These users cannot connect to the server but they can operate in offline mode.

Solution This problem may occur if the tomcat service does not restart after the restore procedure has completed or if the PMC user attempts to log in to the system before the tomcat service has completed the restart process.

To resolve this problem, perform the following procedure:

Procedure

Step 1 Check to determine if the tomcat service is running by entering the following command:

[root]# **service ipics_tomcat status**

Step 2 Perform one of the following actions, depending on the output that you receive:

- If the tomcat service is running, you receive output that is similar to the following example:

```
[root]# service ipics_tomcat status
Tomcat process (pid: 24025) is running on the system
```

  If you receive output that indicates that the tomcat service is running, wait for at least five minutes so that the database has time to synchronize its information with the RMS.

- If the tomcat service is not running, you receive output that is similar to the following example:

```
[root]# service ipics_tomcat status
PID_SEARCH_RESULT=
Tomcat is not running on the system.
```

If you receive output that indicates that the tomcat service is not running, restart the tomcat service and the policy engine by entering the following command:

[root]# **service ipics restart**

Note Cisco IPICS cancels any active dial-in or dial-out calls when you enter the **service ipics restart** command.

Step 3 If you continue to experience problems, contact your Cisco technical support representative for assistance.

Configuration Changes Do Not Get Saved When Multiple Users Configure Cisco IPICS

Problem Multiple users are connected to the Administration Console with separate browser sessions and are making configuration changes concurrently. One user changes a configuration. At a later time, the user notices that their changes were overwritten or not saved.

Solution If multiple users configure Cisco IPICS at the same time, and the users are updating the same data, Cisco IPICS retains the last change that was made. The last configuration change prevails over any other previous configuration changes to the Cisco IPICS Administration Console.

Recovering a Deleted System Administrator User

Problem You deleted the last user who had the System Administrator or All role, and now you cannot perform any system administration tasks in the Administration Console.

Solution If you delete all system administrator users from the system, you can log in as an operator and create a new system administrator user ID. Cisco IPICS includes a safeguard that prevents you from deleting all operators from the system.

Note You must be assigned the operator role and have an operator user ID and password to recover a deleted system administrator user. For more information about operators, refer to the "Performing Cisco IPICS Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

To recover the system administrator role, perform the following procedure:

Procedure

Step 1 Log in to the server by using the operator user ID and password.

Step 2 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 3 Click **Add**.

Step 4 In the required fields, which are indicated by an asterisk, enter the user information.

Step 5 From the Roles drop-down list box, choose **System Administrator** or **All** for the user role.

The new user appears in the SYSTEM ops view; this user can now perform administrative tasks.

Troubleshooting User ID and Password Issues

The following section describes how to troubleshoot issues that you may encounter with user IDs and passwords.

This section includes the following topics:

Resetting a Forgotten or Missing ipics User Password

Problem You attempt to log in to the Administration Console as the ipics user. A pop-up window displays to inform you that you have entered an incorrect user ID or password.

Solution You entered an incorrect password for the ipics user. If you have root user access, you can reset the ipics user password and regain access to the Administration Console by entering the **reset_pw** command.

To reset the ipics user ID and resolve this problem, perform the procedure that is documented in the "Resetting, Changing, or Creating a Password With the reset_pw Tool" section on page 6-7.

Resetting the Password for the ipicsadmin or informix User ID

Problem You attempt to log in to a terminal console as the ipicsadmin or informix user to perform database administration tasks. You cannot retrieve the password for the informix user, or you have lost or forgotten the password for the ipicsadmin user. You are not able to log in to the system.

Note You create a password for the ipicsadmin user during the installation of the Cisco IPICS server software. The installation program also creates a password for the informix user by using a random algorithm; however, you cannot retrieve this password.

Solution If you have root user access, you can log in by using the ipicsadmin or informix user ID by entering either the **su** command or by entering the **reset_pw** command to reset the ipicsadmin or informix password.

