



Release Notes for Cisco VPN 3000 Series Concentrator, Release 4.7.1

Revised 05 July 2005

Part Number OL-7859-01

Introduction

These release notes describe the new features in Cisco VPN 3000 Series Concentrator Release 4.7.1, changes to existing features, limitations and restrictions (“caveats”), fixes, and related documentation. They also include procedures you should follow before loading this release. The section, “[Usage Notes](#),” describes interoperability considerations and other issues you should be aware of when installing and using the VPN 3000 Series Concentrator. Read these release notes carefully prior to installing this release.



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Contents

This document includes the following sections:

- [System Requirements, page 3](#)
- [Upgrading to Release 4.7.1, page 7](#)
- [New Features in Release 4.7.1, page 16](#)
- [Usage Notes, page 18](#)
- [Open Caveats, page 28](#)
- [Resolved Caveats, page 40](#)
- [Related Documentation, page 46](#)
- [Obtaining Documentation, page 47](#)
- [Documentation Feedback, page 49](#)
- [Obtaining Additional Publications and Information, page 49](#)

System Requirements

The following sections describe the system requirements for Cisco VPN 3000 Concentrator Release 4.7.1.

Hardware Supported

Cisco VPN 3000 Series Concentrator software Release 4.7.1 supports the following hardware platforms:

- Cisco VPN 3000 Series Concentrators, Models 3005 through 3080
- Altiga Networks VPN Concentrators, Models C10 through C60
- Cisco VPN 3002 Hardware Client

The following table lists the minimum and recommended memory amounts for each VPN Concentrator platform.


Note

Failure to use the recommended amount of memory results in reduced WebVPN session capacity.

Platform	Minimum Memory (MB)	Highly Recommended for WebVPN (MB)
3005	64	64
3015	128	256
3020	256	256
3030	128	512
3060	256	512
3080	256	512


Note

WebVPN is not supported on the 3005 platform with 32 MB of memory. Upgrade the VPN 3005 to 64M.

**Note**

For models 3030 through 3080, the SEP-E encryption card provides significantly better performance than the original SEP module. The Model 3020 uses only SEP-E.

Platform Files

Release 4.7.1 contains three binary files, one for each of the platforms shown in the following table:

Files beginning with...	Support
vpn3000	VPN Concentrator 3015 through 3080 platforms
vpn3002	VPN 3002 Hardware Client (only)
vpn3005	VPN Concentrator 3005 platform (only)

**Caution**

Be sure to install the correct file for the platform you are upgrading.

SSL VPN Client Privilege Requirements

Users must have Administrator privileges on client PCs that use SSL VPN Client (SVC). Clients connecting without Administrator privileges cannot receive and install an SSL VPN Client. However, Cisco provides an Install Enabler utility to pre-load a client service that lets nonprivileged users load SVC. This utility (STCIE.EXE) is useful if you do not typically configure client PC users with Administrator privileges. It is available within the sslclient-win-*<Version>*.zip file on your distribution media or on the VPN 3000 Concentrator download area on Cisco.com.

You must have Administrator privileges on the client PC to run the Install Enabler and install the service. Once the service is installed, it loads at system startup and facilitates SSL VPN Client setup for nonprivileged users.

To set up the client service, unzip the sslclient-win-*<Version>*.zip file and the start the STCIE.EXE executable file. It creates or updates the SVC in the Program Files\Cisco System folder, which the VPN 3000 Concentrator pushes to the client.

The following command line switches are available:

- STCIE.EXE /? — Displays available command options.
- STCIE.EXE /HELP — Displays available command options.
- STCIE.EXE /NODLG — “Silent mode” installation; suppresses dialog boxes except for errors.
- STCIE.EXE /NODLGNOERROR — Suppresses all dialog boxes, including errors.

Compatibility

Refer to the following sections to ensure compatibility with this release.

Cisco Secure Desktop

If you are using Cisco Secure Desktop (CSD) with VPN 3000 Concentrator Release 4.7.1, you must upgrade to CSD Version 3.0.2 or higher.

Likewise, if you are using CSD 3.0.2 or higher, you must upgrade to Release 4.7.1.

Cisco Security Agent

Cisco Security Agent (CSA) Version 4.5 is the only version compatible with the CSD and the SVC.

Japanese Operating System

WebVPN does not support Japanese versions of Linux, Solaris, and Mac OS.

SSL VPN Client Zyxel Modem SSH

The SVC is not compatible with the Zyxel Prestige 643 V2.50 (AP.3) DSL modem running the Putty SSH protocol.

PDA Support

Some PDA devices are supported as VPN 3000 Concentrator clients. Cisco has certified the following Pocket PC platform elements:

- HP iPaq H4150
- Pocket PC 2003
- Windows CE 4.20.0, build 14053
- Pocket Internet Explorer (PIE)
- ROM version 1.10.03ENG
- ROM Date: 7/16/2004

Due to the limitations of the Pocket PC platform, several caveats apply when using a PDA as a VPN 3000 Concentrator WebVPN client:

- The E-mail Proxy feature of VPN 3000 Concentrator WebVPN is not available. The Pocket PC 2003 E-mail client cannot be configured for secure E-mail access using POP3S, IMAP4s, and SMTPS.
- Port Forwarding (application access) and other features that require Java are not supported.
- PIE cannot display pop-up windows. This has several implications:
 - WebVPN cannot display the floating toolbar.
The bottom left corner icon bar is similar to the floating toolbar on other clients.
 - PIE automatically downloads the SSL certificate when initiating a WebVPN session. It does not prompt you to install the certificate, and you cannot view the certificate.
- PIE does not disconnect from WebVPN (or any secure website that uses HTTPS) when you close the browser window.
- To close a WebVPN session, click X on the toolbar or use the VPN 3000 Concentrator Idle Timeout setting.
- After you log out of WebVPN, the “close browser window” link does not work. PIE does not support this function.
- Microsoft Outlook Web Access (OWA) 5.5 does not work properly on the Pocket PC platform, and thus cannot be used through WebVPN.

- When copying a file from the PDA to a server, the “Browse File” option is not available. This is a PDA limitation apart from interaction with the VPN 3000 Concentrator.
- Web pages that use non-standard HTML coding (including “de facto” standards) might not display correctly in PIE, with or without WebVPN.
- The Citrix Metaframe feature does not work on PDAs if they do not have the corresponding Citrix ICA client software.

Upgrading to Release 4.7.1

This section contains information about upgrading from earlier releases to Release 4.7.1.



Note

After upgrading, you must clear the cache in your browser to ensure that all new screens display correctly when you are managing the VPN 3000 Concentrator. Release 4.7.1 adds features, enhances HTML page layouts and deletes cookies. Clearing your browser cache ensures that the new features display correctly.

Upgrading to a new version of the VPN 3000 Concentrator software does not automatically overwrite the existing configuration file. Configuration options for new features are not automatically saved to the configuration file on an upgrade. The HTML Manager displays “Save Needed” (rather than “Save”) to indicate that the configuration needs to be saved. If the configuration is not saved, then on the next reboot, the new configuration options are added again. If you need to send the configuration file to the TAC, save the running configuration to the configuration file first.



Note

Click “Save Needed” to add the new Release 4.7.1 parameters to the configuration file. The VPN 3000 Concentrator Manager adds the Release 4.7.1 parameters to the running configuration after you upgrade and reboot, but you must click the “Save Needed” or “Save” icon to add them to the saved configuration.

