



CHAPTER 2

Cisco IPICS Dispatch Console Installation, Configuration, and Maintenance

This chapter describes how to install and uninstall the Cisco IPICS Dispatch Console. It also explains how to optimize audio on a client PC for use with the Cisco IPICS Dispatch Console and provides other information that relates to operations.

This chapter includes these topics:

- [Installing the Cisco IPICS Dispatch Console, page 2-1](#)
- [Uninstalling the Cisco IPICS Dispatch Console, page 2-6](#)
- [WAVE Engine Service Requirements, page 2-7](#)
- [Cisco IPICS Dispatch Console Logs, page 2-8](#)
- [Cisco IPICS Dispatch Console Guidelines for Use, page 2-11](#)
- [Optimizing Audio for the Cisco IPICS Dispatch Console, page 2-14](#)

Installing the Cisco IPICS Dispatch Console

The following sections provide information about downloading and installing the Cisco IPICS Dispatch Console on a client PC. The client PC must adhere to the requirements and guidelines that the [“Client PC” section on page 1-2](#) describes.

- [Installation Guidelines, page 2-2](#)

- [Installation Directories, page 2-2](#)
- [Installation Procedure, page 2-3](#)

Installation Guidelines

Before you install the Cisco IPICS Dispatch Console, review the following information:

- The installation process involves downloading a self-extracting Cisco IPICS Dispatch Console installation program from a Cisco IPICS server. This process downloads required installation and configuration files. If you are authorized to use alert tones, the download may also include alert tones (or they may be downloaded separately).
- The installation program automatically installs the Cisco IPICS Dispatch Console software on your client PC. The Cisco IPICS Dispatch Console does not need to be connected to the Cisco IPICS server to perform this installation.
- The installation program performs preinstallation tasks to verify that the client PC is not running another version of the Cisco IPICS Dispatch Console, that the current version of the Cisco IPICS Dispatch Console is not already installed, and that the client PC is running the appropriate operating system.
- The installation automatically adds an entry for the Cisco IPICS Dispatch Console to the Windows Start menu, and adds a Cisco IPICS Dispatch Console shortcut to your Windows desktop.
- If you are running the Cisco Security Agent (CSA) on your client PC and see a CSA access permission dialog box during the installation process, click **Yes** to grant permission to the IDC installation.

Installation Directories

If you are not logged into a client PC with Window Administrator privileges, you must have write privileges to the following Cisco IPICS Dispatch Console installation directories to install, uninstall, or run the Cisco IPICS Dispatch Console.

**Note**

This list shows installation directories under C:\Program Files, which is the default folder for the Cisco IPICS Dispatch Console installation directories. You can change this default folder when you install the Cisco IPICS Dispatch Console.

- C:\Program Files\Cisco Systems\IDC 4.0\4.0\bin\Config
- C:\Program Files\Cisco Systems\IDC 4.0\4.0\bin\IDCUILogs
- C:\Program Files\Cisco Systems\IDC 4.0\4.0\bin\idc.ini
- C:\Program Files\Cisco Systems\IDC 4.0\4.0\bin\idc-gui.ini
- C:\Program Files\Cisco Systems\IDC 4.0\4.0\bin\DeviceGroups.dat
- C:\Program Files\Cisco Systems\IDC 4.0\4.0\bin\Trace\IDCTrace.txt
- C:\Program Files\Cisco Systems\IDC 4.0\4.0\bin\WaveDevices.xml
- C:\Program Files\Cisco Systems\IDC 4.0\Tones
- C:\Program Files\Cisco Systems\IDC 4.0\Users
- C:\Program Files\Cisco Systems\IDC 4.0\Packages

Installation Procedure

Installing Cisco IPICS Dispatch Console involves the two general procedures that the following sections describe:

- [Downloading the Cisco IPICS Dispatch Console installation program from the Cisco IPICS Server, page 2-4](#)
- [Installing the Cisco IPICS Dispatch Console, page 2-4](#)

Downloading the Cisco IPICS Dispatch Console installation program from the Cisco IPICS Server

