



# Release Note for the Cisco Application Velocity System

---

February 18, 2008



**Note**

---

The most current Cisco documentation for released products is also available on [www.cisco.com](http://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 version 5.1 of the Application Velocity System (AVS). This release note contains the following sections:

- [Supported Product Upgrades](#)
- [Account Information](#)
- [Performance Node and Console Version Match](#)
- [Upgrading the AVS 3110](#)
- [Upgrading the AVS 3120 and AVS 3180](#)
- [Reverting to a Previous Software Version Using a Backup File](#)
- [Password Recovery Procedure](#)
- [Frequently Asked Questions \(FAQ\)](#)
- [Software Version 5.1 Resolved Caveats](#)
- [Software Version 5.1 Open Caveat](#)
- [Related Documentation](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)



---

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

© 2007-2008 Cisco Systems, Inc. All rights reserved.

# Supported Product Upgrades

You can upgrade previous releases of the Cisco AVS 3110 or FineGround Velocity product in the field. The method of upgrading depends on the appliance version you have. [Table 1](#) lists the upgrade paths and methods that are available for the appliance. To upgrade to 5.1, the product must be at version 4.0 or later.

**Table 1** Supported AVS Upgrade Methods

Existing Products Release	Upgrade Product Release	Software Upgrade Method	Notes
AVS 5.1	AVS 5.0.1, 5.0.2	Supported	Obtain correct appliance image from <a href="http://www.cisco.com">www.cisco.com</a>
AVS 5.0	AVS 5.0.1, 5.0.2	Supported	Obtain correct appliance image from <a href="http://www.cisco.com">www.cisco.com</a>
Velocity or AVS 4.0	AVS 5.0.0, AVS 5.0.1, AVS 5.0.2	Supported (Must be at 4.0 or greater)	Obtain correct appliance image from <a href="http://www.cisco.com">www.cisco.com</a>
Velocity 3.2.5 Velocity 3.2.1 Velocity 3.2.0 Velocity 3.1.0	AVS 4.0.0	Supported (Must be at 3.1.0-5 or greater)	Obtain correct appliance image from <a href="http://www.cisco.com">www.cisco.com</a>

## 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 5.1, the only accounts with a valid login shell will be fgn and root.
- After updating to version 5.1, 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.

# 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 5.1 software release, you must upgrade all of the performance nodes to version 5.1. Without these performance node upgrades, critical management features such as performance node configuration versioning will not function correctly.

## Upgrading the AVS 3110

To upgrade the AVS 3110 from software versions 4.0 or 5.0 to version 5.1, perform the following procedure. Ensure that you run the installation as the root user.

- 
- Step 1** Obtain the appliance upgrade image file from [www.cisco.com](http://www.cisco.com).
- Step 2** Shut down all AVS related processes, by executing the following commands:
- ```
# /etc/init.d/fgnpn_6628c641c56f7e6e1e6aec5f24e328c17f81683b stop
# /etc/init.d/fgnmc_de1eb23f6ecf273bee6b4561cd29368e3e539712 stop
# /etc/init.d/fgndb_de1eb23f6ecf273bee6b4561cd29368e3e539712 stop
```
- Step 3** Change directory to the following path:
- ```
cd /usr/local/fineground/appliance
```
- Step 4** Make an upgrade51 directory. For example:
- ```
mkdir upgrade51
```
- Step 5** Change to this new directory:
- ```
cd upgrade51
```
- Step 6** Copy the appliance upgrade image file to this location.
- Step 7** Extract the TAR archive. For example:
- ```
tar zxvf AVS3110-K9-version-UPGRADE.tar
```
- Step 8** Change to the bin directory:
- ```
cd bin
```
- Step 9** Execute the appliance upgrade script:
- ```
./run.sh upgrade-fgn
```
- Step 10** Change to the hardening directory:
- ```
cd ../hardening
```
- Step 11** Execute the hardening script:
- ```
./fgn_up2date.sh |tee -a ./rpm-update.log 2>&1
```
- Step 12** Reboot the appliance by issuing the **reboot** command:
- Step 13** After the appliance starts, change to bin directory in the location where you extracted the TAR archive:
- ```
cd /usr/local/fineground/appliance/upgrade51/bin
```

