CHAPTER 1

Overview

The Cisco IPICS Dispatch Console is a component of the Cisco IP Interoperability and Collaboration System (IPICS) that installs and runs on a client (standalone) PC. It is a graphical-based application that allows you to communicate with other users via radio, telephone, mobile device, or PC. It also lets you participate in virtual talk groups (VTGs) and incidents, and manage and operate a variety of resources (including channels, radios, incidents, and VTGs), and perform a variety of other activities.

In addition, users with the Cisco IPICS Dispatcher or All roles can use the Cisco IPICS Dispatch Console to create VTGs and incidents, activate a Cisco IPICS policy, and place and patch telephone calls.

The Cisco IPICS Dispatch Console also provides access to the IPICS Connect features, which enables you to make private and group radio calls and send alerts to Nextel radios.

This chapter provides an overview of Cisco IPICS Dispatch Console operations and explains how to perform some common tasks. It includes these topics:

Client PC

A client PC is a PC on which you install and operate the Cisco IPICS Dispatch Console. For information about minimum requirements for a client PC, see *Cisco IPICS Compatibility Matrix*.

The following guidelines apply to a client PC:

- Make sure that the WAVE Engine service on the client PC is running. This service is installed and started on a client PC when you install the Cisco IPICS Dispatch Console. For related information, see the "WAVE Engine Service Requirements" section on page 2-7.
- The .NET framework 3.5 SP1 or later must be installed on the client PC.
- Configure any security programs that run on the client PC, including the Cisco Security Agent (CSA), to trust the Wave Engine service (WaveEngine.exe) and the RunIDC.exe process.
- Cisco recommends that the Windows time service on a client PC be synchronized with a network time protocol (NTP) server that is synchronized with the Cisco IPICS server that the Cisco IPICS Dispatch Console connects to.
- To view video from an incident on a client PC (except Cisco Video Surveillance Manager videos that are in bwims format), the VLC media player must be installed on the client PC. Videos in bwims format require the Cisco Video Surveillance Client, which you can install as part of the Cisco IPICS Dispatch Console process.
- A client PC should not run any voice or Voice over IP (VoIP) applications when you are running the Cisco IPICS Dispatch Console.
- Only one instance of the Cisco IPICS Dispatch Console can be open on a client PC at a time. Any number of valid Cisco IPICS users can use the same Cisco IPICS Dispatch Console on a client PC, but not concurrently.

Starting the Cisco IPICS Dispatch Console

To start the Cisco IPICS Dispatch Console, perform the following steps on a client PC.

Before logging in, review these guidelines:

- The Cisco IPICS system supports one instance of the IDC application on the client PC at a time.
- If you need to log in to the IDC on a client PC that already has another IDC user logged in, the first user must log out.
- Any number of valid Cisco IPICS users can use the same IDC application, but not concurrently.
- 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.
- To ensure that a radio operates properly, log in to the Cisco IPICS Dispatch Console using the same location as the radio. If you log in from another location, serial radio controls do not work from the Cisco IPICS Dispatch Console (although you can access serial controls from the Serial Radio Control Interface (SRCI) as described in the "Radio Details Tab for Serial Control Radios" section on page 3-26), and tone controls have limited functionality. For related information, see the "Managing Radios and Radio Descriptors" chapter in *Cisco IPICS Administration Guide.*

Procedure

Step 1 Take either of these actions:

- Double-click the Cisco IPICS Dispatch Console icon on your Windows desktop.
- Choose **Start > Programs > Cisco Systems > IPICS Dispatch Console 4.0 > IPICS Dispatch Console 4.0**.

If network security software, such as the Cisco Security Agent (CSA), is installed on your client PC and you are prompted with an access permission dialog box, click **Yes** to grant permission to allow the Cisco IPICS Dispatch Console to

monitor the media device (microphone). If the "Don't ask me again" check box appears as an option, you may check it to instruct the security software not to prompt you again.

Note Be aware that if you allow the CSA to time out based on its default value of No, the Cisco IPICS Dispatch Console may not be able to receive or send traffic, or it may be able to receive traffic only. In this case, you can listen to any active conversations but you will not be able to transmit.

The Cisco IPICS Dispatch Console login screen appears.

Step 2 If a pop-up window prompts you to download a certificate, follow the on-screen prompts to do so.

You are prompted to install a certificate when you try to connect to the Cisco IPICS server for the first time and the client PC does not have a valid trust certificate from the server.

Step 3 In the Cisco IPICS Dispatch Console log in screen, take these actions:

a. In the Server field, enter the IP address or host name of a Cisco IPICS server to connect to.

b. In the User Name field, enter your Cisco IPICS user name.

c. In the Password field, enter your Cisco IPICS password.

d. Click **OK**.

Step 4 If a Recommended Upgrade dialog box appears or a Mandatory Upgrade dialog box appears, take one of the following actions.

One of these dialog boxes appears if the system detects that there is a Cisco IPICS Dispatch Console upgrade available. The Recommended Upgrade dialog box appears gives you the option of upgrading, and the Mandatory Upgrade dialog box appears which requires you to upgrade.

