



Release Note for the Cisco Application Velocity System

August 11, 2006



Note

The most current Cisco documentation for released products is also available on www.cisco.com. The online documents may contain updates and modifications made after the hardcopy documents were released.

Contents

This release note applies to software versions 6.0, 6.0.2, and 6.0.3 for the Application Velocity System (AVS). This release note contains the following sections:

- [Supported Product Upgrades](#)
- [New Features in Version 6.0](#)
- [Performance Node and Console Version Match](#)
- [Account Information](#)
- [Password Recovery Procedure](#)
- [Software Version 6.0.3 Open and Resolved Caveats](#)
- [Password Recovery Procedure](#)
- [Software Version 6.0.3 Open and Resolved Caveats](#)
- [Software Version 6.0.2 Open and Resolved Caveats](#)
- [Software Version 6.0 Open and Resolved Caveats](#)
- [Related Documentation](#)
- [Cisco Product Security Overview](#)
- [Obtaining Technical Assistance](#)



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

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

Supported Product Upgrades

You can upgrade the Cisco AVS 3120 or AVS 3180 products to software version 6.0.x. [Table 1](#) lists the upgrade paths and methods that are available for the appliance.

Table 1 Supported AVS Upgrade Methods

Existing Products Release	Upgrade Product Release	Software Upgrade Method	Notes
AVS 5.0 AVS 5.0.1	AVS 6.0.3, AVS 6.0.2, AVS 6.0	Supported	Obtain correct appliance image from www.cisco.com
AVS 5.0	AVS 5.0.1	Supported	Obtain correct appliance image from www.cisco.com

New Features in Version 6.0

This section describes the new features and changes in software version 6.0.

- A new web application security module provides a policy-based application firewall. For details, see [Chapter 6, “Web Application Security Configuration”](#) in the *Cisco Application Velocity System User Guide*.
- If you are using the new web application security module, the AVS 3120 uses Ethernet ports other than Port 1. For details, see the [“Password Recovery Procedure”](#) section.

Performance Node and Console Version Match

You must upgrade all deployed performance nodes to match the software version of the Management Console. For example, for the AVS 6.0.2 software release, you must upgrade all of the performance nodes to version 6.0.2. Without these performance node upgrades, critical management features such as performance node configuration versioning will not function correctly.

Account Information

The following account information may be helpful to you during and after an upgrade:

- The grub password is set to **FineGr0und5!**
Grub will ask you for this password if you want to change the normal boot process.
- The pam_tally option in `/etc/pam.d/system-auth` disables accounts after a specified number of failed logins. The root account is exempt from this check. The support for this option is included but not activated in `/etc/pam.d/system-auth`. To enable this option, uncomment the auth and account lines that contain references to pam_tally. A disabled account can be restored by the root user by using the following command:

```
/sbin/pam_tally --user username --reset
```
- After updating to version 6.0.x, the only accounts with a valid login shell will be fgn and root.
- After updating to version 6.0.x, the fgn account password is reset to **fineground**.
- The user fgn is allowed to su into root.

- Root cannot log in using ssh. Root log in is allowed only from the serial console (ttyS0) through a PC connected to the serial port and running a terminal emulation program, or the console (tty1) through a keyboard and mouse connected directly to the appliance. These terminals require physical access to the appliance.

AVS 3120 Ethernet Port Assignments

With AVS 6.0.x software, the AVS 3120 may use other Ethernet ports in addition to Port 1. These other ports are used by the web application firewall module and depend on which operating mode the web application firewall is using. The port assignments for the various web application firewall operating modes are summarized in [Table 2](#).

If you are not using the web application firewall component of AVS, then only Ethernet Port 1 is used.

Table 2 *Port Assignments*

Web Application Firewall Operating Mode	Port 1	Port 2	Port 3	Port 4
Inline	management console	not used	incoming client traffic	outgoing server traffic
Gateway	management console and web traffic	not used	not used	not used
Monitor	management console	monitored traffic	not used	not used

For more details on the web application firewall operating modes, see [Chapter 6, “Web Application Security Configuration”](#) in the *Cisco Application Velocity System User Guide*.