Before you can install the Cisco IPICS Dispatch Console on a client PC, you must download its installation file from the Cisco IPICS server. To do so, follow these steps:

Procedure

-
- Step 1** From a web browser on the client PC, enter the fully qualified hostname (for example, `ipics1.cisco.com`) or the IP address of the server on which Cisco IPICS is running.
- A fully qualified hostname is preferred. If you enter an IP address and the PC that you are using does not have a valid trust certificate from the server, a pop-up window prompts you to download a certificate. Follow the prompts to do so.
- Step 2** Log in to the Cisco IPICS server.
- The Cisco IPICS Administration Console appears.
- Step 3** On the **Server** tab, choose **Home > Download IDC**.
- Step 4** In the Download IDC page, click **Download IDC**.
- Step 5** In the dialog box that appears, click **Save**.
- Step 6** Use the Save As pop-up window to save the Cisco IPICS Dispatch Console installation program (called `idcsetup.exe`) on your local hard drive.
-

Installing the Cisco IPICS Dispatch Console

After you download the Cisco IPICS Dispatch Console installation program as described in the [“Downloading the Cisco IPICS Dispatch Console installation program from the Cisco IPICS Server”](#) section on page 2-4, perform the following steps to install it on your PC client.

If there is a version of the Cisco IPICS Dispatch Console on the client PC, uninstall it as described in the [“Uninstalling the Cisco IPICS Dispatch Console”](#) section on page 2-6 before you install a new version.

Before you install, review the information in the “[Installation Guidelines](#)” section on page 2-2. Also, make sure that you are logged in to the client PC with Window Administrator privileges or that you have write privileges to the directories that the “[Installation Directories](#)” section on page 2-2 lists.

Step 1 Start the Cisco IPICS Dispatch Console installation program (called `idcsetup.exe`).

To do so, you can either double-click the `idcsetup.exe` shortcut or navigate to the program and double-click it.

The installation program starts and the IDC Setup Wizard appears.

Step 2 In the IDC Setup Wizard, take these actions:

- a. In the Welcome window, click **Next**.
- b. In the Select Installation Folder window:
 - (Optional) Enter a folder in which to install the Cisco IPICS Dispatch Console. Cisco recommends that you use the default folder unless there is a reason to specify another folder.
 - Click the **Everyone** radio button if you want to allow all Windows accounts on the client PC to access the Cisco IPICS Dispatch Console, or click **Just Me** if you want to allow access only by your Windows account.
 - Click **Next**.

c. In the Confirm Installation window, click **Next**.

The Cisco IPICS Dispatch Console installs. A progress bar provides information about this process.

d. In the Installation Complete window, click **Close**.

The installation is complete and an icon for the Cisco IPICS Dispatch Console appears on your PC desktop.

Step 3 If a dialog box asks if you want to install the Cisco Video Surveillance Client, click **Yes**, then take the following actions.

This dialog box appears if the Cisco Video Surveillance Client is not installed already on the client PC. The Cisco IPICS Dispatch Console requires the Cisco Video Surveillance Client to display VSM videos, which are in bwims format.

- a. In the Cisco Video Surveillance Client Setup window, click **Next**.

- b. In the window that asks for the number of cores on your client PC process, enter that number, then click **Next**.

This window provides instructions for determining this number.

- c. In the window that prompt for user information:
 - Enter your name in the Full Name field.
 - Enter your organization name in the Organization field.
 - Click the **Anyone who uses this computer** radio button if you want to allow all Windows accounts on the client PC to access the Cisco Video Surveillance Client, or click **Only for Me** if you want to allow access only by your Windows account.
 - Click **Next**.
- d. In the window that prompts for a destination folder, enter a folder in which to install the Cisco Video Surveillance Client, then click **Next**. Cisco recommends that you use the default folder unless there is a reason to specify another folder.
- e. In the Window that prompts you to begin the installation, click **Next**.
- f. In the window that informs you that the Cisco Video Surveillance Client has been installed, click **Finish**.

Step 4 In the Cisco IDC window, click Yes if you want to start the Cisco IPICS Dispatch Console now, otherwise click No.

Step 5 (Optional) Exit the Cisco IPICS server.

