



Data Migration Assistant User Guide

Release 5.0(2)

This document describes the Data Migration Assistant (DMA), explains how to install and use it, and provides related information.

Use this document if you are running Cisco Unified CallManager 4.0 or 4.1 and are ready to upgrade to Cisco Unified CallManager 5.0.

This document includes the following topics:

- [Overview of DMA](#)
- [Obtaining DMA](#)
- [Installing DMA](#)
- [Uninstalling DMA](#)
- [Using DMA](#)
- [Migrating CAR Data](#)
- [Migrating Cisco Unified CallManager Attendant Console Data](#)
- [Migrating Existing CAPF 1.0\(1\) Data](#)
- [Copying CAPF 1.0\(1\) Data from a 4.0 Subscriber Server to the 4.0 Publisher Database Server](#)
- [Generating a New CAPF Certificate](#)
- [Running DMA](#)
- [DMA Backup Information File](#)
- [Administering and Troubleshooting DMA](#)
- [Obtaining Documentation](#)
- [Documentation Feedback](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

Overview of DMA

DMA migrates data for Cisco Unified CallManager, as specified in the following sections.

Data Migration

DMA assists you with the first step in migrating Cisco Unified CallManager 4.0 or 4.1 data to Cisco Unified CallManager 5.0 by backing up Cisco Unified CallManager 4.0 or 4.1 data in a format that Cisco Unified CallManager 5.0 can read. Cisco Unified CallManager 4.0 and 4.1 run in a Windows environment, and Cisco Unified CallManager 5.0 runs in a Linux environment, so DMA exports Windows-based data to a format that Linux can import. The Cisco Unified CallManager 5.0 installation process converts the backed up data as needed for Cisco Unified CallManager 5.0, which completes the data migration.

DMA saves the data that it exports in a tape archive (tar) file in a location that you specify.

You must install and run DMA on the Cisco Unified CallManager publisher server before you upgrade to Cisco Unified CallManager 5.0. If you make any Cisco Unified CallManager configuration changes after running DMA, the system does not retain these changes when you upgrade.

In addition to exporting Cisco Unified CallManager data, DMA exports data for these related applications:

- Cisco Unified CallManager Attendant Console (AC)
- Cisco Extension Mobility (EM)
- CDR Analysis and Reporting (CAR)
- Certificate Authority Proxy Function (CAPF)
- Certificate Trust List (CTL)
- International Dial Plan (IDP)

DMA does not export this information:

- Custom Music on Hold (MOH) files—You must reapply these files after you upgrade to Cisco Unified CallManager 5.0.
- TFTP phone load files—You must reapply these files after you upgrade to Cisco Unified CallManager 5.0.
- Files on Cisco Unified CallManager subscriber servers—Subscriber servers obtain required information from the publisher server as part of the Cisco Unified CallManager upgrade process.

Obtaining DMA

If you do not have DMA software on a disk, perform the following steps to download it to the Cisco Unified CallManager publisher server. Only a registered user of Cisco.com can download this software.

Procedure

-
- Step 1** Go to this URL:
<http://cco/cgi-bin/tablebuild.pl/cmva-3des>
- Step 2** Select DMA file.
- Step 3** Follow the onscreen prompts and provide the required information to download the software.
-

Installing DMA

This section provides detailed installation information and instructions for DMA. It includes the following topics:

- [Preinstallation Guidelines and Procedures, page 3](#)—Review this information before you install DMA.
- [DMA Installation Procedure, page 4](#)—Follow these steps to install DMA.

Preinstallation Guidelines and Procedures

Review the following guidelines and perform the appropriate procedures before you install DMA:

- Ensure that Cisco Unified CallManager 4.0 or 4.1 is installed and configured as the publisher on the server before you install DMA on that server.



Note DMA installation wizard checks for the presence of Cisco Unified CallManager publisher. You cannot install DMA unless Cisco Unified CallManager has been previously installed on the server.