To log in as the informix or ipicsadmin user, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 Log in as the ipicsadmin or informix user by performing one of the following actions:

- To log in as the ipicsadmin user, enter the following command:

  [root]# **su - ipicsadmin**

- To log in as the informix user, enter the following command:

  [root]# **su - informix**

Step 3 After you have completed your tasks as the ipicsadmin or informix user, enter **exit** to log out as that user and return as the root user.

To reset the password for the ipicsadmin or informix user, perform the procedure that is documented in the "Resetting, Changing, or Creating a Password With the reset_pw Tool" section on page 6-7.

Changing the root User Password

Problem You need to change the root user password.

Solution You can change the password for the root user ID, as needed, by performing the procedure that is documented in the "Resetting, Changing, or Creating a Password With the reset_pw Tool" section on page 6-7.

Resetting a Locked or Disabled User Account

Problem A user whose account has been locked or disabled cannot log in to the system.

Solution The user account may be locked or disabled. A user account can be locked or disabled under the following conditions:

- The number of invalid login attempts exceeded the number of maximum attempts and Cisco IPICS automatically locked the user. For more information, refer to the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
- A user with Operator or All privileges manually locked or disabled the user. For more information about locking out or disabling a user, refer to the "Performing Cisco IPICS Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

When a user account is disabled, Cisco IPICS disallows any endpoint devices from logging in to the system; any existing login sessions, such as PMC, dial-in, and Administration Console, are automatically terminated.

When a user account is locked, Cisco IPICS disallows any new logins; existing logins continue to work until the user logs out of the system.

To unlock or enable a user account, perform one of the following actions:

- If you have access to the root user ID, perform the procedure that is documented in "Unlocking or Enabling a Locked or Disabled User With the enableuser Tool" section on page 6-3 to unlock or enable the user with CLI commands.
- If you are able to access the Administration Console with a user ID that has Operator or All privileges, perform one of the following actions to unlock or enable a user account; then, proceed to verify your configuration changes:
  - To unlock a user account in the Administration Console, follow the procedure in the "Locking or Unlocking a User" section in the "Performing Cisco IPICS Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

– To enable a user account in the Administration Console, follow the procedure in the "Changing User Status" section in the "Performing Cisco IPICS Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Troubleshooting License Issues

This section contains information about troubleshooting problems with your Cisco IPICS license and includes the following topics:

Resolving Invalid Base Server License Messages that Display After You Upload the License File

Problem You upload the license for your Cisco IPICS server in the **Administration > License Management** window. After you click **Apply** to apply the license, the following message persists in the Administration Console:

```
Your system does not have a valid base server license; please upload
this license file type.
```

You cannot navigate to any other windows in the Administration Console.

Solution This situation might be caused by one or more of the following conditions:

- The license file is invalid

- The license manager does not recognize the license file as a valid file and does not run
- The license manager did not start
- Unnecessary files in the directory in which Cisco IPICS stores the licenses are causing problems with the license manager

Note You can encounter license issues if you change the IP address of the server using an unsupported method. To change the server IP address, use the **modify_ip** command by following the procedure that is documented in the "Changing the Server IP Address With the modify_ip Tool" section on page 6-4. Using other methods to change the server IP address can cause host mismatch problems and invalidate the license.

To resolve these conditions, perform the following procedure:

Procedure

Step 1 To determine that you have a valid license, check the following items:

- Make sure that the MAC address for the license file matches the MAC address of the eth0 interface of the Cisco IPICS server. To locate the hardware MAC address for the eth0 interface, log in to the server by using the root user ID; then, enter the following command and note the information that displays in the HWaddr field in the command output:

  [root]# **ifconfig eth0**

- Make sure that the license file has a file extension of .lic.
- Make sure that there are no spaces or special characters in the name of the license file.

Step 2 If you determine that your license file is invalid or misnamed, purchase a valid license file or obtain a new copy of your existing file. For more information, refer to the "Obtaining Your License File" section in the "Installing Cisco IPICS" chapter in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*.