Before You Begin

Before you upgrade to this release, *back up your existing configuration to the flash and to an external server*. This ensures that you can return to the previous configuration and software if you need to.

Be aware of the following considerations before you upgrade. These are known product behaviors, and your knowing about them at the beginning of the process should expedite your product upgrade experience. Where appropriate, the number of the caveat documenting the issue appears at the end of the item. See “[Open Caveats](#)” [section on page 28](#) for a description of using this number to locate a particular caveat.



Note

Release 4.7.1 does not have an associated VPN Client release.

Before upgrading, note the following:

- If you are upgrading from Release 3.0 to Release 4.7.1 and you are using the “Group Lookup” feature, you must manually set Group Lookup after the upgrade. To enable this feature, go to Configuration | System | General | Authentication and select the Enable check box (CSCdu63961).
- To use the VPN Client, Release 3.0 or higher, you *must* upgrade the VPN 3000 Concentrator to Release 3.0 or higher. The VPN Client, Release 3.0 or higher, does *not* operate with the VPN 3000 Concentrator Release 2.5 or earlier versions.
- Do not update the VPN 3000 Concentrator when it is under heavy use, as the update might fail (CSCdr61206).

Use the following backup procedure to ensure that you have a ready backup configuration.

Backing Up the Existing Configuration to the Flash

Before upgrading, back up the configuration, as follows:

-
- Step 1** Go to Administration | File Management | Files.
 - Step 2** Select the configuration file and click Copy.
 - Step 3** Enter a name for the backup file (in 8.3 format; for example, name it CON70BAK.TXT)
-

Backing Up the Existing Configuration to an External Server

You should also back up the configuration to a server. You can do this in many ways, one of which is to download the file using your web browser from the HTML interface (VPN 3000 Concentrator).

You can upgrade the software with assurance that you can return to your previous firmware using your previous configuration.

Installing SSL VPN Client Software on a VPN 3000 Concentrator

To install the SSL VPN Client software on a VPN 3000 Concentrator, follow these steps:

-
- Step 1** Download the sslclient-win-*<Version>*.pkg file to any location on your PC.
 - Step 2** Install the Release 4.7.1 image on your VPN 3000 Concentrator.
 - Step 3** Navigate to the Configuration | Tunneling and Security | WebVPN | SSL VPN Client screen in the VPN 3000 Concentrator Manager.
 - Step 4** Click **Install a new SSL VPN Client**.
 - Step 5** Click **Browse** and highlight the sslclient-win-*<Version>*.pkg file.
 - Step 6** Click **Apply**.
 - Step 7** Save the configuration.
-

**Note**

If the VPN 3000 Concentrator is configured to leave the SSL VPN Client installed, and you want to uninstall the software from the workstation, go to Program Files\Cisco Systems\SSL VPN Client folder and run Uninstall.exe.

Client Image Installation Notes

The following recommendations and caveats apply to the automatic installation of SSL VPN Client software on clients:

- To minimize user prompts during SSL VPN Client setup, make sure certificate data on clients and on the VPN 3000 Concentrator match:
 - If you are using a Certificate Authority (CA) for certificates on the VPN 3000 Concentrator, choose one that is already configured as a trusted CA on client machines.
 - If you are using a self-signed certificate on the VPN 3000 Concentrator, be sure to install it as a trusted root certificate on clients.

The procedure varies by browser. See the procedures that follow this section.
 - Make sure the Common Name (CN) in VPN 3000 Concentrator certificates matches the name clients use to connect to it. By default, the VPN 3000 Concentrator certificate CN field is its IP address. If clients use a DNS name, change the CN field on the VPN 3000 Concentrator certificate to that name.
- The Cisco Security Agent (CSA) might display warnings during the SSL VPN Client installation.
- The “Remote desktops and laptops” group attaches the appropriate CSA policy. In CSA version 4.5, CSA policies are not enabled by default; you must select them to prevent the CSD and SVC from failing.
- The appropriate CSA policy is attached to the group “Remote desktops and laptops.” The CSA policies are not enabled by default; you must select them to prevent the CSD and SVC from failing with CSA version 4.5.

- We recommend that Microsoft Internet Explorer (MSIE) users add the VPN 3000 Concentrator to the list of trusted sites. Doing so enables the ActiveX control to install with minimal interaction from the user. This is particularly important for users of Windows XP SP2 with enhanced security. Refer to the following sections for instructions.

Adding a VPN 3000 Concentrator to the List of Trusted Sites (IE)

Use Microsoft Internet Explorer to add a VPN 3000 Concentrator to the list of trusted sites as follows:

-
- Step 1** Go to Tools | Internet Options | Trusted Sites.
The Internet Options window opens.
 - Step 2** Click the Security tab.
 - Step 3** Click the Trusted Sites icon.
 - Step 4** Click the Sites button.
The Trusted Sites window opens.
 - Step 5** Type the host name or IP address of the VPN 3000 Concentrator. Use a wildcard such as `https://*.yourcompany.com` to allow all VPN 3000 Concentrators within the `yourcompany.com` domain to be used to support multiple sites.
 - Step 6** Click the Add button.
 - Step 7** Click the OK button.
The Trusted Sites window closes.
 - Step 8** Click the OK button in the Internet Options window.
-

Adding a Security Certificate in Response to an MSIE "Security Alert"

The following procedure explains how to install a self-signed certificate as a trusted root certificate on a client in response to a Security Alert window. This window opens when you establish a Microsoft Internet Explorer connection to a VPN 3000 Concentrator that is not recognized as a trusted site. The upper half of the Security Alert window shows the following text:

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate. The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

Install the certificate as a trusted root certificate as follows:

-
- Step 1** Click the View Certificate button in the Security Alert window.
The Certificate window opens.
 - Step 2** Click the Install Certificate button.
The Certificate Import Wizard Welcome opens.
 - Step 3** Click the Next button.
The Certificate Import Wizard – Certificate Store window opens.
 - Step 4** Select the “Automatically select the certificate store based on the type of certificate” option.
 - Step 5** Click the Next button.
The Certificate Import Wizard – Completing window opens.
 - Step 6** Click the Finish button.
Another Security Warning window prompts “Do you want to install this certificate?”
 - Step 7** Click the Yes button.
The Certificate Import Wizard window indicates the import is successful.
 - Step 8** Click OK to close this window.
 - Step 9** Click OK to close the Certificate window.
 - Step 10** Click the Yes button to close the Security Alert window.
The VPN 3000 Concentrator window opens, signifying the certificate is trusted.
-

Adding a Security Certificate in Response to a Netscape, Mozilla, or Firefox “Certified by an Unknown Authority” Alert

The following procedure explains how to install a self-signed certificate as a trusted root certificate on a client in response to a “Web Site Certified by an Unknown Authority” window. This window opens when you establish a Netscape, Mozilla, or Firefox connection to a VPN 3000 Concentrator that is not recognized as a trusted site. This window shows the following text:

```
Unable to verify the identity of <Hostname_or_IP_address> as a
trusted site.
```

Install the certificate as a trusted root certificate as follows:

Step 1 Click the Examine Certificate button in the “Web Site Certified by an Unknown Authority” window.

The Certificate Viewer window opens.