- Do not use Terminal Services to install DMA.
- You can use Virtual Network Computing (VNC) to install DMA. For more information about VNC, refer to the latest version of *Using Virtual Network Computing*, which is available at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/vnc/index.htm
- Disable the Cisco Security Agent for Unified CallManager (CSA), if it is enabled.



Note In some cases, you may have to uninstall CSA before you can run DMA. If you have difficulties, contact Cisco support for more information.

Make sure to enable the CSA after you complete the installation.

For instructions on disabling and enabling the CSA, refer to *Installing Cisco Security Agent for Unified CallManager*, which is available at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/csa/index.htm

DMA Installation Procedure

To install DMA, perform the following steps.

This procedure should take about 20 minutes to complete.

Before you install DMA, make sure to review the information in the [“Preinstallation Guidelines and Procedures”](#) section on page 3.

**Note**

If you have an earlier version of DMA installed, you must uninstall it before you can install another version. See the [“Uninstalling DMA”](#) section on page 5 for more information.

Procedure

Step 1 Log in to the server as the Windows Administrator.

Step 2 Take one of these actions:

- If you have a DMA installation disk, insert the disk.
- If you have downloaded DMA, go to the folder in which you saved DMA and double-click **DMASetup.exe**.

After preparing to install, DMA Welcome window displays.

Step 3 In DMA Welcome window, click **Next**.

The License Window displays.

Step 4 Accept the license agreement and click **Next**.

The Ready to Install the Program window displays.

Step 5 In the Ready to Install window, click **Install**.

The installation begins. The Installing Data Migration Assistant window shows you the status as the installation proceeds.

After about 20 minutes, the InstallShield Wizard Completed window displays.

Step 6 In the InstallShield Wizard Completed window, click **Finish**.

You are prompted to restart the server.

Step 7 To restart the server, click **Yes**.

The server restarts, and DMA installation completes.

Uninstalling DMA

To uninstall DMA, follow these steps:

Procedure

-
- Step 1** Choose **Start > Settings > Control Panel > Add/Remove Programs**.
- Step 2** From the Add/Remove Programs Window, choose **Cisco Data Migration Assistant**.
- Step 3** Click **Remove**.
-

Using DMA

The following sections describe how to use DMA to export data:

- [Before You Begin, page 5](#)—Perform these procedures before you start DMA.
- [Running DMA, page 8](#)—Follow these steps to run DMA and export data.

Before You Begin

Before you start DMA, perform the procedures that are shown in [Table 1](#).

Table 1 **Procedures to Follow Before Running DMA**

Procedure	Reference
Use the Cisco Unified CallManager Backup and Restore Utility to back up your data. You can use the BARS backup to fall back to your current software version, if necessary.	Refer to the appropriate version of <i>Cisco Unified CallManager Backup and Restore Utility Administration Guide</i> and related documentation at this URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Cisco recommends that you use the Cisco Unified CallManager Upgrade Utility to verify that your system is in a good state before the upgrade	Refer to the appropriate version of <i>Using Cisco Unified CallManager Upgrade Utility</i> at this URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
To back up CAR data, ensure the CAR plugin is installed on the publisher server	See the “ Migrating CAR Data ” section on page 6.
If you use Cisco Unified CallManager Attendant Console, ensure the required files are present on the publisher server.	See the “ Migrating Cisco Unified CallManager Attendant Console Data ” section on page 6.
Copy CAPF data from the subscriber servers to the publisher server.	See the “ Migrating Existing CAPF 1.0(1) Data ” section on page 6.

Migrating CAR Data

Before you can back up Cisco CDR Analysis and Reporting (CAR) data, you must ensure that the CAR plugin is installed on the publisher server. If the CAR plugin is not installed, navigate to **Application>Install Plugins** and install the CAR plugin. For more information, see the *Cisco Unified CallManager Administration Guide* or the *Cisco Unified CallManager Serviceability Administration Guide*.