Frequently Asked Questions (FAQ)

This section provides help on specific issues, problems, and questions.

- Q.** How can I change the IP address of the appliance once it has been already installed?
 - A.** Use the CLI command **set interface** to change the IP address on the AVS 3120 and AVS 3180 appliances.

- Q.** How can I change the host name of the appliance?
 - A.** Use the CLI command **set hostname** to change the host name on the AVS 3120 and AVS 3180 appliances.

- Q.** How do I access the appliance remotely?
 - A.** The only way to access the appliance remotely is by using SSH.

- Q.** Of the multiple network interfaces found on the back panel of the AVS appliance, which one is used for management console connectivity?
 - A.** On the AVS 3120 appliance, the left-most interface (Ethernet 1) is used for management console connectivity. On the AVS 3180 appliance, the lower interface (Ethernet 1) is used for management console connectivity. For details on how the other Ethernet ports are used on the AVS 3120 appliance in AVS 6.0.x, see the [“Password Recovery Procedure” section on page 8](#).

Upgrading AVS 3120 and AVS 3180 to Software Version 6.0.x

Follow the steps in this section to upgrade the AVS 3120 or AVS 3180 from version 5.0.x to version 6.0.x.

The AVS 3180 upgrade process does not automatically back up the database. You must back up the database manually before beginning the upgrade procedure. Follow these steps to back up the database:

-
- Step 1** Obtain PostgreSQL from <http://www.postgresql.org/> and install it onto a remote host system that has enough disk space to hold the full database backup. The amount of disk space required could be as large as 180 GB, if the database is around 160 GB in size.
- Step 2** From the remote host, back up the AVS database by using the PostgreSQL utility **pg_dump**. This utility copies the database from the AVS 3180 into a series of text files on the remote host. The command is as follows:

```
$PG_HOME/bin/pg_dump -h AVShostname -U fineground -p 5432 fgnlog | split -b 1024m - backupFilename
```

The keywords, arguments, and options are:

- **-h AVShostname** - Hostname or IP address of the AVS 3180 where the database resides
- **-U fineground** - Connects to the database with the fineground username
- **-p 5432** - Port number to use to connect to the database
- **fgnlog** - Name of the database
- **| split -b 1024m -** - Splits the output of pg_dump into separate files that have a maximum size of 1024 MB
- **backupFilename** - Pathname of the file to hold the database back up. The split program creates more than one file, appending two letters (aa, ab, and so on) to the name for each subsequent file it creates.



Note It is usually necessary to divide the output of **pg_dump** into a series of files because of the maximum file size limitations of the operating system. The maximum file size for the Linux version 2.4 kernel is 2 GB. The maximum file size on other operating systems may vary.

Iptables could prevent the remote host from connecting to the AVS 3180 where the database resides. If this happens, execute the following commands on the AVS 3180:

```
/sbin/iptables -F
/sbin/iptables -X
```

To proceed with the AVS appliance upgrade, follow these steps:

-
- Step 1** Place the upgrade image file onto a local FTP server that can be accessed with an account that has both read and write access. The image file will be named AVS3120-K9-version.tar.gz for the AVS 3120 or AVS3180-K9-MGMT-version.tar.gz for the AVS 3180.
- Step 2** Reboot into safe mode by using the **reboot** CLI command:
- ```
velocity>reboot safe-mode
```

**Step 3** After one minute, access the AVS appliance using SSH. Use the username **fgn** and the password **fineground**. Change to the super user mode by using the **su** command with the dash option:

```
bash-2.05b$ su - root
```

At the password prompt, enter the root password (the default is FineGr0und5!)

**Step 4** Change to the `/usr/sbin` directory:

```
-sh-2.05b# cd /usr/sbin
```

**Step 5** Run the `upgrade.sh` script. The syntax is:

```
-sh-2.05b# ./upgrade.sh upgradefile ftpserverIP usrid password backup | no-backup
```

The arguments and options are:

- *upgradefile* - File name of the upgrade image file
- *ftpserverIP* - IP address of the FTP server
- *usrid*- User name for the FTP server
- *password*- Password for the FTP server
- **backup** | **no-backup** - Indicates whether a backup file is kept. If you select **backup**, a backup file, (AVS-3120.tar for the AVS 3120 or AVS-3180.tar for the AVS 3180) is copied to the FTP server. This file is an archive of image files generated from partitions of system, application, and configuration data. On the AVS 3180, this backup option does not back up the database. A warning is displayed to back up the database separately before proceeding with the upgrade.



