



Upgrading Memory to 512 MB in the VPN 3000 Series Concentrator

It is now possible to upgrade your VPN Concentrator memory to 512 MB. If your VPN Concentrator is running low on memory resources, upgrading to 512 MB will help. If you are running into either of the following problems and the VPN Concentrator events point to low memory resources as the cause, we recommend upgrading to 512 MB.

- VPN Concentrator is unable to support the necessary number of tunnels.
- VPN Concentrator is unable to accept additional connections.

To determine the amount of memory currently installed in your VPN Concentrator, use the [Monitoring | Status](#) screen.

The VPN Concentrator model 3005 and the VPN 3002 Hardware Client do not support 512 MB memory upgrade.

This document does not include instructions on downgrading the bootcode from version 4.0 or higher to an earlier version. If you need to downgrade your bootcode, contact your Cisco Technical Assistance Center (TAC) representative for instructions.



Caution

The VPN Concentrator and the memory module contain electronic components that are sensitive to electrostatic discharge (ESD). Improper handling could damage components. Leave the module in its protective ESD-shielded envelope until instructed to remove it, and handle it only as instructed. If you have reservations about installing the module, ask for assistance from a qualified technician.

Upgrade Procedure Overview

Upgrading the memory to 512 MB involves the following steps. It is important to do these steps in order:

1. Update the VPN Concentrator software image to Version 4.0 or higher.
2. Update the VPN Concentrator bootcode to Version 4.0 or higher.
3. Install memory cards.



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

Copyright © 2003. Cisco Systems, Inc. All rights reserved.

Updating the VPN Concentrator Software Image to Version 4.x

Check the Administration | Software Update | Concentrator screen to see which version of software your VPN Concentrator is running. If your VPN Concentrator is running a version earlier than 4.0 or higher, update it now.

The software image file must be accessible by the workstation you are using to manage the VPN Concentrator. Software image files ship on the Cisco VPN 3000 Concentrator CD-ROM. Updated or patched versions are available from the Cisco website, www.cisco.com.

Save the current VPN Concentrator configuration file and copy it to a remote system before you proceed. See the Administration | File Management | TFTP Transfer screen in the VPN Concentrator Manager.

-
- Step 1** Using the Administration | Software Update | Concentrator screen, locate and upload the new software image file. The upload process takes a few minutes, and the system displays the progress. Wait for the operation to finish.
 - Step 2** The system prompts you to reboot the VPN Concentrator. Reboot now.
 - Step 3** Using the VPN Concentrator Manager, log in again to the VPN Concentrator.
 - Step 4** Clear the cache in your browser to ensure that all new screens display correctly.
 - Step 5** Using the Monitoring | System Status screen, check the software revision to be sure that the VPN Concentrator is now using the updated software image.
-

Updating the VPN Concentrator Boot Code to Version 4.x

Check the Monitoring | System Status screen to see which version of the boot code your VPN Concentrator is running. If your VPN Concentrator is running a version earlier than 4.0 or higher, update it now.

The boot image file must be accessible by the workstation you are using to manage the VPN Concentrator. Boot code image files ship on the Cisco VPN 3000 Concentrator CD-ROM and also are available from the Cisco website, www.cisco.com.



Warning

Do not power off the VPN Concentrator during the boot code upgrade process. Powering off the VPN Concentrator will render it unusable.

-
- Step 1** Download the new boot code file to the PC you are using to manage the VPN Concentrator. (This PC might be the console PC or it might be a different one.)
- Step 2** Using the VPN Concentrator Manager Admin | File Management | File Upload screen, upload the bootcode file from the PC into the VPN Concentrator memory. When this operation is complete, a File Upload Success screen appears.
- Step 3** Click the **Click here to see the list of files** link. The Administration | File Management screen appears. Check that the boot code file appears in the chart.
- Step 4** At the beginning of the upgrade, all network interfaces to the VPN Concentrator are automatically taken down. They are restored afterwards. All current users will be disconnected. Warn users of the pending disconnect.
- Step 5** Using the CLI, log in to the VPN Concentrator from the console port PC. The VPN Concentrator Main menu appears:
- ```

1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

Main ->

```
- Step 6** Enter 2 (Administration). The Administration menu appears:
- ```

1) Administer Sessions
2) Software Update
3) System Reboot
4) Reboot Status
5) Ping
6) Access Rights
7) File Management
8) Certificate Management
9) Back

Admin ->

```

Step 7 Enter 2 (Software Update). The Software Update menu appears:

```
1) Concentrator
2) Clients
3) Bootloader
4) Back
```

```
Admin ->
```

Step 8 Enter 3 (Bootloader). The following warning appears:

```
WARNING:-- Before beginning the bootloader upgrade, be aware of the following:
```