Step 3 From the Administration Console, navigate to the **Administration > License Management** window; then, click the **Apply** button to restart the license manager.

Step 4 If the server continues to display the invalid license message, log in to the server by using the root user ID.

Step 5 To check the status of the license file, enter the following command:

[root]# **service ipics_lm status**

Step 6 Perform the following action, depending on the message that Cisco IPICS displays:

- If the following message displays, the license manager is not running. Continue with Step 7.

```
ipics_lm is not running.
```

- If the following message displays, the license manager is running. Proceed to Step 10.

```
ipics_lm is running (PID 24856).
```

Note The license manager does not start until it detects a valid license file. If the license manager does not reflect a running status after you upload a license file, this condition could indicate that the license manager does not recognize a valid license file.

Step 7 If the license manager is not running, restart the license manager by entering the following command:

[root]# **service ipics_lm restart**

Step 8 To recheck the status of the license manager, enter the following command:

[root]# **service ipics_lm status**

Step 9 Perform one of the following actions, depending on the message that displays:

- If a message displays to indicate that the license manager is running, proceed to Step 10.
- If a message displays to indicate that the license manager is not running, continue with Step 11.

Step 10 To check for unnecessary files, delete them, and upload license files, perform the following steps:

a. Log in to the Cisco IPICS server by using the root user ID.

b. To navigate to the directory that includes the license files, enter the following command:

[root]# **cd /root/tomcat/current/webapps/license**

c. Remove all of the license files that are in the **/root/tomcat/current/webapps/license** directory by entering the following command:

[root]# **rm *.lic**

d. Enter **yes** when the system prompts you to confirm the deletion of each license file.

Note Make sure that you do not remove any other files in this directory. The cisco.opt file in this directory is required for the correct operation of Cisco IPICS.

e. Upload the license file(s) by following the procedure in the "Uploading the Cisco IPICS License Files" section in the "Installing Cisco IPICS" chapter in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*.

Note Be sure to click **Apply** after you upload each file.

Step 11 If you still cannot upload the license file, perform the following steps:

a. To create a log file and a .tar file that contain diagnostic and logging information, enter the following command:

[root]# **/opt/cisco/ipics/bin/diagnosticscript** <*output-file-name*>**.log** <*tar-file-name*>**.tar**

where:

<*output-file-name*>**.log** is the name that you designate for the log file, and <*tar-file-name*>**.tar** is the name that you designate for the .tar file.

b. Save, to your PC, the .tar file that you created in Step a. by following the procedure that is documented in the "Downloading the Server Diagnostic Information" section in the "Understanding Cisco IPICS Serviceability and Diagnostic Information" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

c. If you require further assistance, contact your Cisco technical support representative; you may need to provide the .tar file.

After Uploading Multiple License Files, All Features Do Not Display in the Administration Console

Problem You uploaded multiple license files, but the summary in the **Administration > License Management** window does not display all of the features that you have licensed.

Solution Perform the following actions to make sure that the name of the license file matches the MAC address of the server eth0 interface so that the license manager can read each license correctly.

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user ID.

Step 2 To navigate to the directory that includes the license files, enter the following command:

[root]# **cd tomcat/current/webapps/license**

Step 3 Remove all of the license files that are in the **tomcat/current/webapps/license** directory by entering the following command:

[root]# **rm *.lic**

Step 4 Enter **yes** when the system prompts you to confirm the deletion of each license file.

Note Do not remove any other files in this directory.

Step 5 From the Administration Console, navigate to the **Administration > License Management** window.

Step 6 Upload the license file(s) by following the procedure that is documented in the "Uploading the Cisco IPICS License Files" section in the "Installing Cisco IPICS" chapter in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*.

Note Make sure that each license file has the correct MAC address.