**Note** We recommend that you use the **backup** option to generate a backup file in case you need to revert to the previous software version. To allow you to revert to the previous software version, you must use this option to generate a backup file.

Once the upgrade completes successfully, the message “The Upgrade Completed Successfully” is displayed.

**Step 6** Enter the **reboot** command to reboot the AVS appliance into the runtime image:

```
-sh-2.05b# reboot
```

## Reverting to a Previous Software Version by Using a Backup File

After you upgrade an appliance by using the previous upgrade procedure, you may wish to revert to the previous software version. To revert to the previous software version, use the backup file that was generated if you specified the **backup** option for the `upgrade.sh` script. To revert to the previous software version using the backup file, follow these steps:

**Step 1** Place the backup image file onto a local FTP server. If you followed the upgrade procedure in the previous section and chose the **backup** option, the backup image file will exist on the same FTP server you used for the upgrade.

**Step 2** Reboot into safe mode by using the **reboot** CLI command:

```
velocity>reboot safe-mode
```

- Step 3** After one minute, access the AVS appliance using SSH. Use the username **fgn** and the password **fineground**. Change to the super user mode by using the **su** command with the dash option:

```
bash-2.05b$ su - root
```

At the password prompt, enter the root password (the default is FineGr0und5!)

- Step 4** Change to the `/usr/sbin` directory:

```
-sh-2.05b# cd /usr/sbin
```

- Step 5** Run the `restore.sh` script. The syntax is:

```
-sh-2.05b# ./restore.sh backupfile ftpserverIP usrid password
```

The arguments are:

- *backupfile* - File name of the backup image file
- *ftpserverIP* - IP address of the FTP server
- *usrid* - User name for the FTP server
- *password* - Password for the FTP server

Once the process completes successfully, the message “Restore has completed” is displayed. On the AVS 3180, you must restore the database separately because it is not backed up by the backup utility. See the following procedure for details.

- Step 6** Enter the **reboot** command to reboot the AVS appliance into the runtime image:

```
-sh-2.05b# reboot
```

To restore the database on the AVS 3180 from a backup that was made by using the procedure described in the section [Upgrading AVS 3120 and AVS 3180 to Software Version 6.0.x](#), follow the steps below.

- Step 1** From the remote host, restore the AVS database by using the PostgreSQL utility **psql**. This utility reads in the backup files and enters the data back into the AVS database. The command is as follows:

```
cat backupFilename* | $PG_HOME/bin/psql -h AVShostname -U fineground -p 5432 fgnlog
```

The keywords and arguments are:

- **cat backupFilename\*** - Pathname of the database backup file that you specified during the backup procedure. The asterisk at the end ensures that all of the multiple split files are read.
- **| \$PG\_HOME/bin/psql** - Restores the database from the backup files
- **-h AVShostname** - Hostname or IP address of the AVS 3180 where the database resides that you are restoring
- **-U fineground** - Connects to the database with the fineground username
- **-p 5432** - Port number to use to connect to the database
- **fgnlog** - Name of the database

The backed up data is appended to the database during the restore procedure, except for duplicate records, which are not added to the database.

# Password Recovery Procedure

To reset the root password for the AVS appliance, follow the procedure below. This procedure applies to the AVS 3120 and AVS 3180.

**Step 1** Connect a console to the application appliance and then restart the application appliance.

**Step 2** When you see the following boot screen, press the “p” key.

```
GRUB Loading stage1.5.
```

```
GNU GRUB version 0.94 (635K lower / 4127680K upper memory)
```

```

0: Cisco AVS Runtime Image
1: Cisco AVS Maintenance Image

```

Use the ^ and v keys to select which entry is highlighted.  
Press enter to boot the selected OS or 'p' to enter a password to unlock the next set of features.