- o You must first download the latest bootloader from the Cisco website to your local disk and upload it to the device.
- o Before the upgrade, all network interfaces to the device are automatically shut down and restored afterwards. Because of this, you may want to warn users of the pending disconnect.
- o During the upgrade, reboots are automatically disallowed.
- o Do not power off the device during the bootloader upgrade process. Powering off the device will render it unusable.

```
Do you really want to upgrade the bootloader? (Y/N) [N]
```

Step 9 Enter y. The following message appears:

```
The network interfaces are down...
```

```
[List of files.]
```

```
Name of the file for bootloader upgrade?
```

Step 10 Enter the name of the boot code file. The following message appears:

```
Bootloader upgrade in process. This should take about 30 seconds.
DO NOT POWER DOWN THE SYSTEM DURING THIS POCEDURE.
```

When the upgrade completes, you see the following message:

```
The network interfaces are restored ...
update success: New bootloader will become active on next reboot!
```

```
Reboot now? (Y/N) [Y]
```

Step 11 Enter y. The VPN Concentrator reboots. Wait for the reboot to complete.

Step 12 Using the VPN Concentrator Manager, log in to the VPN Concentrator.

Step 13 Using the Monitoring | System Status screen, check the boot code version to be sure that the VPN Concentrator is now using the updated boot code.

Troubleshooting the Boot Code Upgrade

Error	Recoverable?	Cause	Solution
File image transfer failure	Yes	The TFTP process failed.	
Invalid boot image file	Yes	The file used to upgrade is not a boot code file.	
Boot image checksum validation error	Yes	The boot code file is corrupted.	
Flash erasure	No	Fatal error.	Try the upgrade again immediately. If the second try also fails, return the VPN Concentrator to Cisco Systems.
Flash write failure	No	Fatal error.	Try the upgrade again immediately. If the second try also fails, return the VPN Concentrator to Cisco Systems.
Flash image checksum failure	No	Fatal error.	Try the upgrade again immediately. If the second try also fails, return the VPN Concentrator to Cisco Systems.

Installing the 256 Mb Memory Modules

**Caution**

The VPN Concentrator and the memory module contain electronic components that are sensitive to electrostatic discharge (ESD). Improper handling could damage components. Leave the module in its protective ESD-shielded envelope until instructed to remove it, and handle it only as instructed. If you have reservations about installing the module, ask for assistance from a qualified technician.

Parts Cisco Supplies

The upgrade kit includes these parts:

- Two 256 MB memory modules.
- Disposable wrist strap ESD protection kit.

Tools You Need

No. 2 Phillips screwdriver.

Shutting Down and Powering Off

Shut down and power off the VPN Concentrator before you install the module.

-
- Step 1** Using the VPN Concentrator Manager, shut down the VPN Concentrator (see the Administration | System Reboot screen).
 - Step 2** Turn power off: press **O** on the power switch on the rear of the chassis.
 - Step 3** Disconnect power cord from the system and the power outlet.
 - Step 4** Disconnect all network cables and the console cable.
-

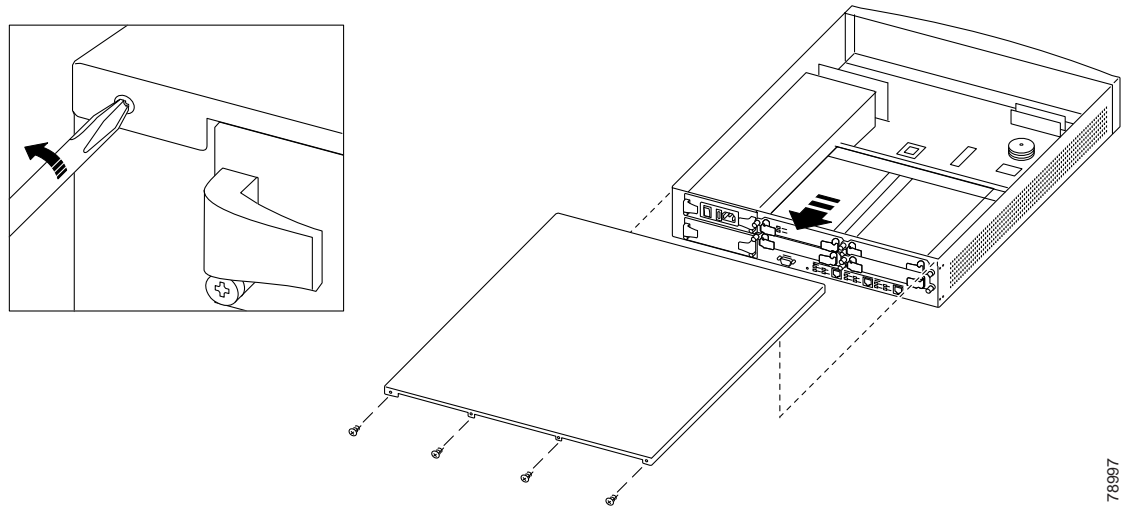
**Warning**

Hazardous voltages and the risk of electrical shock may be present inside the VPN Concentrator chassis. Always disconnect the power cord before removing the chassis cover. Never operate the VPN Concentrator with the cover removed.