- To perform an upgrade:
  a. Click **Yes**. The Cisco IPICS Server Authentication window appears.
  b. Uninstall the Cisco IPICS Dispatch Console as described in the "Uninstalling the Cisco IPICS Dispatch Console" section on page 2-6.
  c. Follow the instructions in the "Installation Procedure" section on page 2-3.

- For a recommended upgrade, if you do not want to perform the upgrade now, click **No** and continue with the log in process.

For related information, see the "About Upgrades" section on page 1-10.

Step 5 If a dialog box prompts whether you want to download an alert tone package, either follow the on-screen prompts to do so or exit this window.

This dialog box appears if the system detects that an alert tone package is available. If you download it, the alert tones become available for your Cisco IPICS Dispatch Console.

Step 6 In the Select your Location screen, take these actions:

a. (Optional) In the Location field, choose the location to which you want to connect.

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. A remote connection always uses G.729 (compressed) codec, so a connection of this type has a slightly reduced audio quality. A remote connection uses SIP-based trunking into the RMS component, which is directly tuned into the multicast channel.

b. If the IDC Version field is blank, click Cancel to exit the log in process, then install a supported version of the Cisco IPICS Dispatch Console as described in the "Installing the Cisco IPICS Dispatch Console" section on page 2-1.

c. Click **OK**.

The Cisco IPICS Dispatch Console appears.

Exiting the Cisco IPICS Dispatch Console

To exit the Cisco IPICS Dispatch Console, choose **File > Close**, then click **OK** to confirm. This process logs you out of the Cisco IPICS Dispatch Console and closes the application. Any patches or calls that you established through the Cisco IPICS Dispatch Console are torn down when you exit.

Cisco IPICS Dispatch Console License Types

Cisco IPICS Dispatch Console can be run under either a Silver user license or a Platinum user license. The system determines the license type automatically when you log in to the Cisco IPICS Server from the Cisco IPICS Dispatch Console, based on the number of concurrent licenses available and your Cisco IPICS user role. Licenses grant access to Cisco IPICS Dispatch Console features and functions as follows:

- Platinum user license—Provides access to all Cisco IPICS Dispatch Console features.
- Silver user license—Provides access to all features except the VTGs tab and the Incidents tab in the Items Tabs area. Therefore, a Silver user license does not allow adding an incidents or VTGs. (Figure 3-1 on page 3-2 illustrates the Items Tab area for a Platinum User license.)

When the Cisco IPICS Dispatch Console starts, licences are granted as follows:

- A user with the Cisco IPICS Dispatcher role or All role is granted a Platinum user license, if Platinum user licenses are available. If no Platinum user licenses are available, this user is granted a Silver license. If neither license type is available, this user cannot start the Cisco IPICS Dispatch Console until licenses become available.
- A user with a Cisco IPICS role other than Dispatcher or All is granted a Sliver user license, if Silver user licenses are available. If no Silver licenses are available, this user cannot start the Cisco IPICS Dispatch Console until a Silver user licenses become available.

For additional information about Silver and Platinum user licenses, including how to determine how many licenses are available, see *Cisco IPICS Administration Guide*.

Cisco IPICS Dispatch Console Operating Modes

The Cisco IPICS Dispatch Console can function in either of these operating modes:

- On-line mode—The Cisco IPICS Dispatch Console has a connection to the Cisco IPICS server. In this mode, radio, channel, and dial communication features function normally. In addition, the Cisco IPICS Dispatch Console

polls the Cisco IPICS server at regular intervals to determine if updates have been made on the server to configurations, VTGs, incidents, and more. If updates have been made, information and displays in the Cisco IPICS Dispatch Console updates, based on information that the server provides.

- Off-line mode—The Cisco IPICS Dispatch Console does not have connection to the Cisco IPICS server. In this mode, radio and channel communication functions, but the Cisco IPICS Dispatch Console does not receive updates from the Cisco IPICS server.

  If the connection from the Cisco IPICS Dispatch Console to the Cisco IPICS is restored server within 15 minutes (by default) after the connection is lost, the Cisco IPICS Dispatch Console goes into on-line mode automatically. If the connection is restored after 15 minutes, a pop-up message informs you that you must log in to the server to go back to on-line mode. Click OK to log in. (You can change this default 15-minute period by updating the **Logout Client After** option in the Cisco IPICS Administration Console.)

You can determine the operating mode by looking at the Cisco IPICS Dispatch Console operating mode indicator. This indicator appears in the System Information area at the bottom right of the Cisco IPICS Dispatch Console Main window, as shown in Figure 3-35 on page 3-93. (If you cannot see the System Information area, click the **Show** button  at the bottom of the Cisco IPICS Dispatch Console Main window, directly under the Cisco logo.) The indicator can appear as follows:

-  —Green indicates that the Cisco IPICS Dispatch Console is in on-line mode
-  —Red indicates that the Cisco IPICS Dispatch Console is in off-line mode

The following guidelines apply to off-line mode:

- You must have at least one successful login from the IDC to the Cisco IPICS server before you can use the IDC in offline mode.
- After the Cisco IPICS server returns to an on-line state, you may encounter an invalid user or password error when you try to log in to the IDC. This situation may occur if the IDC attempts to connect to the server while the server database is being restored.