Uninstalling the Cisco IPICS Dispatch Console

Removing (uninstalling) the Cisco IPICS Dispatch Console from a client PC removes the application from the PC. To uninstall the Cisco IPICS Dispatch Console, perform the following steps on the PC.

If you are running the CSA on your client PC and see a CSA access permission dialog box during the uninstallation process, click **Yes** to continue.

Before you uninstall, make sure that you are logged in to the client PC with Window Administrator privileges or that you have write privileges to the directories that the “[Installation Directories](#)” section on page 2-2 lists.


Procedure

-
- Step 1** Choose **Start > Program Files > Cisco Systems > IPICS Dispatch Console 4.0 > Uninstall IPICS Dispatch Console 4.0**.
- Step 2** In the confirmation pop-up window, click **Yes** to continue.
- This IDC is removed from your client PC. This process can take several minutes.
-

WAVE Engine Service Requirements

The Cisco IPICS Dispatch Console requires the WAVE Engine service to be running on the client PC. This service enables the Cisco IPICS Dispatch Console to send, receive, and play audio. The WAVE Engine service is installed and started on a client PC as part of the Cisco IPICS Dispatch Console installation process.

To determine if the WAVE Engine service is running, choose **Start > Control Panel > Administrative Tools > Services**, and make sure that “Started” appears in the status column for the line that includes WAVE Engine in the Extended tab.

If the WAVE Engine service stops, you cannot to send, receive, or play audio on the Cisco IPICS Dispatch Console, and an alert icon  appears for resources in the IDC View area.

If the WAVE Engine service stops, the IDC attempts to restart it. If the restart is successful, you can continue to operate as normal. If the restart is not successful, try exiting and then logging back in to the Cisco IPICS Dispatch Console. This procedure should restart the WAVE Engine service. If it does not, you can restart this service manually.

To restart the WAVE Engine service manually, perform the following procedure. This procedure requires you to be logged in to the client PC as a user with Windows administrator privileges.

Procedure

-
- Step 1** Exit the Cisco IPICS Dispatch Console if it is running.
- Step 2** Choose **Start > Control Panel > Administrative Tools > Services**.
The Services window appears.
- Step 3** In the Extended tab, click the line in the Services list that includes WAVE Engine.
- Step 4** Click **Start** or **Restart**.
- Step 5** Exit the Services window.
-

**Note**

Some Windows security applications do not allow the WAVE Engine service to run or to communicate at the levels that audio processing requires. In this situation, you must modify the settings in the security application to give the WAVE Engine service permission to run with no restrictions.

Cisco IPICS Dispatch Console Logs

The Cisco IPICS Dispatch Console maintains a variety of log files on the client PC. [Table 2-1](#) describes these logs.

**Note**

This table shows these logs in the C:\Program Files folder, which is the default installation folder for the Cisco IPICS Dispatch Console. If you install the Cisco IPICS Dispatch Console in another folder, the log files will be under that folder.

Table 2-1 Cisco IPICS Dispatch Console Logs

Location	File Name	Description
C:\Program Files\Cisco Systems\ Cisco IDC 4.0\4.0\Bin\Trace	IDCTrace <i>n</i> .txt (<i>n</i> may appear, and is a digit 1 through 9, which differentiates up to 10 IDCTrace files)	Contains technical traces information that you can provide to the Cisco Technical Assistance Center for troubleshooting, if needed. When the IDCTrace.txt file reaches a size of 2 MB (by default), the system creates a new file and begins writing log information to it. The new file is named IDCTrace1.txt. When the new file reaches a size of 2 MB, system creates another file, named IDCTrace2.txt. This process continues until the system creates 10 files, by default. When the tenth file reaches a size of 2 MB, the system begins to overwrite files, starting with IDCTrace.txt.
C:\Program Files\Cisco Systems \Cisco IDC 4.0\Users <i>IP_address</i> (<i>IP_address</i> is the IP address of the Cisco IPICS server to which the Cisco IPICS Dispatch Console connected.)	Authentication.log	Contains a history of all user login and logout attempts per Cisco IPICS Dispatch Console installation. This log appears in XML format.