- Step 14** Execute the system upgrade script with the `upgrade-system` flag to upgrade the operating system and the system:

```
./run.sh upgrade-system
```



**Note** The system upgrade process (system hardening) takes time to complete. Do *not* interrupt the process by typing Ctrl-C (or any other interrupt keys). You must wait until the shell prompt appears. To monitor the progress, open a new shell and use the following command:  
**tail -f /usr/local/fineground/appliance/upgrade51/hardening/logs/hardenlog**

- Step 15** Reboot the appliance by issuing the **reboot** command:
- Step 16** Reregister all upgraded nodes with the Management Console. To do this, open the Management Console, open a node and click the **Edit Properties** command. Click **Apply**, without making any changes to the properties. Repeat this for each node defined in the Management Console.
- If no errors occurred during the upgrade process, the appliance should be upgraded.
- Step 17** Perform this procedure on each appliance that you want to upgrade.

---

The following non-critical error message is logged in `hardening/logs/update-rpms.log`:

```
sleep: relocation error: /lib/i686/librt.so.1: symbol __pthread_clock_settime, version GLIBC_PRIVATE not defined in file libpthread.so.0 with link time reference
```

This message occurs because `glibc` and its dependencies are updated, and when `sshd` is restarted after the update it refers to preloaded `glibc` libraries that have been replaced. This message can be ignored.

# Upgrading the AVS 3120 and AVS 3180

This section contains information on the steps you must take prior to upgrading your AVS 3120 or AVS 3180, how to back up an appliance prior to upgrading, and the software upgrade procedure. Refer to the following topics to upgrade your appliance.

- [Before Upgrading the AVS 3120 or AVS 3180](#)
- [Backing up the AVS 3180 Before Upgrading](#)
- [Upgrading the AVS 3120 and AVS 3180 to Software Version 5.1](#)

## Before Upgrading the AVS 3120 or AVS 3180

Due to caveat **CSCse73892** (as described in [Software Version 5.1 Open Caveat](#)), you must perform the following procedure before upgrading the software on AVS 3120 or AVS 3180. Note that this caveat does not apply to AVS 3110.

- 
- Step 1** Reboot the system using the safe mode option.
- Step 2** Login as root.
- Step 3** Mount the file system to copy the group file. For example:
- ```
mount /dev/hda2 /mnt
```
- Step 4** Copy the `/etc/group` file to local tmp directory. For example:
- ```
cp -p /mnt/etc/group /tmp/group.backup
umount /mnt
```
- Step 5** Run the upgrade process as described in [Upgrading the AVS 3120 and AVS 3180](#).
- Step 6** When the upgrade process is completed, mount the file system and copy the group file. For example:
- ```
mount /dev/hda2 /mnt
cp -p /tmp/group.backup /mnt/etc/group
```
- Step 7** Reboot the system.

## Backing up the AVS 3180 Before Upgrading

The AVS 3180 upgrade process does not back up the database automatically. 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 may 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.

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

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

## Upgrading the AVS 3120 and AVS 3180 to Software Version 5.1

To upgrade the AVS 3120 or AVS 3180 to version 5.1, perform the following procedure.

**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.

- AVS 3120 - The image file is AVS-K9-UPGRADE-5.1.0-34-tftp.tar.gz
- AVS 3180 - The image filename is AVS-K9-MGMT-UPGRADE-5.1.0-34.img.tgz

**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.

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 Using a Backup File

This section describes how to revert to a previous software version using the backup file generated when you specified the **backup** option for the upgrade script. This section also describes how to restore the AVS 3180 database.