Step 2 Click the “Accept this certificate permanently” option.

Step 3 Click OK.

The VPN 3000 Concentrator window opens, signifying the certificate is trusted.

HTTP/HTTPS Management Configuration after Upgrading to Release 4.7.1

By default, HTTP/HTTPS management is enabled on the private interface. To manage the VPN 3000 Concentrator through the public/external interfaces after upgrading to Release 4.7.1 or later, you must explicitly enable HTTP/HTTPS management in those interfaces. You can use the Console CLI via SSH or Telnet, or use HTTP/HTTPS access via the private interface. To do the latter, go to Configuration | Interfaces | Ethernet, click the WebVPN tab, and set the “Allow Management HTTPS sessions” parameter (CSCec37514).

Repairing the CompactFlash in the VPN 3005 Series Concentrator

Because of the manufacturing process problem described in Field Notice 29117, some VPN 3005 Concentrators might have corrupted file systems. This defect might result in failure to save certificates and configuration files. The affected VPN 3005 Concentrators include, but are not limited to, those with serial numbers in the range CAM0708xxxx through CAM0750xxxx, where xxxx is a unique suffix for each Concentrator (CSCed68739, CSCed72955).

Release 4.7.1 automatically detects this problem if it exists on your VPN 3005 Concentrator, but you must do the following procedure to repair the underlying file corruption on the corrupted CompactFlash on a VPN 3005 Concentrator that is running Release 4.7.1:

-
- Step 1** Save the configuration file locally.
 - Step 2** Back up all necessary files to a remote host.
 - Step 3** From the CLI prompt, navigate through the menus to:
Administration > File Management > Reformat Filesystem
 - Step 4** At the prompt, type YES.
 - Step 5** Reload the configuration.
 - Step 6** Reinstall the certificates.suffix for each Concentrator.
-



Note If you perform this repair procedure, there is no need to replace the CompactFlash card in your VPN 3005 Concentrator.

Downgrading from Release 4.7.1

If you need to return to a release prior to Release 4.7.1, do the following:

-
- Step 1** Reload the firmware for the desired release. (Do not reboot yet.)
 - Step 2** Make a copy of the existing configuration file and give the copy a new name (for example, rename it as CON471BK.TXT).
 - Step 3** Delete “CONFIG.”
 - Step 4** Copy the previously saved backup file (for example, CON710BK.TXT) to CONFIG. Do not click Save (otherwise, your original CONFIG file will be overwritten with the running configuration).
 - Step 5** Perform a software reset.
-

Your prior firmware and image are restored.

**Note**

After downgrading, the Concentrator might display errors due to functions in the 4.7.1 software that are not present in earlier versions. You can ignore them.

New Features in Release 4.7.1

This section describes the new features in Release 4.7.1 of the VPN 3000 Series Concentrator.

Network Admission Control Support for RADIUS Authentication

Network Admission Control (NAC) now provides configuration support for a specified RADIUS authentication server (CSCeg84883). This support includes the operation for which to use the server. The operation must be one of the following:

- User Authentication—For user authentication only.
- Posture Validation—For posture validation only.
- User Auth and PV—For both user authentication and posture validation.

This release also improves the following tables:

- The new Active and Total Hold-off column in the NAC Session Summary tables shows the number of EAPoUDP associations lost.
- The NAC Result column, now called “NAC Result Posture Token,” in the Remote Access Sessions tables, shows the state of the host as determined by the ACS server during posture validation (CSCsa62068). Although these are configurable on ACS, typical ACS posture token values are Healthy, Checkup, Quarantine, Infected, and Unknown.

**Note**

If you enabled NAC on a VPN 3000 Series Concentrator running Release 4.7 and you upgrade to 4.7.1, modify the RADIUS server configuration to specify posture validation as the operational use. To do so, change the setting of the “Used For” parameter to “Posture Validation” or “User Auth and PV.”

For instructions, refer to the *VPN 3000 Network Access Device 4.7.0 NAC Administration and Configuration* guide, which is at this URL:

<http://www.cisco.com/warp/public/471/vpn3k-nac-config-471.html>

CIFS Japanese Content Encoding

This release features global character encoding that supports Japanese Shift_JIS characters (CSCed12302) or the Japanese Yen sign (CSCee77590).

The new Character Encoding parameter in the Configuration | Tunneling and Security | WebVPN | Home Page includes the following choices:

- Western European (ISO-8859-1)
(Default setting) With this selection configured, the WebVPN pages display the same way as they do in Release 4.7.
- Japanese (Shift_JIS)
This selection prevents the insertion of the “font-family” into the HTML files. The browser uses the local font associated with its encoding setting. This selection provides accurate handling and display of Common Internet File System (CIFS) file sharing when file names or directory paths might contain double-byte Shift_JIS characters.
- None
Use this selection if the encoding method is not specified or unknown. It also prevents the insertion of the “font-family” into the HTML files. The browser uses the local font associated with its encoding setting. This selection provides support for the Yen sign when another type of Japanese encoding, such as EUC-JP or ISO-2022, is in use. It might also be useful with other languages for which there are character corruption issues.

The CLI “Set Character Encoding” menu line under the Configuration | Tunneling and Security | WebVPN | Home Page menu provides the same function. The choices match those on the Web browser.

The <WebPortal> XML record includes the <charset_encoding> XML tag. The keywords to set the character encoding are as follows:

- none
- western_european_8859_1
- japanese_shift_jis

Usage Notes

This section lists interoperability considerations and other issues to consider before installing and using Release 4.7.1 of the VPN 3000 Series Concentrator software.

Browser Interoperability

Known behaviors and issues with web browsers include the following:

- For best results, use a supported web browser. Currently, the VPN 3000 Concentrator fully supports Internet Explorer 6.0 SP2, Netscape 7.2, Mozilla 1.7.3, and Firefox 1.0 for both administrators and end users. The VPN 3000 Concentrator also supports Pocket PC 2003 for end users.

Using other browsers might cause unacceptable behavior; for example, if you attempt to use an unsupported web browser to manage the VPN 3000 Concentrator, clicking any of the links might open the Login window. (CSCdx87630).

- When File Sharing is in use, Internet Explorer 5.5 closes when you cancel a file open or save operation. With Internet Explorer 5.5, clicking on a file to open or save might close the browser. The browser might also close when you click Cancel when opening or saving the file.

Microsoft has confirmed this problem with the Internet Explorer 5.5. For more information, refer to the Microsoft Knowledge Base article in the following link:

<http://support.microsoft.com/default.aspx?scid=kb:en-us:275290&Product=ie>

To work around this problem, use Save Target As (CSCec51902).

- The appointment reminder might fail when you use OWA 2000 with Internet Explorer.

To prevent this problem, clear the browser's cache.

Browsers: Internet Explorer Proxy With SSL VPN Client and CSD

If you have Internet Explorer configured with a proxy, you must activate the “Use HTTP 1.1 through proxy connections” setting to use the SSL VPN Client, Cisco Secure Desktop (CSD), or any other ActiveX application. If this option is not set, the SSL VPN connection does not come up.

In Internet Explorer, choose Internet Options from the Tools menu. Click the Advanced tab, and under the HTTP 1.1 Settings, check “Use HTTP 1.1 through proxy connections.”