After Changing the Server IP Address, You Experience Host Name Mismatch or Problems Installing the License

Problem After you reboot your server, following an IP address change, you cannot apply the license file. The following message persists in the Administration Console and you cannot navigate to any area in the Administration Console except the **Administration > License Management** window:

```
Your system does not have a valid base server license; please upload
this license file type.
```

Solution Some methods of changing the IP address do not update the /etc/hosts file, which can cause host mismatch or other IP connectivity problems. To ensure that Cisco IPICS properly processes any IP address changes, use only the **modify_ip** tool to change the IP address by following the procedure that is documented in the "Changing the Server IP Address With the modify_ip Tool" section on page 6-4.

Changing System Date Invalidates Time-Bound License

Problem After you change the server date, your time-bound license becomes invalid.

Solution Cisco IPICS can invalidate time-bound licenses when you change the system date in the operating system to a date that is before the license start date. Invalid licenses cause the Cisco IPICS system to become inoperable.

Note You must restart the license manager, or reboot the server, for system date changes to become effective.

To resolve issues that pertain to these system date changes, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in using the root user ID.

Step 2 Change the system date to a date that is after the system start date by entering the following command:

[root]# date *mmddyyyy*

where:

mmddyyyy is the current date.

Step 3 Restart the license manager by entering the following command:

[root]# **service ipics_lm restart**

Suppressing Server Expiration Messages After Installing a More Recent Time-Bound License

Problem You have existing time-bound licenses, and you install a more recent time-bound license on your server. After the installation, you continue to see warning messages that alert you of an upcoming license expiration.

Solution You may see the license expiration warning message if you do not remove additional time-bound licenses from the server. To suppress this warning message, remove the time-bound licenses that are about to expire by performing the following procedure:

Procedure

Step 1 Open a terminal window and log in by using the root user ID.

Step 2 Navigate to the directory where Cisco IPICS stores the license files by entering the following command:

[root]# **cd tomcat/current/webapps/license**

Step 3 View the license files by entering the following command:

[root]# **ls -l *.lic**

The license files display with the time and date that the license was last modified.

Step 4 Make a note of the licenses that you no longer need.

The time and date that displays with the file information might assist you with determining which files you need to delete.

Step 5 Delete the unnecessary license files by entering the following command:

[root]# **rm** <*licensefilename*>**.lic**

where:

<*licensefilename*>**.lic** is the name of the license file that you want to delete.

Caution Make sure that you do not delete the cisco.opt file. This file is required for the correct operation of Cisco IPICS.

Step 6 Repeat Step 5 for each license file that you need to delete.

Step 7 Restart the server by entering the following command:

Step 8 [root]# **service ipics restart**

Step 9 Log in to the Administration Console by using the ipics user ID and navigate to the **Administration > License Management** window.

Step 10 To apply the license deletions to the system configuration, click **Apply**.

Step 11 If a message displays that indicates that a license is about to expire, click **Dismiss Warnings**.

Troubleshooting Policy Engine Issues

This section contains information about troubleshooting problems with the policy engine and includes the following topics:

Uploading a Large Zipped File of Prompts Causes an Error

Problem From the Administration Console, you attempt to upload a large zipped file that contains dial engine prompts and see the following error message:

```
The form could not be properly constructed.
```

When you view the system logs from the **Serviceability > System Logs** window, the following error messages display:

```
java.lang.IllegalArgumentException: invalid directory: \\CHANNEL\
    at com.cisco.file.File.<init>(L885)
    at com.cisco.file.File.<init>(L724)
    at
com.cisco.ivr.config.api.impl.ManageRepositoryAPI.getFileList(L143)
    at com.cisco.ivr.config.api.impl.ManagePrompts.getFileList(L383)
    at com.cisco.ivr.config.api.impl.ManagePrompts.getPromptList(L369)
    at
com.cisco.ipics.ippe.dialengine.promptmanagement.handlers.PromptHandle
r.getPromptList(L215)
    at
com.cisco.ipics.ippe.dialengine.promptmanagement.actions.PromptAction.
doInit(L444)
```

```
    at
com.cisco.ipics.ippe.dialengine.promptmanagement.actions.PromptAction.
unspecified(L152)
```

Solution You attempted to upload a zipped file that is larger than Cisco IPICS can handle. Cisco IPICS can upload zipped files with a maximum size of 1024 MB (1 GB). To resolve this problem, create a smaller zipped file or divide the zipped file into smaller zipped files; then, retry the upload process.