**Step 3** Enter the password when prompted (the default password is FineGr0und5!) and press **Enter**:

```
Password: *****
```

**Step 4** Enter the letter “e” next (without pressing **Enter**).

**Step 5** Use the down arrow key to select choice 1 (kernel) from the following list.

```

0: root (hd0,1)
1: kernel /boot/vmlinuz-espresso ro root=/dev/sda2 console=ttyS0
2: initrd (hd0,1)/boot/initrd-espresso

```

**Step 6** Enter the letter “e” next (without pressing **Enter**). The following command is displayed:

```
grub edit> kernel /boot/vmlinuz-espresso ro root=/dev/hda2 console=ttyS0
```

**Step 7** Add a space character followed by the word **single** to the command line, as follows, then press **Enter**:

```
grub edit> kernel /boot/vmlinuz-espresso ro root=/dev/hda2 console=ttyS0 single
```

**Step 8** Enter the letter “b” (without pressing **Enter**).

**Step 9** The appliance will boot into single user mode. The command prompt will be displayed after the boot process.

**Step 10** Use the **passwd** command to change the root password:

```
sh-2.05b# passwd
Changing password for user root.
New password:
```

**Step 11** Reboot the appliance by using the **reboot** command:

```
sh-2.05b# reboot
```

## Software Version 6.0.3 Open and Resolved Caveats

The following caveat is open in software version 6.0.3:

- **CSCse83418**—In the AVS 3120, you can configure websec to protect the web servers from an SQL injection attack. You can also define SQL patterns and create policies using those patterns. However, websec crashes when you try to attach greater than seven SQL policies to a policy map.

The following caveat was resolved in software version 6.0.3:

- **CSCek45988**—AVS SNMP uses a loopback IP address to periodically probe websec components to check their state. Because the websec components do not clean up the session properly, they fail to respond to the probes. This results in several half-opened connections, and for the websec components that do not respond to the probes, SNMP traps are generated declaring that websec is not operational.

## Software Version 6.0.2 Open and Resolved Caveats

Table 3 lists the open caveats in software version 6.0.2.

**Table 3** Open Caveats in Software Version 6.0.2

| Tracking Number | Description                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek14514      | It is possible to access the same AVS 3120 node from more than one AVS 3180 Management Station. This can result in inconsistent configuration of the AVS 3120. Do not attempt to configure an AVS 3120 node from more than one AVS 3180 Management Station.                                                                                           |
| CSCsc04598      | Due to an inconsistency in the BIOS and run-time image clock settings, you must configure the initial date and time by using the following commands:<br><br><pre>set date tz timezone set ntp start ntp_ip</pre> Or, if you do not want to use an NTP server, you must use this command:<br><br><pre>set date time MM:DD:hh:mm:YYYY tz timezone</pre> |
| CSCsc32485      | A syntax error in httpd.conf will not cause an error message to be logged to the error log.                                                                                                                                                                                                                                                           |
| CSCsc64837      | Web browsers other than Internet Explorer are not supported for accessing the Management Console. You must use Internet Explorer version 6.0 or later for accessing the Management Console. This is unchanged from AVS 5.0.x                                                                                                                          |

Table 4 lists the resolved caveats in software version 6.0.2.

**Table 4 Resolved Caveats in Software Version 6.0.2**

| Tracking Number | Description                                                                                                                                                    |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek34737      | Upgrading from AVS 5.0 to 6.0.2 on the AVS 3180 now uses a single installable upgrade image instead of required you to extract a tar file.                     |
| CSCek36050      | Disable associating an empty traffic class map with a policy map.                                                                                              |
| CSCek39642      | Added support to handle response code 100 properly.                                                                                                            |
| CSCek42025      | If the proxy drops a connection due to insufficient buffer space, it is logged.                                                                                |
| CSCsb41642      | The SNMP agent now uses the correct interface IP address in traps, instead of the loopback address.                                                            |
| CSCsc13072      | Availability Manager clustering configuration commands can be executed in any order and the appliance will initialize properly.                                |
| CSCsd89732      | The Saved Logs function in the web application security module now displays the log messages from all /var/log/messages files, instead of just the first file. |
| CSCse08493      | The last digit of the server address is now correctly displayed in the configuration output.                                                                   |
| CSCse15465      | Added support to display error logs.                                                                                                                           |

## Software Version 6.0 Open and Resolved Caveats

Table 5 lists the open caveats in software version 6.0.