Adding the Upgrade Modules

After you shut down the VPN Concentrator and disconnect the power cord, you can add the memory modules, following these steps:

- Step 1** Remove the VPN Concentrator chassis cover. Four screws hold it in place. Pull the cover back and lift it off. Do not let screws fall into the unit.

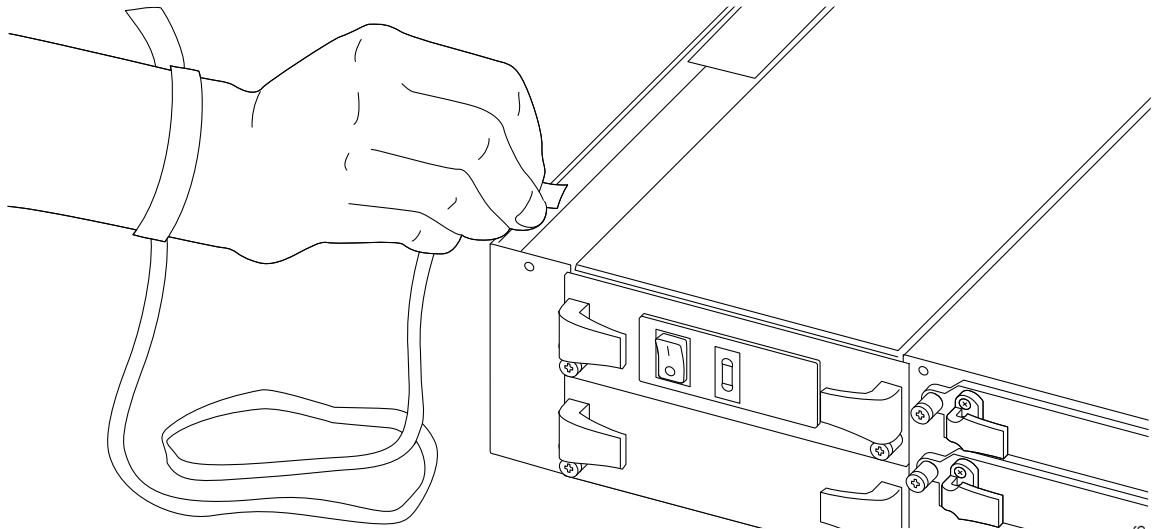


78997

**Caution**

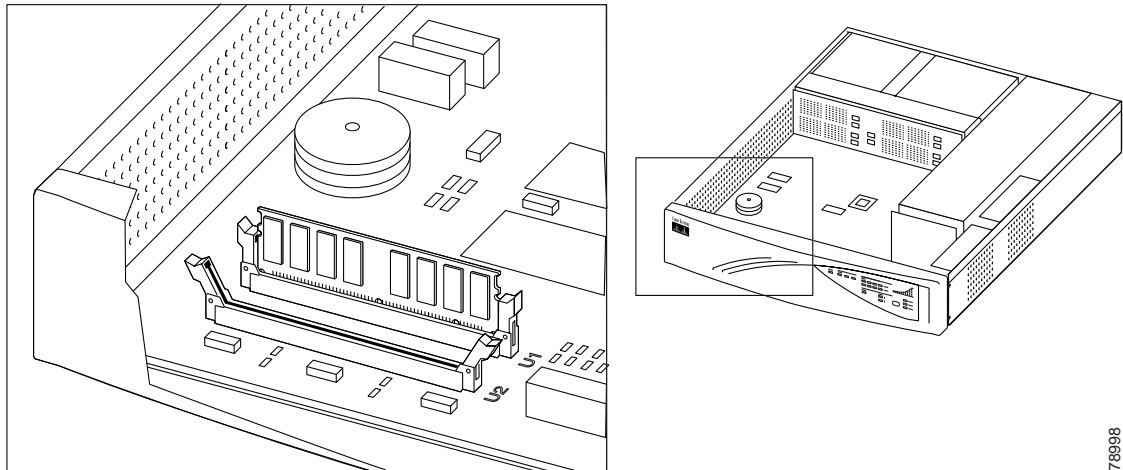
The memory module contains electronic components that are sensitive to electrostatic discharge (ESD). Improper handling could damage the module. Leave the module in its protective ESD-shielded envelope until instructed to remove it, and handle it only as instructed.