- [Reverting to a Previous Software Version](#)
- [Restoring the AVS 3180 database](#)

## Reverting to a Previous Software Version

To revert to a previous software version using a backup file:

---

**Step 1** Place the backup image file onto a local FTP server. If you followed the upgrade procedure in this document 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
```

---

## Restoring the AVS 3180 database

For the AVS 3180, you must restore the database separately because it is not backed up by the backup utility. To restore the database on the AVS 3180 from a backupfile:

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 syntax 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 3110, 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-espesso ro root=/dev/sda2 console=ttyS0
2: initrd (hd0,1)/boot/initrd-espesso
-----
```

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

```
grub edit> kernel /boot/vmlinuz-espesso 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-espesso 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
```

## 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. On the AVS 3110 appliance, you can run the `/usr/local/appliance/bin/appliance-netconf.py` utility or edit the network configuration file `/etc/sysconfig/network-scripts/ifcfg-eth0` using a text editor and change the `IPADDR=` directive. You must run the `appliance-netconf.py` script from the appliance console.
- 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. On the AVS 3110 appliance, edit the network configuration file `/etc/sysconfig/network` using a text editor and change the `HOSTNAME=` directive.
- 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 active?
- A.** On the AVS 3120 appliance, the left-most interface (Ethernet 1) is the active interface. On the AVS 3180 appliance, the lower interface (Ethernet 1) is the active interface. On the AVS 3110 appliance, the interface closest to the VGA monitor port is the active interface.

## New Features in the AVS 3180A

In software version 5.1, the AVS 3180A can register clusters of the AVS 3120 (which must also be running software version 5.1) and the Cisco ACE 4700 Series Application Control Engine Appliances (ACE).

- The AVS 3180A provides full management functionality, including configuration and AppScope reporting, for the AVS 3120.
- The AVS 3180A supports the ACE 4710 appliances for AppScope reporting only. The AVS 3180A does not provide configuration management for the ACE 4710 appliances. Configuration management for the ACE 4710 is supported using the embedded device manager or by using the Cisco Application Networking Manager (ANM) software.

## Software Version 5.1 Resolved Caveats

The following caveats were resolved in software version 5.1.

- **CSCsh58527**—Apply the DST timezone patch to the AVS platforms. Once the AVS is rebooted using the latest runtime image, the time is set to UTC by default, though the timezone still points to the time that was already set. If you have an NTP client configured, it does not come up automatically; you must start it manually. Once the AVS boots up, perform the following steps to use the DST timezone.
  1. Set the time to the correct local time using the **set date [time mm:dd:hh:mm] [tz timezone]** command. Note that
  2. This step applies only to AVS devices that have an NTP client configured. Start the NTP client using the **set ntp {start | stop} server\_ip\_address** command.
- **CSCsd94732**—Versions of the Cisco Application Velocity System (AVS) prior to software version AVS 5.1.0 do not prompt users to modify system account passwords during the initial configuration process. Because there is no requirement to change these credentials during the initial configuration process, an attacker may be able to leverage the accounts that have default credentials, some of which have root privileges, to take full administrative control of the AVS system. After upgrading to software version AVS 5.1.0, users will be prompted to modify these credentials.

Cisco will make free upgrade software available to address this vulnerability for affected customers. The software upgrade will be applicable only for the AVS 3120, 3180, and 3180A systems. The workaround identified in this document describes how to change the passwords in current releases of software for the AVS 3110. Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0029 has been assigned to this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080123-avs.shtml>.

# Software Version 5.1 Open Caveat

The following caveat is open in software version 5.1. **CSCse73892**—Logging on to the appliance after an upgrade will fail when you add or modify existing users. During an upgrade, the file `/etc/group` gets corrupted and a user's `sudo` privileges are lost. Workaround: Before upgrading the software, perform the following procedure.

---

**Step 1** Reboot the system using the safe mode option.

**Step 2** Login as root.

**Step 3** Mount the file system to copy the group file. For example:

```
mount /dev/hda2 /mnt
```

**Step 4** Copy the `/etc/group` file to local tmp directory. For example:

```
cp -p /mnt/etc/group /tmp/group.backup
umount /mnt
```

**Step 5** Run the upgrade process as described in either [Upgrading the AVS 3110](#) or in [Upgrading the AVS 3120 and AVS 3180](#).

**Step 6** When the upgrade process is completed, mount the file system and copy the group file. For example:

```
mount /dev/hda2 /mnt
cp -p /tmp/group.backup /mnt/etc/group
```

**Step 7** Reboot the system.

## Related Documentation

Refer to the following documentation for 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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, 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, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, 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, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0801R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.