- If the RMS entries are changed while you are running the IDC, your SIP-based channels may become disconnected. The IDC retrieves the updated channel list, with the newly-allocated SIP channels, after successful login to the server.

Cisco IPICS Dispatch Console Features Available by User Type

The features that are available in the Cisco IPICS Dispatch Console depend on your Cisco IPICS role. A user with the Cisco IPICS Dispatcher role or All role can access all features (if granted a Platinum user license, as described in the "Cisco IPICS Dispatch Console License Types" section on page 1-6). A user with a Cisco IPICS role other than Dispatcher or All cannot access all features.

The following Cisco IPICS Dispatch Console features are unavailable or restricted based on the Cisco IPICS user role:

- Items Tabs area:
  - VTGs tab—Only users with the Dispatcher role or All role and a Platinum User license can access this tab. Therefore, only these users can add a VTG.
  - Incidents tab—Only users with the Dispatcher role or All role and a Platinum User license can access this tab. Therefor, only these users can add an incident.
  - Policies tab—Users with the Dispatcher role or All role see all policies that are configured in the Cisco IPICS Administration Console. Other users see only policies with which they are associated.
- VTG Details tab—Only user with the Dispatcher role or All role can access this tab. Therefore, only these users can update VTG resources of features.
- Incident Details tab—Users with the Dispatcher role or All role can use all features on this tab. Other users can add journals, images, and videos only.
- Dial Pad and Channel Patch area—Only users with the Dispatcher role or All role can see this area.

Understanding Incidents

An incident is an event that you create in the Cisco IPICS Dispatch Console and for which various users can coordinate responses by using the Cisco IPICS Dispatch Console. The Cisco IPICS Dispatch Console provides the ability to respond to incidents by managing the resources within an incident.

An incident can be any event, such as a fire or other situation, that requires a response. Resources include channels, radios, VTGs, and users that work together to respond to an incident. Incident participants can upload and share journals (text entries), images, and videos that relate to the incident.

You use the Cisco IPICS Dispatch Console to create an incident. When you do so, the incident is added to the list of incidents on the Cisco IPICS server (if the Cisco IPICS Dispatch Console is in on-line mode) and the incident is put in active state on the server. In addition, the user who created the incident is added to the incident as a resource. An active incident is one that you can access on the Cisco IPICS Dispatch Console, to which you can add or remove resources, and for which you can perform other activities.

However, participants in an incident cannot communicate with each other via the incident resources until you activate the *incident VTG* for the incident. An incident VTG is a temporary talk group for an incident. When it is activated, the following events occur:

- An internal VTG is created on the Cisco IPICS server, which the server uses to enable communication for the incident. An incident VTG does not appear in the list of regular VTGs on the Cisco IPICS server.
- All resources for audio capabilities (channels, radios, other VTGs) are added to the incident VTG.
- Cisco IPICS enables other system resources to allow communication via the VTG.

You can activate and deactivate an incident VTG as needed from the Cisco IPICS Dispatch Console. When an incident VTG is deactivated, you can still add and remove resources for the incident. Deactivating an incident VTG does not deactive the incident from the Cisco IPICS server. To deactivate an incident (so that it no longer appears in the Cisco IPICS Dispatch Console) use the Cisco IPICS Administration console.

Using the Cisco IPICS Dispatch Console in a High Availability Deployment

High availability (HA) is an optional feature for Cisco IPICS that allows a secondary server to take over automatically and without interrupting communication if a primary Cisco IPICS server fails.

To enable the Cisco IPICS Dispatch Console to take advantage of HA, log in to the active Cisco IPICS server from the Cisco IPICS Dispatch Console after you configure HA on the server. If you have never logged in to the primary Cisco IPICS server and a secondary is the active server due to a failover, log in to the secondary server

The Cisco IPICS Dispatch Console works as follows in an HA environment:

- If you are logged in to the primary Cisco IPICS server from the Cisco IPICS Dispatch Console and a failover occurs, the Cisco IPICS Dispatch Console connects to the secondary server automatically. If a secondary server not available, the Cisco IPICS Dispatch Console goes into off-line mode.
- If you log into to the primary Cisco IPICS server from the Cisco IPICS Dispatch Console after a failover has occurred, the login redirects automatically to the secondary server.

After a failover or fallback, there may be a break of up to a few seconds in the audio on your Cisco IPICS Dispatch Console.

About Upgrades

Cisco IPICS is operates with specific versions of the Cisco IPICS Dispatch Console. When you start the Cisco IPICS Dispatch Console, Cisco IPICS checks the Cisco IPICS Dispatch Console version that you are using. If an upgrade is available, the Cisco IPICS Dispatch Console prompts you to upgrade.

There are two types of upgrades:

- Recommended—For these upgrades, the Cisco IPICS Dispatch Console gives you the option of performing the upgrade. If you decline, you can continue to work with the existing version.
- Mandatory—For these upgrades, you must perform the upgrade before you can use the Cisco IPICS Dispatch Console.