Table 2-1 Cisco IPICS Dispatch Console Logs (continued)

Location	File Name	Description
C:\Program Files\Cisco Systems \Cisco IDC 4.0\Users \IP_address\ SYSTEM\user_name (IP_address is the IP address of the Cisco IPICS server to which the Cisco IPICS Dispatch Console is connected and user_name is your Cisco IPICS user name.)	ChannelActivity.log	Contains a history of activation, deactivation and PTT events for channel, radio, and VTG within the Cisco IPICS Dispatch Console. This log appears in XML format.
	DebugLog.Txt	This log contains detailed debugging information that is relevant to how the IDC operates. Several different debug levels can be enabled. This log appears in text format; it is rotated each time that you execute the IDC application

By default the Cisco IPICS server uploads the Authentication.log and the ChannelActivity.log files at regular intervals. You can configure this process and view these files from the Administration > Options > Client tab in the Server drawer in the Cisco IPICS Administration Console, and you can generate activity log reports from the Cisco IPICS server. For related information, see *Cisco IPICS Administration Guide*.

When the Cisco IPICS Dispatch Console writes to any of the log files, the application checks to make sure that available disk space exists to capture this data. If the amount of free disk space falls below a predefined level, logging activities stop and data that can no longer be written to the disk is lost. When the free disk space increases to sufficient levels, the Cisco IPICS Dispatch Console automatically resumes logging and activities.

All of the logs, except for the debug log, are based on size. The system creates a new log when the predefined limit has been reached.

The following information pertains to the Cisco IPICS Dispatch Console log files:

- The debug log (DebugLog.txt) file starts a fresh log each time you start the Cisco IPICS Dispatch Console.
- By default, the Cisco IPICS system retains one current active copy (DebugLog.txt) of the debug log.
- The Cisco IPICS system writes most error messages to the IDCTracen.txt log.

- The server may request that a log file be uploaded from the Cisco IPICS Dispatch Console whenever a new log file is created based on file size rollover.
- The Cisco IPICS Dispatch Console timestamps all log entries in GMT format. However, it does not synchronize its clock to any central source. Therefore, Cisco recommends that the Cisco IPICS Dispatch Console client PC and the Cisco IPICS server synchronize their clocks to a central source by using Network Time Protocol (NTP).
- The Authentication.log, ChannelActivity.log, ChannelStatistics.log, and UserInterface.log appear in XML format. The Cisco IPICS server parses them and turns them into syslog format, then sends the syslog messages to the router for collection.

Cisco IPICS Dispatch Console Guidelines for Use

Be aware of the following guidelines when you use the Cisco IPICS Dispatch Console:

General Guideline

- When using the push-to-talk (PTT) feature, talk in short bursts and monitor the incoming traffic indicator for a resources so that you do not talk over other Cisco IPICS users.
- To help ensure that Cisco IPICS operates efficiently, your IDC should not have more than 50 channels, radios, and VTGs in any combination powered on at any time, when no incidents are powered on. If one or more incidents are powered on, your IDC should not have more than 36 resources (channels, radios, incidents, and VTGs) in any combination powered on.
- Reboot your client PC at least once a week. This process helps ensure that Microsoft Windows operates efficiently, which in turn helps your IDC operate efficiently.

Connectivity Guidelines

- Before you launch the IDC, establish network connectivity to make sure that you have a valid IP address.

- If the Cisco VPN Client is installed on your client PC, disable the “Stateful Firewall (Always On)” option. Otherwise, SIP and multicast connections may not work correctly.
- You may need to modify your Windows firewall settings so that the IDC can send and receive the required protocols.
- Network limitations may prevent some client PCs from sending audio. In these cases, choose the remote location to connect to Cisco IPICS.
- If you use a docking station or pluggable audio devices with your PC client, exit the IDC and unplug your audio devices before you undock your PC. Otherwise, your PC may become unresponsive and require you to reboot.
- The Cisco IPICS server contains the location information to determine how the IDC should connect. For optimum connectivity and higher quality audio, use the most appropriate location for your connection type when you log in to the IDC. If you choose a location and you do not hear any voice traffic, choose a different location until you hear the audio on the channel.
- If both wired and wireless connections are active, and if you selected a location other than remote, either disable the wireless connection or make sure that the IDC uses the IP address that is assigned to the wired connection.
- To connect the IDC via a SIP-based remote connection, make sure that the IDC can establish connectivity to the RMS router. (The IDC connects to the RMS by using the IP address of the Loopback0 interface that is assigned to the RMS.) If the IDC cannot establish connectivity to the RMS, you may experience channel activation issues (such as fast busy) you they attempt to use a SIP-based remote connection.