IppeAgentImpl ERROR Messages Display in the ipics.log File

Problem When you view the system logs that are located in the **Serviceability > System Logs** window in the Administration Console, you see an error message that is similar to the following example:

```
2007-02-06 21:19:45,000 [http-8443-Processor68] ERROR
IppeAgentImpl:200 -
com.cisco.ipics.ippe.communicator.subsystem.IppeSubsystemRemoteService
```

Solution Error messages that include IppeAgentImpl in the text indicate that your system could not connect to the Cisco IPICS policy engine. This message may display because your system is not licensed for the policy engine, or the policy engine processes did not start.

Note Messages that display INFO in the ipics.log file are only for informational purposes and do not signify a problem with the policy engine.

If your system is not licensed for the policy engine, no action is required. To determine if your system is licensed and to check the status of the policy engine, perform the following procedure.

Procedure

Step 1 Check that your system is licensed for the policy engine by navigating to the **Administration > License Management > Summary** window in the Server tab of the Administration Console.

Step 2 Check the status of your license in the Policy Engine Base License field.

If the field shows a status of Not Licensed, IppeAgentImpl messages typically display in the logs and require no action.

If the field shows a status of Licensed, continue with Step 3.

Step 3 Perform the following steps to check if the policy engine processes are running and restart them, if necessary:

a. Open a terminal window and log in to the server by using the root user ID.

b. To check the status of the policy engine processes, enter the following command:

[root]# **service ippe_dial_engine status**

If the policy engine processes are running, Cisco IPICS displays information similar to the following text:

```
CVD process (pid 7606) is running...
Engine process (pid 7714) is running...
```

If the policy engine processes are not running, Cisco IPICS displays information similar to the following text:

```
CVD process is NOT running...
Engine process is NOT running...
```

c. If the policy engine processes are not running, start them by entering the following command:

[root]# **service ippe_dial_engine start**

Cisco IPICS displays the message `[OK]` as each process starts.

d. Check the status of the policy engine by reentering the **service ippe_dial_engine status** command.

e. If the policy engine processes are not running, contact your Cisco technical support representative for assistance.

Resolving Communication Problems Between the Policy Engine and the Prompt Manager

Problem You encounter errors with the policy engine; messages that are similar to the ones shown below display in the **Serviceability > System Logs** window or in the ipics.log file:

```
2006-08-18 14:20:53,961 [http-8443-Processor25] ERROR PromptUtil:200 -
Unable to communicate with prompt manager.
2006-08-18 14:20:53,962 [http-8443-Processor25] ERROR PromptUtil:200 -
Unable to communicate with prompt manager.
2006-08-18 14:20:56,747 [http-8443-Processor21] ERROR PromptUtil:200 -
```

Solution This situation indicates that the policy engine processes are not running. To start the policy engine processes, perform the procedure that is documented in the "Manually Starting the Dial Engine" section on page 2-15.

Resolving Reconnection Failures After a Dial-In Caller Uses the Hold or Call Waiting Feature

Problem After dialing in and connecting to a channel with a Cisco Unified IP Phone, you receive another call. You place the dial-in call on hold and use the call waiting feature to answer the incoming call. When you attempt to reconnect with the channel, you receive several seconds of silence, followed by a fast busy tone.

Solution The Cisco Unified IP Phone requires Media Termination Point (MTP) resources to use the hold or call waiting feature. MTP resources must exist in your SIP provider (for example, Cisco Unified Communications Manager) to successfully reconnect to a dial-in call after you use the hold or call waiting feature.