Browsers: Internet Explorer 6.0 SP1 Security Error

When you browse certain sites through WebVPN with Internet Explorer 6.0 SP1, a Security Information Error dialog window shows the following text:

This page contains both secure and nonsecure items. Do you want to display the nonsecure items? Yes/No

Clicking either Yes or No displays the content correctly, and the content is secure. This window opens when you connect to sites that have ActiveX controls and or Java applets. You can ignore the error, or use a different browser (CSCeg69971).

Setting the Secure Connection (Key) Icon

The Key icon indicates a secure connection. Microsoft Windows XP automatically hides this icon among those that have not been recently used. The end user can prevent XP from hiding this icon as follows:

-
- Step 1** Go to the taskbar where the tray icons are displayed and right click the left angle bracket (<).
 - Step 2** Select “Customize Notifications...”
 - Step 3** Select “Cisco Systems SSL VPN Client” and set to “Always Show.”
-

Cisco Secure Desktop and SSL VPN Client

To ensure proper operation of Cisco Secure Desktop and the Cisco SSL VPN Client, follow the DSL and cable routers manufacturer's instructions to upgrade to the latest available firmware revision.

End users of the SSL VPN Client who establish an SSL VPN connection should not click Launch Login Page in the CSD interface.

Cisco Security Agent

The following sections describe known behaviors and issues regarding interoperability with Cisco Security Agent (CSA).

Cisco Security Agent (CSA) Version 4.5 is the only version compatible with the Cisco Secure Desktop (CSD) and the SVC.

When the Cisco Security Agent, Version 4.0, build 119 or greater, is installed on a PC that is attempting to use Port Forwarding, in this case MAPI Proxy, the Cisco Security Agent blocks access to the TCP connection on port 80. If you are using the Cisco Security Agent, you must create a policy to allow access to 127.0.0.x on the specified ports (CSCec06741).

PC Wireless Client Configurations

If a client wireless adapter profile supports scanning for a better access point, and you use the SVC or Cisco VPN Client (IPSec) with that profile, disable such scanning. These scans can cause disconnections or stall traffic on the tunnel. To support scanning for non-SVC/IPSec connections, create another profile.

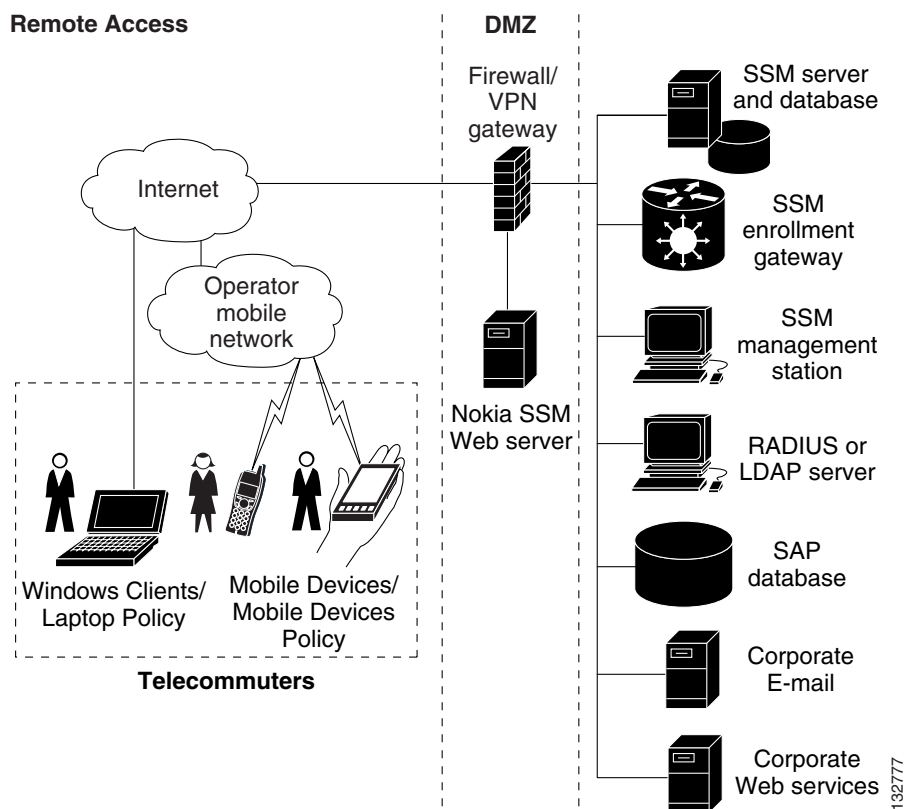
Nokia Back-end Service Requirement

Beginning with Release 4.7, the VPN 3000 Concentrator supports connections from VPN clients on Nokia 92xx Communicator series phones, using the challenge/response for authenticated cryptographic keys (CRACK) protocol.

To enable CRACK authentication, add an IKE proposal with CRACK authentication to the Active Proposals list. The VPN Concentrator includes IKE proposals with CRACK authentication in the default proposal list. Configure the proposals on the Configuration | Tunneling and Security | IPSec | IKE Proposals screen.

The Nokia back-end services must be in place to support both Nokia clients and the CRACK protocol. This requirement includes the Nokia Security Services Manager and Nokia databases (see [Nokia 92xx Communicator Service RequirementFigure 1](#)).

Figure 1 *Nokia 92xx Communicator Service Requirement*



To learn more about the Nokia services required to support the CRACK protocol on Nokia clients, and to ensure they are installed and configured properly, contact your local Nokia representative.

Disable Group Lock When Using SDI or NT Domain Authentication

This feature is supported only when using Internal or RADIUS authentication. See the following page to ensure that you are using this feature properly:

<http://www.cisco.com/warp/customer/471/altigagroup.html>

File Sharing Considerations

The following notes apply to file sharing.

File Sharing currently displays a maximum of 2520 servers per domain or workgroup. For those that are not displayed, you can browse for a server by entering the name of the server in the Network Path entry box (CSCec73349).

With File Sharing, share names can be up to 12 characters long. Share names longer than 12 characters are not displayed. This is a limitation of the CIFS protocol (CSCed21075).

With File Sharing, if a dollar sign (\$) is used at the end of the share name, the shared folder is not displayed. Users also cannot browse this shared resource. This is the proper behavior. According to Microsoft, shares whose names end in the dollar-sign character (share\$) are hidden shares. Users cannot browse these hidden shares (CSCed09634).

“Group Strip” and “Strip Realm” Settings

The Group Lookup capability (for IPsec users) has a switch called “Group Strip.” This switch specifies whether to strip the group from the username when authenticating the username. The default behavior is to “Strip” the groupname.

In releases previous to 4.1, internal authentication always stripped the groupname and external authentication relied on the “Strip Realm” setting with a group delimiter of '@' (! and # groups were not stripped).

If you are using group lookup with external user authentication *and* user authentication is now failing (following an upgrade), check your “Group Strip” and “Strip Realm” settings (CSCec20818).

Hosts File Recovery

Using the Task Manager to terminate Java processes might cause Application Access to fail to terminate correctly when using the SVC. If this occurs, log out and log back in, or reboot.