Account Lockout and Password Expiration Guidelines

- If you incorrectly enter your IDC password multiple times and exceed the maximum number of consecutive invalid login attempts as configured in the server, your user account may be locked. In this case, the IDC does not allow you to log in to the system. A message displays to alert you to contact your system administrator to unlock your user account.
- If the number of consecutive invalid login attempts has been exceeded while you are already logged in to the IDC, the IDC allows you to continue to use the password for your current session. The IDC does not allow additional logins, however, until your user account is unlocked or your password is reset.

- If the number of consecutive invalid login attempts has been exceeded while you are logged in to the IDC via off-line mode, the IDC allows you to continue to use the password after it returns to on-line mode. The IDC does not allow additional logins, however, until your user account is unlocked or your password is reset.
- If your password has expired, the IDC does not allow you to log in to the system until after you have changed your password. To change your password, log in to the Cisco IPICS server and navigate to **Home > My Profile** to enter your old and new passwords.
- If your password expires while you are logged in to the IDC, the IDC allows you to continue to use the password for your current session. You must change your password before the next login.
- If your password expires while you are logged in via off line mode, the IDC allows you to continue to use the password after the IDC returns to online mode. You must change your password before the next login.

Cisco Security Agent (CSA) Guidelines

If the Cisco Security Agent (CSA) is installed on your client PC, follow these guidelines:

- If you see a CSA access permission dialog box when you try to perform an IDC operation, click **Yes** to grant permission and continue with that operation.
- If you see a CSA access permission dialog box when you activate a channel on the IDC, be sure to click **Yes** to grant permission.
- If you are prompted with a CSA access permission dialog box when you start a new version of the IDC or after a system reboot, make sure that you click **Yes** to allow the IDC to monitor the media device (microphone). If you allow the CSA to time out based on its default value of No after you launch the IDC, the IDC will be able to receive voice traffic but it will not be able to send voice traffic.
- If the CSA “Don’t ask me again” check box displays as an option, you may check it to instruct CSA not to prompt you again.

Optimizing Audio for the Cisco IPICS Dispatch Console

After you install the Cisco IPICS Dispatch Console, check the settings for playback and recording audio devices on your client PC to ensure that you are using the preferred or default sound devices with the Cisco IPICS Dispatch Console. The following sections guide you through the audio configuration. They also provide information about properly using a USB DSP headset and microphone.

- [Using a USB DSP Headset with the Cisco IPICS Dispatch Console, page 2-14](#)
- [Using a Microphone with the Cisco IPICS Dispatch Console, page 2-15](#)
- [Voice Quality Guidelines, page 2-16](#)

Be aware that if the microphone on the client PC is busy, or if it cannot be opened by the Cisco IPICS Dispatch Console for other reasons, you can listen to active conversations but you will not be able to talk.

If you change your audio settings while you are running the Cisco IPICS Dispatch Console, you may need to exit then restart the Cisco IPICS Dispatch Console for the changes to become effective.

Using a USB DSP Headset with the Cisco IPICS Dispatch Console

When you use a USB DSP headset (that is, a headset that includes its own sound card) with the Windows operating system, Windows may configure that headset as the default speaker and microphone. Therefore, make sure that you connect the USB DSP headset to the client PC before you launch the Cisco IPICS Dispatch Console.

If you launch the Cisco IPICS Dispatch Console after you plug the headset into your PC client, the Cisco IPICS Dispatch Console may not automatically remember the audio setting for the USB DSP headset and may revert to the default Windows operating system audio settings.