**Note**

If you do not have to carry over your CDR records to Cisco Unified CallManager 5.0, Cisco recommends that you purge the CDR records before you run DMA.

Migrating Cisco Unified CallManager Attendant Console Data

If you use Cisco Unified CallManager Attendant Console, make sure that the following files exist on the publisher server before you run DMA. If the files do not exist on the publisher, copy them to the publisher from the subscriber server before you run DMA.

- C:\Program Files\Cisco\CallManagerAttendant\bin\CorporateDirectory.txt
- C:\Program Files\Cisco\CallManagerAttendant\etc\acserver.properties
- C:\Program Files\Cisco\CallManagerAttendant\etc\DialRules.xml

Migrating Existing CAPF 1.0(1) Data

**Caution**

Failing to perform the tasks that are described in this section may cause a loss of CAPF data. Use the following information in conjunction with the [“Copying CAPF 1.0\(1\) Data from a 4.0 Subscriber Server to the 4.0 Publisher Database Server”](#) section on page 7.

For information on using CAPF with Cisco Unified CallManager 5.0, refer to the *Cisco Unified CallManager Security Guide*.

Review the following details before you upgrade to Cisco Unified CallManager 5.0:

- Upgrades from Cisco Unified CallManager 4.0 where CAPF was installed on the Cisco Unified CallManager 4.0 publisher database server—If you performed certificate operations with Cisco Unified CallManager 4.0 and CAPF 1.0(1) ran on the publisher database server, the latest operation status migrates to the Cisco Unified CallManager 4.1 database.
- Upgrades from Cisco Unified CallManager where CAPF was installed on a Cisco Unified CallManager 4.0 subscriber server—If you performed certificate operations with Cisco Unified CallManager 4.0 and CAPF 1.0(1) ran on a subscriber server, you must copy the CAPF data to the 4.0 publisher database server before you upgrade to Cisco Unified CallManager 5.0.

**Caution**

If you fail to copy the data prior to the Cisco Unified CallManager 5.0 upgrade, the CAPF data on the Cisco Unified CallManager 4.0 subscriber server does not migrate to the Cisco Unified CallManager 5.0 database, and a loss of data may occur. If a loss of data occurs, the locally significant certificates that you issued with CAPF utility 1.0(1) remain in the phones, but CAPF 5.0 must reissue the certificates, which are no longer valid.

- Upgrades from one release of Cisco Unified CallManager 4.1(x) to Cisco Unified CallManager 5.0—The upgrade automatically migrates the CAPF data.

Copying CAPF 1.0(1) Data from a 4.0 Subscriber Server to the 4.0 Publisher Database Server

**Caution**

If you installed CAPF utility 1.0(1) on a Cisco Unified CallManager 4.0 subscriber server, you must copy the CAPF data to the 4.0 publisher database server before you upgrade to Cisco Unified CallManager 5.0. Failing to perform this task causes a loss of CAPF data; for example, you may lose the phone record files in C:\Program Files\Cisco\CAPF\CAPF.phone. If a loss of data occurs, the locally significant certificates that you issued with CAPF utility 1.0(1) remain in the phones, but CAPF 5.0 must reissue the certificates because the certificates are not valid.

Use the following procedure in conjunction with the [“Migrating Existing CAPF 1.0\(1\) Data”](#) section on page 6. To copy the files, perform the following procedure:

Procedure

- Step 1** Copy the files in [Table 2](#) from the machine where CAPF 1.0 is installed to the publisher database server where Cisco Unified CallManager 4.0 is installed:

Table 2 Copy from Server to Server

Files to Copy	From Machine Where CAPF 1.0 Is Installed	To Publisher Database Server Where Cisco Unified CallManager 4.0 Is Installed
*.0	in C:\Program Files\Cisco\CAPF	to C:\Program Files\Cisco\Certificates
CAPF.phone	in C:\Program Files\Cisco\CAPF	to C:\Program Files\Cisco\CAPF
CAPF.config files	in C:\Program Files\Cisco\CAPF	to C:\Program Files\Cisco\CAPF

- Step 2** Upgrade every server in the cluster to Cisco Unified CallManager 5.0.
- Step 3** After you upgrade the cluster to Cisco Unified CallManager 5.0, perform the following tasks before you use the phones:
- Delete the existing Cisco CTL client.