- Step 2** Put on disposable wrist strap from an ESD kit according to package instructions. Be sure to attach ground connector to *bare* metal (unpainted metal) on the VPN Concentrator chassis.



78996

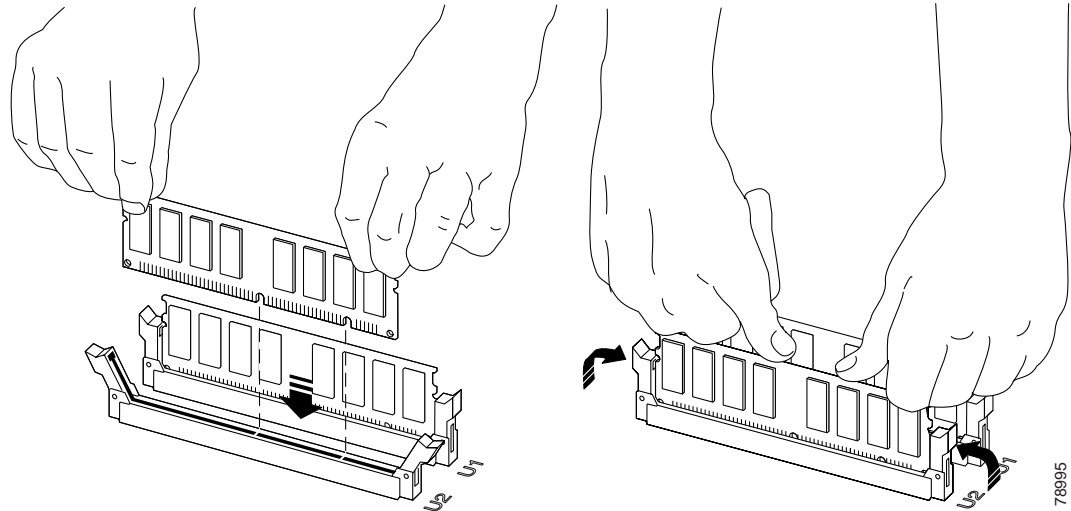
- Step 3** Locate the two memory module slots. If either slot contains a 128-Mb module, remove it.



78998

- Step 4** Open the two white latches on ends of one slot: push them away from the slot.

- Step 5** Remove a new 256 MB memory module from its ESD envelope.
- Step 6** Orient and install memory module into that slot. The module has notches in the connector edge that fit over pins in the socket, and it will fit only one way. The corners must also fit in the open latches. Push straight down, firmly. The connector is tight; you may need to wiggle the module end-to-end to seat it. *Do not bend or twist the module.*



- Step 7** Secure the latches on both ends of module: push them up against the module.
- Step 8** Repeat steps four to seven to install the second memory module in the other slot.
- Step 9** Remove wrist strap connector from chassis.
- Step 10** Replace chassis cover with its four screws. Slide the cover toward the front of the chassis then insert the screws.

**Warning**

Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.

- Step 11** Reconnect the power cord to the system and the power outlet.
- Step 12** Turn the power on: press | on the power switch on the rear of the chassis.
- Step 13** Log in to the VPN Concentrator, using the VPN Concentrator Manager.
- Step 14** Using the Monitoring | Status screen, check the memory size. The memory size should now be 512 MB.

Testing and Configuring the Upgrade Modules

After you have installed the new memory module, follow these steps.

-
- Step 1** Connect network cables and the console cable.
 - Step 2** Connect power cord to the power supply module, and plug the power cord into a power outlet that provides a reliable Earth ground.
 - Step 3** Turn power on: press | on the power switch. The VPN 3030 Concentrator automatically detects the new module during reboot. Confirm that the front-panel System LED is ON (green).
 - Step 4** Confirm that the front-panel LEDs for Expansion Module insertion Status and Run Status are ON (green) for both SEP modules installed.
 - Step 5** Confirm that the back-panel Power and Status LEDs are ON (green) on both SEP modules.
 - Step 6** Using the VPN Concentrator Manager, check the Monitor | System Status screen. Be sure the RAM Size is 512 MB.
-

Troubleshooting the Memory Installation

Problem	Possible Cause	Solution
Memory module not detected.	<ul style="list-style-type: none"> • Module is not seated properly. 	<ul style="list-style-type: none"> • Shut down and power off the VPN 3030. Remove chassis cover. Attach ESD kit. Remove the memory module by pushing the latches away from the module. Reinstall it. Be sure it is inserted all the way in the socket and the latches are tight up against the module.
	<ul style="list-style-type: none"> • Module is defective. 	<ul style="list-style-type: none"> • Contact Cisco support.

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 © 2003, Cisco Systems, Inc.
All rights reserved