**Note**

If you use the microphone on a USB headset for an extended time, your voice may become unintelligible. If this problem occurs, close the Cisco IPICS Dispatch Console and unplug the Cisco IPICS Dispatch Console headset from the client PC. Then, plug the USB headset back into the client PC and restart the Cisco IPICS Dispatch Console.

Using a Microphone with the Cisco IPICS Dispatch Console

Cisco IPICS might be configured to use voice activity detection to squelch (silence) transmissions that contain undetectable speech. If the Cisco IPICS system cannot detect your voice when you transmit, the system may squelch the transmission. In this situation, another Cisco IPICS user may start speaking over your transmission because your voice cannot be heard and the Cisco IPICS Dispatch Console receive indicator for the listener may not display any indication of the transmission.

To avoid issues that may arise from incomplete transmissions, follow these guidelines, make sure that you use a high-quality microphone with the Cisco IPICS Dispatch Console. In addition, check the placement and settings of your microphone before you begin using the Cisco IPICS Dispatch Console.

If you encounter a situation in which you can hear other users but they cannot hear you, make sure that your microphone is not set to mute.

To check the audio recording and playback capability of a microphone on your client PC, perform the following steps to access the Windows Sound Recorder to record your voice and then listen to the recording. (Make sure that you have an audio input device connected to your PC.)

Procedure

Step 1 Choose **Start > Program Files > Accessories > Entertainment > Sound Recorder**.

The Sound Recorder dialog box appears.

Step 2 Click **File > New**.

Step 3 To begin recording, click the **Record** button.

This button appears in the lower right corner of the Sound Recorder dialog box.

- Step 4** Speak into the microphone to record your voice.
- Step 5** To stop recording, click the **Stop** button.
- Step 6** Take either of these actions:
- To listen to your recording, click the **Play** button. You should hear your voice as it was recorded.
 - Alternatively, you can choose **File > Save as** and then enter a file name to save your recording file. Recorded sounds are saved as waveform (.wav) files. To play the file, choose **File > Open**, locate the sound file that you want to play, then, double-click the file.
- Step 7** To stop playing the recording, click the **Stop** button.
-

Voice Quality Guidelines

The following tips can help to ensure good voice quality when you use the Cisco IPICS Dispatch Console:

- Make sure that you use a high-quality headset and microphone, and check the placement and settings of both components. A high-quality and properly-configured headset can greatly enhance voice quality for both receive and transmit activity.
- The use of a PC analog sound card or the use of the analog ports on most laptop computers typically results in lower quality voice transmissions. Therefore, Cisco recommends that you do not use your PC sound card or analog ports as an alternative to a high-quality headset and microphone.
- For enhanced voice quality, make sure that you plug your USB headset or audio device into a dedicated USB port instead of a USB hub. The use of USB hubs, which multiplex data from USB devices into one data stream, can result in timing issues and can affect voice quality.
- If other Cisco IPICS users tell you that they hear a persistent or intermittent noise, such as an audible hum, when you talk, the problem may be due to defective headset hardware. In this situation, Cisco recommends that you isolate the source of the audio quality issue by replacing the defective headset with a new, high-quality headset.

- Check your Windows audio settings to make sure that the volume is not set too low. If the volume is set low, increase the input gain on your microphone by sliding the bar up on the volume controls to increase the volume.
- For optimum connectivity, use the most appropriate location for your connection type when you log in to the Cisco IPICS Dispatch Console. For example, if you are using a wireless connection, choose the location that correlates to wireless connectivity for your organization. You can ensure higher quality audio by choosing the appropriate connection type.
- Be aware that a slow-speed connection, such as a digital subscriber line (DSL) or any slow wired link, may affect voice quality. If possible, try to use a high-speed connection with the Cisco IPICS Dispatch Console.
- Try to limit the use of applications that consume significant CPU and network bandwidth on a client PC when you use the Cisco IPICS Dispatch Console. If your CPU is overburdened by other programs, there may insufficient CPU cycles for the Cisco IPICS Dispatch Console to run properly. Check the CPU activity on your client PC and close any programs that do not need to be open.