- b. Install the latest Cisco CTL client by choosing **Application->Plugins** in Cisco Unified CallManager Administration.
- c. Configure the client to create or update the CTL file.



Tip For information on installing and configuring the Cisco CTL client, refer to the *Cisco Unified CallManager Security Guide*.

The Cisco CTL client copies the CAPF certificate to all the servers in the cluster.

- Step 4** Uninstall the CAPF utility that you used with Cisco Unified CallManager 4.0.
- Step 5** See the [“Generating a New CAPF Certificate” section on page 8](#).

Generating a New CAPF Certificate

The Certificate Authority Proxy Function includes its own certificate and private key that is used for authentication. If the CAPF certificate or private key does not exist, for example, after you delete the CAPF 1.0(1) utility, perform the following procedure:

Procedure


- Step 1** Save the current copy of the CAPF.cer file that exists in /usr/local/cm/.security/certs to a location that you will remember.
- Step 2** Delete the CAPF.cer file that exists in /usr/local/cm/.security/certs.
- Step 3** In Cisco Unified CallManager Serviceability, stop and start the Cisco Certificate Authority Proxy Function (CAPF) service.
- Step 4** Update the CTL file; then, reboot all servers in the cluster.
- Step 5** Verify that the phone downloaded the updated CTL file.

Running DMA

To run DMA on a Cisco Unified CallManager publisher server, perform the following steps. Before you start DMA, make sure to review the information in the [“Before You Begin” section on page 5](#).

Procedure

- Step 1** Choose **Start > Programs > Cisco DMA > DMAAdmin**.
- Step 2** When prompted, log in as the Windows Administrator.
The Data Migration Assistant Home page displays.
- Step 3** From the Data Migration Assistant menu bar, choose **Backup > Storage Location**.
The Backup Storage Location page displays.

- Step 4** In the Backup Storage Location page
- a. Choose the destination where DMA stores the tar file by clicking one of the following radio buttons:
 - **Network Directory**—Stores the tar file in a network folder. Enter information in these fields:
 - Path Name—Network path to the appropriate folder
 - User Name—Username for network access
 - Password—Password for network access
 - **Local Directory**—Stores the tar file in a folder on the server on which you are running DMA. In the Path Name field, enter the path to the folder or click **Browse** to choose a folder.
-
-  **Note** Do not specify a mapped network directory for the Local Directory. If you do, DMA may not be able to create the destination folder.
-
- **Tape Device**—Stores the tar file to a backup device. Choose an available tape device from the pulldown menu.

If a tar file already exists in the destination that you chose, DMA will delete that file when it creates the new one.

 - b. Click **Update**.
 - c. If you chose **Local Directory** as the backup storage location, click **OK** when you see this prompt:

Please ensure that you transfer the contents from the LOCAL path to an external device before upgrading. The files will not be readable from the local directory during the upgrade installation

Step 5 From the Data Migration Assistant menu bar, choose **Backup > Backup Now**.
The Migrate Data Source Server page displays.

Step 6 In the Migrate Data Source Server page, click **Start Backup Now**.
The backup begins.

A status window shows you the status of the backup as it proceeds. If you close the status window, you can display it again by clicking the **View Latest Status** link in the Migrate Data Source Server page.

The backup process can take a long time to complete. You can stop this process at any time by choosing **Start > Programs > Cisco DMA > Cancel Backup** and then clicking **Cancel Backup Now** in the Cancel Backup Process dialog box. The system could require several minutes to cancel the backup process.



Note If you close the DMA window while a backup process is running, the backup continues. However, when you restart DMA, the main window will display the **Reset Status** button. Clicking the **Reset Status** button cancels the backup process that is currently running.