To successfully reconnect with a dial-in call, either add MTP resources to your SIP provider, or configure your SIP provider so that it can allocate MTP resources from another source. For more information about configuring the SIP provider, refer to the "Configuring the SIP Provider" sections of the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Troubleshooting Dial-In Call Connection Failures

Problem When you call in to the Cisco IPICS policy engine, your call does not connect. Instead, you hear a fast busy tone or a message that indicates that the call cannot be completed.

Solution One or more of the following conditions can cause dial-in calls to fail to connect:

- Your dial engine or ops view configuration might be incorrect
- The policy engine was not manually restarted after you performed SIP configuration changes
- The **bind control source-interface Loopback0** command was not successfully applied to your RMS configuration
- The dial peer configuration for the RMS might be incomplete or incorrect. Problems with dial-in and dial-out calls can be caused by incorrect or misconfigured dial peers. For information about configuring your dial peers for use with Cisco IPICS, refer to the "Configuring the Cisco IPICS RMS Component" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

To resolve this issue, perform the following procedure:

Procedure

Step 1 Check your ops view configuration to make sure that a dial number and dial ports are associated with an ops view by navigating to the **Configuration > Ops Views** window in the Server tab.

The Ops Views window displays.

Step 2 Check to make sure that a that a dial-in number exists in the ops view configuration and enter a number if it does not exist by following these steps:

a. Click the name of the ops view.

The **Ops Views >** <*opsviewname*> window displays.

b. Determine if a dial-in number exists in the ops view configuration by checking the Dial Number field in the General tab.

c. If the Dial Number field is empty, enter the dial-in information in this field.

For information about adding a dial-in number for an ops view, refer to the "Performing Ops Views Tasks" section of the "Configuring and Managing Cisco IPICS Operational Views" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Step 3 Determine if dial port licenses have been allocated for the ops view by viewing the Dial Ports field in the License Allocation pane.

Step 4 If the number in the Dial Ports field is 0, increase the number to allocate sufficient licenses for dial ports in the ops view.

For information about allocating dial ports for an ops view, refer to the "Allocating Dial Ports for the Dial-In/Invite and Notification Features" section of the "Configuring and Managing Cisco IPICS Operational Views" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Step 5 Check to make sure that a sufficient number of dial ports exist for dial-in calls in the ops view by viewing the following fields:

- Dial ports reserved for dial-in/invite feature
- Dial ports reserved for dial-in/invite or notifications

Step 6 If the number that displays in the fields in Step 5 is equal to zero, decrease the number of ports in the **Dial ports reserved for notifications** field; then, perform one of the following actions:

- Add the ports that you removed to the **Dial ports reserved for dial-in/invite feature** field.
- Take no action. Cisco IPICS adds the ports that you removed to the total number of ports that are reserved for the dial-in/invite feature and notifications.

Step 7 Make sure that you have specified a host, user name, and password for the SIP provider by navigating to the **Dial Engine > SIP Configuration** window; then, view the fields that display in the SIP Provider Configuration pane.

Step 8 If any fields in the SIP Configuration window are missing or incorrect, add or change them.

For more information about configuring SIP, refer to the "Configuring SIP" and "Configuring the SIP Provider" sections of the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Step 9 Perform the following steps to make sure that the proper SIP configuration has been applied to the RMS:

Note If you enter the **bind control source-interface Loopback0** command while there are any active calls or permanent connections in the RMS, the RMS does not apply the command to its running configuration. In this situation, you will encounter a fast busy tone when you call the dial engine directory number. In addition, the Cisco IOS SIP debug logs show a SIP 403 (forbidden) message from the dial engine.

a. Log in to the RMS.

b. Enter the following command in privileged mode to make sure that the **bind control source-interface Loopback0** command is applied to the running configuration of the RMS:

   Router# **show running-config | include bind control source-interface**

c. If the **bind control source-interface** command is present in the running configuration, continue to Step 10. If the **bind control source-interface** command is not present in the running configuration, continue to the next step to add the command.

d. Enter the following command, and view the output that displays in the Total call-legs field, to determine if there any active calls on the RMS:

   Router# **show call active voice brief**

e. If the Total call-legs field displays zero, continue to Step g. If the field displays a value that is greater than zero, enter voice port configuration mode for the call that is active; then, enter the following command to take the voice port offline and cancel any active voice calls:

   Note The following command takes the voice port out of service. Make sure that you enter this command during a maintenance window or other off-peak hours.