**Table 5 Open Caveats in Software Version 6.0**

| Tracking Number | Description                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCek14514      | It is possible to access the same AVS 3120 node from more than one AVS 3180 Management Station. This can result in inconsistent configuration of the AVS 3120. Do not attempt to configure an AVS 3120 node from more than one AVS 3180 Management Station.                                                                                                                       |
| CSCek34737      | To upgrade from AVS 5.0 to 6.0 on the AVS 3180 requires that you extract a tar file, rather than having a single installable binary.                                                                                                                                                                                                                                              |
| CSCsb41642      | The SNMP agent uses the loopback IP address (127.0.0.1) instead of the interface IP address in traps.                                                                                                                                                                                                                                                                             |
| CSCsb82920      | There is no provision for displaying the ARP table by using the CLI.                                                                                                                                                                                                                                                                                                              |
| CSCsc04598      | Due to an inconsistency in the BIOS and run-time image clock settings, you must configure the initial date and time by using the following commands:<br><br><pre>set date tz <i>timezone</i> set ntp start <i>ntp_ip</i></pre> Or, if you do not want to use an NTP server, you must use this command:<br><br><pre>set date time <i>MM:DD:hh:mm:YYYY</i> tz <i>timezone</i></pre> |

**Table 5**      **Open Caveats in Software Version 6.0 (continued)**

| <b>Tracking Number</b> | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCsc13072             | Availability Manager clustering configuration commands must be executed in the following sequence, otherwise, the appliance will not initialize properly:<br><br><pre> set am enable set lb cluster set lb server           </pre>                                                                                                                                                        |
| CSCsc13075             | A change to the DNS server configuration (Resolv.conf) takes effect only after restarting the Condenser.                                                                                                                                                                                                                                                                                  |
| CSCsc32485             | A syntax error in httpd.conf will not cause an error message to be logged to the error log.                                                                                                                                                                                                                                                                                               |
| CSCsc64837             | Web browsers other than Internet Explorer are not supported for accessing the Management Console. You must use Internet Explorer version 6.0 or later for accessing the Management Console. This is unchanged from AVS 5.0.x                                                                                                                                                              |
| CSCsd89732             | The Saved Logs function in the web application security module displays only the log messages in the /var/log/messages file on the AVS 3180 Management Station. Other log files, such as /var/log/messages.1, /var/log/messages.2, and so on, are created when needed but are not displayed by the Saved Logs function. These other log files can be retrieved via console access or FTP. |

Table 6 lists the resolved caveats in software version 6.0.

**Table 6 Resolved Caveats in Software Version 6.0**

| Tracking Number | Description                                                                                                                                                                                                           |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCsc72489      | Changed IP_CONN_TRACK from a static-compiled kernel component to a kernel loadable module. This component is needed by the Availability Manager. Making it loadable only when needed improves the system performance. |
| CSCsc80179      | Fixed a performance issue with the JPull module, which processes FgnStatLog files. JPull no longer sleeps for a few seconds before processing the next available FgnStatLog file.                                     |

## Related Documentation

Refer to the following documentation for more information on the AVS 3120 and the AVS 3180 products:

| Document Title                                                                | Provides                                                                                                               |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| <i>Cisco AVS 3120 Application Velocity System Hardware Installation Guide</i> | Information on installing the Cisco AVS 3120 Application Velocity System.                                              |
| <i>Cisco AVS 3180 Management Station Hardware Installation Guide</i>          | Information on installing the Cisco AVS 3180 Management Station.                                                       |
| <i>Cisco Application Velocity System User Guide</i>                           | Comprehensive information on using the AVS software, including configuration, administration, and reporting functions. |

## 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](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML 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= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

## Ordering Documentation

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](mailto: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 submit comments about Cisco documentation 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

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—[security-alert@cisco.com](mailto: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.

- For Nonemergencies—[psirt@cisco.com](mailto: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 (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.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](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.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

# 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)—An existing 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 operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- 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>

---

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0705R)

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