When the backup completes, the status window displays the following lines:

```
Archive built successfully
Backup information file DMABackupinfo.inf saved to D:\DMA
```

Step 7 If you saved the tar file in a local directory in [Step 4](#), copy that file to a network server or to a tape device before you upgrade.

The following format shows how the tar file is named, where *date* and *time* indicate when the file was created:

DMABackup*date#time*.tar

You must perform this step because a tar file on the local disk will not be accessible during the upgrade process, and the file will be deleted when the upgrade process reformats the local server disks.

DMA Backup Information File

DMA automatically creates a backup information file when it backs up data. This file contains configuration and environment data regarding the DMA software, the server on which you ran DMA, and the software for which you backed up data.

The system saves the backup information file, which is named DMABackupInfo.inf, in the D:\DMA folder on the server on which you run DMA. The file also gets saved as part of the tar file.

Administering and Troubleshooting DMA

The following sections provide information that you can use to administer and troubleshoot DMA:

- [Determining DMA Software Version, page 10](#)
- [Reviewing the Results of the last DMA Backup Procedure, page 10](#)
- [Log Files, page 11](#)
- [Trace Files, page 13](#)

Determining DMA Software Version

To determine the version of DMA that is installed on a server, follow these steps:

Procedure

- Step 1** Take one of these actions to display the Data Migration Assistant home page, if it is not displayed already:
- If DMA is running, choose **Backup > Home** from DMA menu bar.
 - If DMA is not running, choose **Start > Programs > Cisco DMA > DMAAdmin** and log in as the Windows Administrator when prompted.
- Step 2** In the Data Migration Assistant home page, click the **Details** button.
-

Reviewing the Results of the last DMA Backup Procedure

To see the results of the last backup procedure that you performed with DMA, follow these steps:

Procedure

- Step 1** Choose **Start > Programs > Cisco DMA > DMAAdmin**.
- Step 2** When prompted, log in as the Windows Administrator.
- Step 3** From the Data Migration Assistant menu bar, choose **Backup > Backup Now**.
- Step 4** In the Migrate Data Source Server page, click the **View Latest Status** link.

If you click the **View Latest Status** link during a backup procedure, the status of the current procedure displays.

Log Files

Table 3 describes the log files that DMA creates. If necessary, you can provide log files to the Cisco Technical Assistance Center (TAC) for assistance with troubleshooting.

Table 3 DMA Log Files

File Type	Description	File Location	File Name
Installation log files	Created each time that you perform the DMA installation procedure.	C:\Program Files\ Common Files\Cisco\Logs	DMAInstalldate_time.log, where <i>date_time</i> specifies the date and time that the file was created DMAInstallUI.log
Backup operation log file	Created each day that you run DMA to back up data. If you run the backup procedure more than once on the same day, DMA appends information to the existing file for that day.	C:\Program Files\ Common Files\Cisco\Logs\ DMA\BACKUP	Backupdate.log, where <i>date</i> specifies the date that the file was created This log also displays when you click the View Latest Status Link.
Database export operation log file	Created the first time that you run DMA to back up data. Each subsequent time that you run the backup procedure, DMA appends information to this file.	C:\CiscoWebs\DMA\Bin	exportdb.log
Directory export operation error log file	Created each time that you run DMA to back up data. If the file exists, DMA overwrites it.	C:\CiscoWebs\DMA\ DirExport\logs	DirExport_Error.log
Directory export operation report file	Created the first time that you run DMA to back up data. Each subsequent time that you run the backup procedure, DMA appends information to this file.	C:\CiscoWebs\DMA\ DirExport\logs	DirExport_Reprt.txt

Table 3 DMA Log Files (Continued)

File Type	Description	File Location	File Name
Directory export operation results file	Created each time that you run DMA to back up data. If the file exists, DMA overwrites it.	C:\CiscoWebs\DMA\ DirExport\logs	DirExport_Result.txt
Data validation log	Contains any validation errors that are found during the verification of database and directory data during the backup process	C:\CiscoWebs\DMA\Bin	datavalidation.log

Common Errors

DMA can return the errors described in [Table 4](#), which can cause it to fail.