   Router(config-voiceport)# **shutdown**

f. Repeat Step e until you have taken all active calls offline.

g. Enter the following command in SIP configuration mode to bind the source address of SIP signaling packets to the IP address of the Loopback0 interface:

   Router(conf-serv-sip)# **bind control source-interface Loopback0**

h. To bring the voice ports back online, enter the following command in voice port configuration mode:

   Router(config-voiceport)# **no shutdown**

i. To verify that the output reflects the SIP configuration change that you performed in this procedure, enter the following command:

   Router# **show running-config | include bind control source-interface**

j. To update your configuration on the RMS, enter the following command:

   Router# **copy running-config startup-config**

Note For more information about configuring the RMS, refer to the "Configuring the Cisco IPICS RMS Component" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Step 10 If you made any changes to the SIP configuration, you must restart the policy engine and the tomcat service by performing the following procedure:

a. Log in to the Cisco IPICS server by using the root user ID.

b. To restart the policy engine and the tomcat service, enter the following command:

   [root]# **service ipics restart**

Note Be aware that Cisco IPICS cancels all active dial-in or dial-out calls when you enter the **service ipics restart** command.

Step 11 If you still cannot determine the cause of the dial-in failure, contact your Cisco technical support representative for assistance.

Troubleshooting Dial-Out Invitation Failures

Problem You cannot send dial-out invitations from the Cisco IPICS system.

Solution The Cisco IPICS configuration for dial-out invitations or notifications might be incorrect. To check your configuration and fix any problems that you find, perform the following procedure:

Procedure

Step 1 Make sure that you have configured an outbound dial number by performing the following steps:

a. Navigate to the **Dial Engine > Dial Engine Parameters** window from the Policy Engine tab.

b. Check the Outbound Dial Number field to determine if you have configured an outbound dial number.

c. If a valid number does not exist in the Outbound Dial Number field, create an outbound dial number by following the procedure that is in the "Configuring Dial Engine Parameters" section of the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Step 2 Check to see if you have ports that are configured for dial-out invitations by navigating to the **Configuration > Ops Views >** <*opsviewname*> window in the Server tab.

Step 3 Determine if ports exist for dial-out invitations by checking the following fields in the window:

- Dial ports reserved for dial-in/invite feature
- Dial ports reserved for dial-in/invite or notifications

Step 4 If the number in both fields is equal to zero, perform the following steps to add ports for dial-in/invite feature:

a. Decrease the number of ports in the **Dial ports reserved for notifications** field.

b. Perform one of the following actions:

– Add the ports that you removed to the **Dial ports reserved for dial-in/invite feature** field.

– Take no action. Cisco IPICS adds the ports that you removed to the total number of ports that are reserved for dial-in calls, invitations, or notifications.

Troubleshooting Dial-Out Notification Failures

Problem Dial-out notifications do not succeed. You cannot send an e-mail, SMS, pager, or phone message to users.

Solution The configuration for dial-out notifications may be incorrect. To check your configuration and fix any problems that you find, perform the following procedure:

Note If you are performing dial-out notifications from one ops view to another, see the "Troubleshooting Dial-Out Notification Failures Between Users in Different Ops Views" section on page 3-46.

Procedure

Step 1 If the notification is a dial-out notification, make sure that you have configured an outbound dial number by completing Step 1 in the "Troubleshooting Dial-Out Invitation Failures" section on page 3-43.