IMAPS Proxy Opens Multiple Mail Server Sessions without Closing Them

Because of the way IMAP Clients function, VPN 3000 Concentrator administrators and mail server administrators might see multiple sessions from the same source or client (for example, you might see that an IMAPS Session is opened when checking mail and an IMAPS Session is opened when synchronizing folders). This would result in two IMAPS Sessions listed in the session table on the VPN 3000 Concentrator from the same source and two IMAPS Sessions on the mail server with a source IP address of the VPN 3000 Concentrator and the same mail user (CSCec18358).

Kerberos Authentication

Beginning with Release 4.0, the VPN 3000 Concentrator supports authentication to Kerberos/Active directory, which is the default authentication mechanism in Windows 2000 and Windows XP. Kerberos is an authentication protocol for use on untrusted networks. The protocol comprises two stages of authentication--the first level is to a key distribution center (KDC), and the second level is between each client and server.

To configure this feature, you must add a Kerberos authentication server on a group basis or add the server to the global authentication servers list and configure such parameters as server IP address, server port, number of retries, and so on. The IPSec group tab includes Kerberos as an authentication type, and statistical displays also include Kerberos authentication statistics.

Before you use the VPN 3000 Concentrator to authenticate a user to a Linux or Unix server running a Kerberos server, follow these steps:

-
- Step 1** Check the keys available for the user you want to authenticate. Run:
- ```
kadmin.local -q "getprinc username"
```
- Step 2** Make sure that “DES cbc mode with RSA-MD5, Version 5” is one of the available keys. If you do not see “DES cbc mode with RSA-MD5, Version 5,” edit the `kdc.conf` file and add or move `des-cbc-md5` selections to the beginning of the `supported_encyptypes =` line. For example:
- ```
[realms]
MYCOMPANY.COM = {
master_key_type = des-cbc-crc
supported_encyptypes = des-cbc-md5:normal des-cbc-md5:norealm
des-cbc-md5:onlyrealm
```
- Step 3** Save the file. Then, restart the `krb5kdc`, `kadmin`, and `krb524` services.
- Step 4** To create the “DES cbc mode with RSA-MD5” keys, change the users password, as follows:
- ```
kadmin.local -q "cpw -pw newpassword username"
```
- 

Now you should be able to authenticate that user to your Linux/Unix Kerberos 5 server (CSCea20236).

## LAN-to-LAN PIX Default Configuration

If you configure a tunnel between a PIX or ASA 7.0 device and a VPN 3000 Concentrator using the ASDM LAN-to-LAN setup wizard, the wizard selects SHA1 as the default authentication method for IPsec Phase 1 and Phase 2 negotiation. The VPN 3000 Concentrator selects MD5 as its default authentication method. Change the configuration of one of the two devices so that they match.

## NAC URL Redirection

NAC URL redirect does not occur for hosts that use SOCKS proxy. URL redirect monitors ports 80 and 443 for HTTP connections. SOCKS proxy HTTP connections occur on a different port. As a result, the host is either not redirected or it displays a “Page not found” error.

URL redirect is configured on an ACS server and passed to the VPN 3000 Concentrator during posture validation. You cannot change its settings from the VPN 3000 Concentrator.

## Password Expiry Does Not Change User Profile for LAN

To use Password Expiry (which is only for IPSec users), you must enable Start Before Logon on the VPN Client and make sure that DNS and WINS servers are properly configured (CSCdv73252).

## Port Forwarding (Application Access) Considerations

The following notes apply to Port Forwarding (Application Access).

When using the TCP Port Forwarding feature to transmit files at broadband and Ethernet throughput speeds, the downloaded Java applet might use a high amount of system processing power on the client PC (CSCeb38638).

Running Microsoft Visual Studio on a client PC might at times conflict with the Port Forwarding Java applet in WebVPN. If you experience problems, close Visual Studio and restart WebVPN.

TCP Port Forwarding (Application Access) does not work on a Windows ME PC that has Norton Antivirus loaded on it. When you attempt to load the Application Access menu, Norton Antivirus prevents the forwarded TCP ports from being opened or might cause the PC to fail. This is a Norton Antivirus issue (CSCec18162).

## Certificate Revocation List Processing with Cisco SSL VPN Client

A certificate revocation list (CRL) contains a number of certificate serial numbers that have been revoked. The client downloads this list from a CRL server, then looks up the VPN 3000 Concentrator's certificate in the list. The client displays a window to indicate one of the following if it detects an error:

- CRL server is offline  
This message signifies that the server is inside a private network or is down.
- Download or lookup of the CRL has failed

Therefore, Cisco SVC requires a CertificateRevocation key with a value of 1 to enable the checking of the certificate revocation list. Otherwise, a dialog window prompts the end user to accept or deny the certificate that has the revocation error. The following path shows the CertificateRevocation key and value on the end user's PC:

```
My Computer | HKEY_USERS | <Secure ID_of_Logged_User> | Software |
Microsoft | Windows | CurrentVersion | CertificateRevocation REG_DWORD
0x00000001
```

The tunnel client attempts to read the value of the “CertificateRevocation” flag shown above to determine whether the client checks for revocation of the VPN 3000 Concentrator certificate. It logs the following application events to the system Application event log if the registry flag is missing:

```
Function: User Secure ID:
S-1-5-21-1801674531-2025429265-839522115-14761
Return code: 0
File: f:\temp\build\workspace\SSLClient\Agent\ssl.cpp
Line: 1404
Description: unknown

Function: RegQueryValueEx
Return code: 2
File: f:\temp\build\workspace\SSLClient\Agent\ssl.cpp
Line: 1435
Description: The system cannot find the file specified.

Function: FailedToGetCertRevocationFlag
Return code: 0xFE1B0045
File: f:\temp\build\workspace\SSLClient\Agent\ssl.cpp
Line: 1494
Description: SSL_ERROR_WINDOWS_REGISTRY_FAILED
```

To view the Application log, select Control Panel | Administrative Tools | Event Viewer, and select Application Log.

To restore the missing flag, select Control Panel | Internet Options, click on the Advanced tab, and do either of the following:

- Click on the Restore Defaults button near the bottom of the window.  
This option restores all of the options under the Advanced tab to the original settings. To avoid doing so, use the second option.
- Insert a check mark next to “Check for server certificate revocation (requires restart),” click Apply, click OK, and restart Windows.

## WebVPN Considerations

The following notes apply to WebVPN.

If you connect to a website that loads content (such as images) from a second, previously unauthenticated server, the content might not be rendered correctly.

WebVPN clientless mode does not support websites that require authentication for access to content from secondary servers.

When using WebVPN with NAT-T, do not set the NAT-T port to 443.

We recommend using port 80 for NAT-T, as firewalls should allow this.

# Open Caveats

Caveats describe unexpected behavior or defects in Cisco software releases. The following list of open caveats includes any available workarounds. If no workaround is included, none exists.

The list is sorted by identifier number.

**Note**

---

If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II on CCO, select Software & Support: Online Technical Support: Software Bug Toolkit or navigate to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl).

---

The following caveats in Release 4.7.1 are not resolved:

- CSCds44095

The VPN 3000 Concentrator does not allow two or more clients behind the same NAT device to establish an L2TP/IPSEC connection.

- CSCdt08303

When configuring a LAN-to-LAN connection with IOS or PIX, it is important to match the keepalive configuration (both “ON” or both “OFF”). If the keepalive configuration is OFF for the VPN 3000 Concentrator and ON for the IOS device, the tunnel will be established with data.