Table 4 DMA Errors Messages and Descriptions

Error Message	Description
<p>Failure- Product check; Database contains models that are no longer supported in this release.</p> <p>AT, AS, and ICS gateways are not supported. Please remove unsupported models and repeat export.</p>	<p>This error displays if any of the following are present in the device table:</p> <ul style="list-style-type: none"> • Cisco AT-2 Gateway PRODUCT_AT2_GATEWAY • Cisco AT-4 Gateway PRODUCT_AT4_GATEWAY • Cisco AT-8 Gateway PRODUCT_AT8_GATEWAY • Cisco AS-2 Gateway PRODUCT_AS2_GATEWAY • Cisco AS-4 Gateway PRODUCT_AS4_GATEWAY • Cisco AS-8 Gateway PRODUCT_AS8_GATEWAY • All ICS platforms
Failure, Pre-SD CCM Migration	This error indicates that a problem occurred during the migration from Cisco CallManager 3.x to Cisco Unified CallManager 4.1.
<p>Failure - Sony devices exist in the database, but there is no corresponding csv file.</p> <p>Please reinstall the Sony installation.</p>	This error indicates that the system cannot find a CSV file for a Sony phone. Before you can continue with the migration, you must reinstall the device.

Table 4 DMA Errors Messages and Descriptions (Continued)

Error Message	Description
Failure - Tandberg devices exist in the database, but there is no corresponding csv file. Please reinstall the Tandberg installation.	This error indicates that the system cannot find a CSV file for a Tandberg phone. Before you can continue with the migration, you must reinstall the device.
Failure- Invalid enum 31970 in Zimbabwe Locale csv file. Zimbabwe network locale needs to be replaced with a newer version before upgrade.	The error indicates that you have an invalid version of the Zimbabwe locale file. Before you can continue with the migration, you must download a new copy of the Zimbabwe locale file from Cisco.com and install it on your system.
Failure- Zimbabwe network locale needs to be replaced with a newer version before upgrade.	The error indicates that you have an invalid version of the Zimbabwe locale file. Before you can continue with the migration, you must download a new copy of the Zimbabwe locale file from Cisco.com and install it on your system.
Failure- Tandberg.xml file is invalid and needs to be replaced before upgrade. Please reinstall Tandberg with a newer installation.	The error indicates that you have an invalid version of the Tandberg.xml file. Before you can continue with the migration, you must download a new copy of the Tandberg.xml file from Cisco.com and install it on your system.

Trace Files

Table 5 describes the trace files that DMA creates. If necessary, you can provide trace files to the Cisco Technical Assistance Center (TAC) for assistance with troubleshooting.

Table 5 DMA Trace Files

File Type	Description	File Location	File Name
DMA operation trace file	Created each day that you run DMA to back up data. If you run the backup procedure more than once on the same day, DMA appends information to the existing file for that day	C:\Program Files\Cisco\Trace\DMA	Tracedate.log, where <i>date</i> specifies the date that the file was created or updated.
Database export operation trace file	DMA creates one file each time that it backs up Cisco Unified CallManager data and one file each time that it backs up CAR data.	C:\Program Files\Cisco\Trace\DBL	<ul style="list-style-type: none"> Export: installdbccm.log W1install: installdbw1.log

Table 5 DMA Trace Files (Continued)

File Type	Description	File Location	File Name
Directory export operation trace file	Created the first time that you run DMA to back up data. Each subsequent time that you run the backup procedure, DMA appends information to this file.	C:\CiscoWebs\DMA\DirExport\logs	DirExport_Trace.log
Database install setup trace file	Displays the Informix setup status	C:\CiscoWebs\DMA\Bin	dbcmds.log

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://ciscoiq.texterity.com/ciscoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