Step 2 If the notification is an e-mail, SMS or text-based pager notification, make sure that you have configured an SMTP server and a sender e-mail address by performing the following steps:

a. Navigate to the **Dial Engine > Dial Engine Parameters** window from the Policy Engine tab.

b. Determine if you have configured an SMTP server for e-mail notifications by checking the Outbound Dial Number field.

c. Determine if you have configured an e-mail address for your server by checking the Sender Email Address field.

d. Add the SMTP server or sender e-mail address, as required, by following the procedure in the "Configuring Dial Engine Parameters" section in the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Step 3 Check that ports are configured for dial-out notifications by navigating to the **Configuration > Ops Views >** <*opsviewname*> window in the Server tab.

Step 4 Check that ports are configured for dial-out notifications by checking the following fields in the window:

- Dial ports reserved for notifications
- Dial ports reserved for dial-in/invite or notifications

Step 5 If the number of dial ports that are reserved for notifications (specified in the **Dial ports reserved for notifications** and **Dial ports reserved for dial-in/invite or notifications** fields) is equal to zero, perform the following steps to add ports for notifications:

a. Decrease the number of ports in the **Dial ports reserved for dial-in/invite feature** field.

b. Perform one of the following actions:

- Add the ports that you removed to the **Dial ports reserved for dial-in/invite feature** field.
- Take no action. Cisco IPICS adds the ports that you removed to the total number of ports that are reserved for dial-in calls, invitations, or notifications.

Troubleshooting Dial-Out Notification Failures Between Users in Different Ops Views

Problem Dial-out invitations and notifications do not succeed from users who belong to different ops views. Users who receive a dial-out message and attempt to authenticate, receive an error message stating that their user ID or Personal Identification Number (PIN) is invalid.

Solution If you associate a policy with an ops view, that policy is available only to users who belong to that ops view. Make sure that all users in a policy belong to the same ops view.

You cannot associate users from different ops views to a policy. For example, if a policy belongs to the police ops view, make sure that you associate only users from the police ops view to a policy that contains dial-out invitations and notifications.

Note This policy-to-ops-view association information does not apply to the SYSTEM ops view, to which all users belong. For more information about ops views, refer to the "Configuring and Managing Cisco IPICS Operational Views" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Understanding a PARTIAL_SERVICE Status For the Dial Engine and Subsystem Manager

Problem The dial engine and subsystem manager display a PARTIAL_SERVICE status. In this release, a fully functional system displays a status of PARTIAL_SERVICE, which indicates that the system is properly configured and operating normally.

Solution If the SIP Subsystem and the IPPE Subsystem display a status of IN_SERVICE, the dial engine and subsystem manager are operating normally. Check the status of the SIP Subsystem and the IPPE Subsystem by navigating to the **Dial Engine > Control Center > Status** window in the Policy Engine tab.

Note The SIP Subsystem status displays as SHUTDOWN until you configure it.

Analyzing a SHUTDOWN Status For the SIP Subsystem

Problem After you update your SIP configuration, the SIP Subsystem displays a SHUTDOWN status.

Solution This situation may be caused by a SIP misconfiguration or a failure to restart Cisco IPICS after saving a change to the SIP configuration. The SIP Subsystem should display an IN_SERVICE status if it is properly configured and operational.

To resolve issues with your SIP configuration, perform the following procedure:

Procedure

Step 1 Check the status of your SIP configuration by navigating to the **Dial Engine > Control Center > Status** window.

If the status of the SIP Subsystem displays SHUTDOWN, continue to Step 2.

Step 2 Make sure that you have configured all of the required fields in the **Dial Engine > SIP Configuration** window. For information about how to configure the SIP Subsystem, refer to the "Configuring the SIP Provider" section in the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Step 3 If the status of the SIP Subsystem continues to show a status of SHUTDOWN, restart the policy engine and the tomcat service by performing the following steps:

a. Log in to the Cisco IPICS server by using the root user ID.

b. To restart the policy engine and the tomcat service, enter the following command:

[root]# **service ipics restart**

Note You must restart the ipics service after you make any changes to the SIP subsystem configuration.

Step 4 If the SIP Subsystem continues to show a status of SHUTDOWN, contact your Cisco technical support representative for assistance.