IOS tears down the tunnel because the VPN 3000 Concentrator does not respond to IOS style keepalives if keepalives are configured to be OFF for the VPN 3000 Concentrator.

- CSCdx47596

Due to a Microsoft limitation, Windows XP PCs are not capable of receiving a large number of Classless Static Routes (CSR). The VPN 3000 Concentrator limits the number of CSRs that are inserted into a DHCP INFORM message response when configured to do so.

The VPN 3000 Concentrator limits the number of routes to 28-42, depending on the class.

- CSCdx89348

The VPN 3000 Concentrator might display the following events during a VPN Client connection:

```
131500 06/20/2002 17:08:34.300 SEV=4 IPSEC/4 RPT=4632
IPSec ESP Tunnel Inb: Packet authentication failed, username:
gray, SPI:
4e01db67, Seq Num: 0000850f. Dump of failed hash follows.
Linksys has been notified about the problem.
```

These events are due to the Client being behind a Linksys Cable/DSL router that was incorrectly modifying the Client's packets, causing them to fail authentication when received by the VPN 3000 Concentrator. The problem is more prominent with LZS compression.

*Workaround:*

Although no workaround currently exists, disabling LZS compression on the VPN 3000 Concentrator helps reduce the number of events. To disable LZS compression on the VPN 3000 Concentrator set the "IPComp" setting on the IPsec tab of the group configuration to "none."

- CSCdy26161

The Microsoft L2TP/IPsec client for Windows 98, Windows ME, and Windows NT does not connect to the VPN 3000 Concentrator using digital certificates.

*Workaround:*

Use Preshared keys.

- CSCdz83332

When switching between tabs under the interfaces section of the html-management page, the action might eventually fail.

If this happens, go back to the interface summary page and drill back down into the desired interface. Everything will resume working again.

- CSCdz87108

The LDAP Authorization failure reasons depend on how the LDAP server implements these error codes. RFC 1777-LDAP states that the LDAP server might not return an error code, therefore in those situations the VPN 3000 Concentrator failure reason is “Invalid response received from server.”

For the case in which the LDAP server *does* return a specific error diagnostic (for example, noSuchAttribute) the VPN 3000 Concentrator failure reason displays the appropriate string.

- CSCeb21763

After logging into the Concentrator using the WebVPN feature from a browser, the banner acceptance pop-up box appears more than once when using the Back button on the browser. Normally, the banner is displayed once, immediately after the user logs in.

Use of the [Back] and [Previous] buttons in Netscape 7.x and Mozilla 1.x always causes the page to be retrieved from the cache, regardless of the browser cache configuration and cache properties of the page sent from the Concentrator. This leads to the situation where the banner pop-up reappears if you click the [Back] button to return to the WebVPN home portal site.

*Workaround:*

Use the Home button on the WebVPN control bar to return to the home portal site, instead of the Back button.

- CSCeb38638

When using the TCP Port Forwarding feature, under very high data transfer rates, the Java applet might run at greater than 50% CPU utilization. The faster the client PC’s CPU, the less of an impact Java has on CPU utilization.

- CSCeb59310

Groups defined with a large list (greater than 10) of WebVPN ACL entries that are erroneous or not DNS-resolvable cause the VPN 3000 Concentrator to consume all the CPU cycles as it tries to parse the ACLs entries. As a result, other tunnel establishment and HTTP(S) management sessions are denied.

*Workaround:*

Verify that the URLs used in the WebVPN ACL definitions are valid.

- CSCeb86147  
RC4-128 SSL encryption, although supported, is not recommended for WebVPN connections due to its very high CPU utilization rate. We recommend that customers use DES-56 or 3DES-168 for encryption, because these methods are hardware-based encryption, unlike RC4-128, which is software based.
- CSCec03101  
If the group drop-down tab is selected on the Monitoring Sessions page, when a monitoring refresh occurs, the main frame goes blank and stays blank even if the administrator selects different links in the left or top frames.  
*Workaround:*  
Do *one* of the following:
  - Logout/login
  - Right-click in the right frame and select “Refresh.”This behavior occurs only with MSIE 6.0. It has not been seen with MSIE 5.0, Netscape 4.78 or Netscape 6.2.
- CSCec09317  
The Master Browser Server option in NBNS is not functional. Name resolution currently works only when using a WINS server.
- CSCec20414  
In some cases, when an OWA user is inviting attendees to a new calendar object, selecting the invite attendees button causes the page to reset. This occurs because the page has not loaded completely. To be sure the page has loaded completely when inviting attendees into a new calendar object, check that the calendar object's start and end time dropdowns have been populated with the current date and time.
- CSCec24244  
When using File Sharing and copying files, there is no confirmation prompt when the file being copied would overwrite an existing file. You must ensure that the file name being added (copied) does not already exist.

- CSCec30364

Selecting the “View” option on certain files in the Admin | File Management table with known windows extensions like “.grp” always fails to display these files.

*Workaround:*

Make a copy of the file with a new file name and then view the newly renamed copy.
- CSCec34817

The VPN 3002, with user authentication enabled, fails to redirect web browser sessions bound to an HTTP redirected interface to a VPN 3002 user login prompt.

If you enter the private IP address of the VPN 3000 Concentrator into a Web browser located on the PC that is authenticating itself with the VPN 3002, then the prefix https:// is appended to the first IP address in the browser drop-down list. When an https is present, the VPN 3002 fails to direct the browser to the login prompt.

*Workaround:*

Delete the “s” from https in the address bar on the browser that is attempting to authenticate with the VPN 3002. Ultimately, the connection is made using https, but eliminating the “s” during the step described above allows you to work around the VPN 3002's failure to offer the login prompt if the “s” is present initially.
- CSCec37257

Using Internet Explorer with File Sharing, users can do only two simultaneous downloads. Icons or action buttons seem to not respond to clicks while the two downloads are in progress. The WebVPN File Share resumes responding when one of the downloads completes.
- CSCec38676

WebVPN does not support Radius with Expiry authentication method in this release.
- CSCec46197

The VPN 3002 Hardware Client intermittently truncates the crashdump file when the device panics due to lack of free memory.

- CSCec46657  
When using OWA/WebDAV over WebVPN, clicking Change Password causes a connection error. It appears that this is an insecure practice on MS Exchange Servers, and MS no longer supports its use.  
*Workaround:*  
Change your password when directly connected to the Exchange Server.
- CSCec47541  
When clicking on a link (for instance, one that is contained in an E-mail message), that link might use the browser window that is running the Application Access Java applet, rendering Application Access useless. The implication of this redirect is that WebVPN Port Forwarding terminates if this window is redirected.  
Microsoft Internet Explorer prevents this. Netscape and Mozilla browsers have this problem and do not provide an option to prevent this.
- CSCec75742  
With File Sharing, download of filenames that contain 2 dots will be renamed. For example, the file filename.v1.zip when downloaded will be renamed to filename[1].v1.zip.  
*Workaround:*  
Manually rename the file in the Save As dialog box.
- CSCec75765  
After upgrading Release 4.0 to Release 4.7.1 or to Release 4.7, the following error events might be generated.
  - SET validation Bad Value Error on alSessionLimit.0.
  - SERVE Bad Value Error.These events are harmless, and if the configuration is saved, then these messages do not appear upon subsequent reboots.
- CSCec77427  
Using the Mozilla browser, after you log out as a WebVPN user, the link to close the browser window fails to close the browser window.  
*Workaround:*  
Manually close the browser window.

