Overview

This chapter provides an overview of the Cisco IPICS software installation. It also contains information about system requirements for the Cisco IPICS server software and the Cisco IPICS Dispatch Console (IDC) application.

This chapter includes the following sections:

Installation Overview

You can install the Cisco IPICS software under the VMware ESX or ESXi virtual machine (VM) that runs on a supported Cisco UCS device.

For information about supported devices, see *Cisco IPICS Compatibility Matrix* at http://www.cisco.com/en/US/products/ps6718/products_device_support_tables_list.html.

The software that installs the Cisco IPICS server software is mostly automated, but it does require some user interaction to complete.

Table 1-1 describes the general steps that you need to perform to set up the installation of the Cisco IPICS server software.

Table 1-1 Cisco IPICS Server Software Setup

Step	Description
1. End user license agreement	This window displays the end user license agreement for the Cisco IPICS server software. You must accept this agreement to continue with the installation.
2. Password creation for the ipics user	This procedure permits you to create a password for the ipics user, who performs all administrative tasks in the Cisco IPICS Administration Console.

Table 1-1 Cisco IPICS Server Software Setup (continued)

Step	Description
3. Password creation for the ipicsadmin user	This procedure enables you to create a password for the ipicsadmin user, who has the Cisco IPICS operating system privileges that are related to the database server files and folders.
4. Package installation	This window displays the progress of the installation and the Cisco IPICS files that the installer writes to the server. This installation also installs the Cisco IPICS policy engine (hereafter referred to as *policy engine*).
5. Uninstaller creation	This procedure creates a utility to uninstall the Cisco IPICS software.
6. Option to restart the server	This procedure allows you to choose between restarting the server immediately or at a later time.

For more information about the steps that you need to follow to install the Cisco IPICS server software, see the "Installing the Cisco IPICS Server Software" section on page 2-6.

Installed Components

The Cisco IPICS installation includes the Cisco IPICS server software, with the following components:

- Cisco IPICS Administration Console
- Cisco IPICS Data Store (IBM Informix Dynamic Server)
- Cisco IPICS Web Application Server (tomcat service)

System Requirements

For the list of hardware and software components that Cisco supports for use with Cisco IPICS, see *Cisco IPICS Compatibility Matrix* at http://www.cisco.com/en/US/products/ps6718/products_device_support_tables_list.html.

Hardening

When you install Cisco IPICS, the Universal Media Services (UMS), the Cisco IPICS ISSI Gateway (ISSIG), or the Cisco Digital Fixed Station Interface Gateway (DFSIG), standard US Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) methodology is applied automatically to the server on which you install the software component.

You can optionally apply the following hardening features:

- DISA STIG GEN000980—Allows the server root account to be logged in to from only from the system console

- DISA STIG GEN001120—Prevents logging in to the server as root from an encrypted remote access program, such as SSH
- DISA STIG GEN002960—Enables the cron.allow and cron.deny files to control access to the cron utility
- DISA STIG GEN006620—Configures the access control program to grant system access to and deny system access from specific hosts

To apply these additional hardening features, after you install a Cisco IPICS software component, log in to the server as the root user and enter these commands:

[root]# **cd /usr/local/bin/stig**

[root]# **./stig-execute -f PDI-DB_harden_root**

To remove these additional hardening features from a server, log in to the server as the root user and enter these commands:

[root]# **cd /usr/local/bin/stig**

[root]# **./stig-execute -u**