- CSCec78536  
WebVPN does not support Java applets that generate http requests. For example, you cannot login to the CiscoSecure ACS application because of this.
- CSCed05959  
Web pages that generate responses where the content between a set of HTML tags exceeds 9K bytes are dropped by WebVPN. As a result, web pages might not be displayed correctly.
- CSCed12191  
With File Sharing, browsing workgroups at times does not display the member servers. The failure is due to slow response from the servers.  
*Workaround:*  
To reach the server, enter its name in the Enter Network Path entry box.
- CSCed14579  
When entering an absolute path to a folder within a share, ensure that the folder name has the correct case. Otherwise, the user cannot view the contents of the folder. For example, if SharedFolder is a sub-folder within a share, the absolute path to this folder in the Network Path entry field must be: \\server\share\SharedFolder.
- CSCed45861  
With File Sharing, using Netscape 4.7, sharenames with spaces are not accessible. Netscape fails to open the shared resource and gives no indication of the failure. This does not occur with the latest version of Netscape.  
*Workaround:*  
Upgrade to the Netscape 7.1 or higher.
- CSCed53867  
In a WebVPN session, within a PDF document, clicking the Acrobat icon in the document's toolbar pops up the warning that proceeding will result in a session logout.

- CSCeg52870

If you click X on the icon toolbar in the OWA2000 Help window on Netscape, Mozilla, or Firefox to close the session, and click OK in response to the “Are you sure you want to close your session?” prompt, the session fails to close.

*Workaround:*

Close the Help window and press the X on the icon toolbar on the main OWA2000 page, or use Internet Explorer SP1, Internet Explorer SP2, or Mozilla.

- CSCeg52910

The Calendar reminder does not function properly when you use the Netscape or Mozilla browsers with OWA 2000.

*Workaround:*

Use Internet Explorer SP1 or SP2.

- CSCeg53550

Microsoft Outlook cannot synchronize offline folders that contain Forms with Exchange over WebVPN Port Forwarding (MAPI).

*Workaround:*

Use the SSL VPN Client to connect.

- CSCeg77653

When a WebVPN ACL specifies that a DNS URL be denied, the error output to a client trying to access the URL is incorrect. It displays a “DNS Error” popup saying, “Unable to connect to server myserver.com. The server might not exist, or access to it might not be allowed.”

- CSCeg79913

If you use OWA over HTTPS and you open or create an appointment in the Calendar component, and click the “Availability” tab, the following error message might appear: “The action can't be performed. End tag ‘head’ does not match the start tag ‘META.’” Likewise, the following error message might appear if you do the same when using OWA 2003 over HTTP: “No entries were found.”

- CSCeh06917

The VPN 3000 Concentrator might display a runtime error message if you use OWA 2000 or 2003 to create a new calendar and click the options on the page before the page fully loads.

*Workaround:*

Wait for the page to load completely before completing the required fields.
- CSCeh30953

The descriptions of the split tunneling and local LAN parameters in the *VPN 3000 Series Concentrator Reference Volume 1: Configuration, Release 4.7* and the Online Help reference only the SSL VPN clients. These parameters apply to both the Cisco IPsec and SSL VPN clients.
- CSCeh31023

The VPN 3000 Concentrator does not properly send filters with rules that use network lists to the Cisco IPsec VPN Client. Consequently, the Cisco IPsec VPN Client does not display them, and uses existing alternate IP addresses or wildcards.

*Workaround*

Do not use filter rules that use network lists.
- CSCeh32391

The Online Help describes a Use Event List option for Events to E-mail. This option is not present.
- CSCeh34359

The LDAP and Radius attributes Tables A-2 and A-4 in the *VPN 3000 Series Concentrator Reference Volume 1: Configuration, Release 4.7* section “Configuring an External Server for VPN Concentrator User Authorization” do not contain the latest list of Release 4.7 attributes.
- CSCeh92590

When you use Internet Explorer to connect to an OWA 2000 server and save a message as a draft, the icon toolbar appears in the body of the message in addition to the top of the page.

*Workaround*

Ignore the redundant toolbar or use Netscape to connect to an OWA 2000 server.

- CSCsa69717

With WebVPN, iNotes displays an unable to process your request at this time warning message when you try to open a new To Do item on the Calendar page.

- CSCsa72004

The LDAP and Radius attributes Tables A-2 and A-4 in the *VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.7* section “Configuring an External Server for VPN Concentrator User Authorization” do not include the new Release 4.7 configuration values of the cVPN3000-WebVPN-Enable-functions attribute.

*Workaround for cVPN3000-WebVPN-Enable-functions description in Table A-2 (VPN Concentrator Support LDAP Authorization Schema Attributes)*

The revised description of this attribute follows:

Attribute Name—cVPN3000-WebVPN-Enable-functions

OID (Object Identifier)—1.2.840.113556.8000.795.2.57

Syntax/Type—Integer

Single or Multi-Valued—Single

Possible Values

1 = URL entry [U]

2 = File access [F]

4 = File server entry (requires File Access) [SE]

8 = File server browsing (requires File Access) [SB]

16 = (Unused)

32 = Port forwarding [P]

64 = Outlook/Exchange Proxy [M]

128 = ACL Apply [AC]

256 = Citrix support [C]

512 = (Unused)

1024 = Auto Applet Download (requires either Port Forwarding or Outlook/Exchange Proxy) [A]

2048 = Enable SSL VPN Client [S]

4096 = Require SSL VPN Client (requires enabled SSL VPN Client) R]

8192 = Keep SSL VPN Client (requires enabled SSL VPN Client) [K]

Enter the sum of service-associated values to enable multiple services. For example, the value 111 enables the following services: URL entry (1) + file access (2) + file server entry (4) + file server browsing (8) + Port Forwarding (32) + Outlook/Exchange Proxy (64).

*Workaround for the cVPN3000-WebVPN-Enable-functions description in Table A-4 (VPN Concentrator Supported RADIUS Attributes and Values)*

The drop-down list consists of options in the following format:

*<Hex\_word>* *<Bitmap>* *<Field\_keys>*

*<Hex\_word>* is the sum of values representing the desired services in the Possible Values column shown in the table above. The drop-down list is in order by ascending value.

*<Bitmap>* is the binary representation of *<Hex\_word>*.

*<Field\_keys>* is a pipe ( | ) delimited list of positions. Each position in the delimited list represents one service. Each position contains a letter (signifying the associated service is enabled) or a dash (signifying the associated service is disabled). The letter matches the one shown in brackets to the right of the service in the Possible Values column in the table above.

The following examples show two entries in the drop-down list:

```
0C41 00110001000001 |-|-|S|A|-|-|--|M|-|-|--|--|-|U|
2DA1 10110110100001 |K|-|S|A|-|C|AC|-|P|-|--|--|-|U|
```

The next example indicates all supported services are enabled:

```
3DEF 11110111101111 |K|R|S|A|-|C|AC|M|P|-|SB|SE|F|U|
```

To set the value of this attribute, refer to the attribute description shown in the table above. Add the decimal values associated with the desired services while noting the associated keys, convert the sum to hexadecimal, and select the hexadecimal value from the drop-down list. Use the *<Field\_keys>* in the drop-down list to confirm the value you select is correct.

- CSCsa83034  
Contrary to the description on the Configuration | Systems | Servers | DNS window, configuring DNS is required for executable installations of the Cisco Secure Desktop client.
- CSCsa85744  
The NAC authentication server configuration does not include Help.  
*Workaround*  
Refer to the *VPN 3000 Network Access Device 4.7.0 NAC Administration and Configuration* guide, which is at this URL:  
<http://www.cisco.com/warp/public/471/vpn3k-nac-config-471.html>
- CSCsa93495  
Release 4.7 or 4.7.1 of the VPN 3000 Concentrator does not support Web portal pages in WEBVPN created using VB script. However, Release 4.1 and earlier work using VB script even though it is not supported.
- CSCsb06794  
WebVPN does not work properly with iNotes Version 6.5.4.  
*Workaround*  
Use IPSEC VPN Client or SSL VPN Client.

# Resolved Caveats

Release 4.7.1 resolves the following issues:

- CSCec36405

In the WebVPN end user Logout screen, the link, “Click here to close the browser window,” does not work with Mozilla 1.4 and Netscape 7.x.

- CSCed12302

Japanese characters in link names and file upload/download dialogs are corrupted in Internet Explorer and Safari browsers. Japanese Shift JIS characters, particularly 0x5c, are not handled correctly.

- CSCee77590

In Japanese, the Yen symbol should be used as a path separator. Currently, the CIFS pages use a backslash as a path separator.

- CSCee87333

A trace route issued from the PPTP/L2TP client always gets a response with the private interface IP address of the VPN 3000 Concentrator displayed, even if the address being traced is not through the private interface.

For example, if one initiates a trace route for the host on the external interface, the result displays the private interface address as the first hop.

- CSCef45520

The vpn 3000 Concentrator incorrectly strips the characters preceding a backslash (\) in a username obtained from an SDI server.

- CSCeg00323

Using an IKE scan utility to send IKE aggressive mode requests can cause the enumeration of the group name.

- CSCeg73754

When attempting user authentication in challenge and response mode, the VPN 3000 Concentrator includes authentication values that do not comply with RFC2865/2868. Subsequently, the RADIUS server disconnects VPN 3000 Concentrator when it issues an authentication request. The noncompliant values are for attributes 6 (service type), 7 (framed protocol), and 66 (Tunnel Client Endpoint).

- CSCeg84883  
The VPN 3000 Concentrator does not support the configuration of RADIUS servers specifically for NAC.
- CSCeg88463  
Using OWA 2003, if you select more than 6 items in a folder and try to delete them, the system might display an error message and deletion fails. This is an intermittent problem.
- CSCeh14595  
The VPN 3000 Concentrator sometimes did not delete the Reverse Route Injection (RRI) route upon the disconnection of an IPsec session.
- CSCeh19581  
The HTML source code might display on some OWA screens when you are using OWA 2000 with WebVPN.
- CSCeh21471  
If you use CIFS to upload a file that is already present on the server, WebVPN overwrites the file without issuing a confirmation prompt first.
- CSCeh39113  
If a disabled interface on the VPN 3000 Concentrator is configured with IP address 0.0.0.0 and netmask 0.0.0.0, and VPN clients get an address from the range in the private IP subnet, and then a VPN client connects, the VPN 3000 Concentrator inserts a static ARP entry with the MAC address of the disabled interface into the ARP table. This results in the presence of two static ARP entries. The VPN 3000 might then issue proxy ARPs with the wrong MAC address toward hosts on the inside that want to communicate with the VPN client.
- CSCeh46295  
The VPN 3000 Concentrator can only use the following format in the extension “CRL distribution points:”
 

```
[1]CRL Distribution Point
 Distribution Point Name:
 Full Name:
 URL=http://.../ia1(2).crl
[2]CRL Distribution Point
 Distribution Point Name:
 Full Name:
 URL=http://.../ia1(2).crl
```

The VPN 3000 Concentrator does not recognize or use entries generated in the Microsoft 2003 Enterprise Server PKI Infrastructure format. For example:

```
[1]CRL Distribution Point
 Distribution Point Name:
 Full Name:
 URL=http://.../ia1(2).crl
 URL=http://.../ia1(2).crl
```

- CSCeh52141

After a user submitted login credentials on the WebVPN Home page, the VPN 3000 interpreted the cookie name “Domain” as a value, dropped the cookie during the mangling process, and reopened the login page of the internal Web server.

- CSCsa41034

The RRI route disappears even though the phase 2 SAs are active. This occurs with multiple subnets on the head end and a single network on the hardware client end. The VPN 3000 Concentrator removes the route if one of the SAs times out.

- CSCsa61867

The VPN 3000 Concentrator might not decrement the Simultaneous IKE counter correctly while under a very heavy load of incoming IKE sessions. This causes a gradual limitation of the total number of IKE sessions that the VPN 3000 Concentrator can negotiate at any one time.

- CSCsa62068

The Administer Sessions summary should display the NAC posture token status.

- CSCsa65275

The VPN 3000 Concentrator blocks the proxy source address 0.0.0.0 sent by non-Unity clients.

- CSCsa66263

The SEP-E module might go off line.

- CSCsa70251

The VPN 3000 Concentrator reports a “login failed, Cisco SSL VPN Client required” message even though it actually registers the session as active, if the all following conditions are true:

- The SSL VPN Client is disabled via the Configuration | Tunneling and Security | WebVPN | Cisco SSL VPN Client path.
- Either the Cisco SSL VPN Client and Required Cisco SSL VPN Client, or the Required Cisco SSL VPN Client, is enabled. These options are under the WebVPN tab inside Configuration | User Management | Base group/Groups.
- A user belonging to the group tries to log in.

- CSCsa73752

The CAPI subsystem sometimes fails. An example failure signature follows:

```
Address function file:line
00027094 CapiBcmLower capi_dm.c:518
```

- CSCsa75009

The Microsoft IPsec policy agent cannot make a connection over a Cisco VPN client to a head-end VPN 3000 Concentrator destined for a server on the internal (protected) network.

- CSCsa81458

The VPN 3000 Concentrator issued the following error during an upgrade of the SVC software:

```
ASSERT: b_free error - BDPtr: 0x0685B800 - SIG1: 0x21524110 -
SIG2: 0x21524110 Assertion: "0" failed, in file buffer.c, line 435
```

- CSCsa84569

Opening large files causes ICA sessions to hang. However, the VPN 3000 Concentrator can support subsequent ICA sessions, depending on the amount of graphics and the sizes of the files.

- CSCsa84636

The WebVPN login page appears if a client machine fails to match CSD criteria.

- CSCsa86510  
The SVC client might lose data or cause other data buffers to be lost.
- CSCsa87679  
URL mangling with a squirrel mail application causes the VPN 3000 Concentrator to fail.

## 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.

## Related Documentation

The documentation updated for this release is limited to these release notes and the *VPN 3000 Network Access Device 4.7.0 NAC Administration and Configuration* guide, which is at this URL:

<http://www.cisco.com/warp/public/471/vpn3k-nac-config-471.html>

Related documents include:

- *VPN Client User Guide for Windows* (for the IPsec Client, not the SSL client)
- *VPN Client Administrator Guide* (also for the IPsec Client)
- *VPN 3002 Hardware Client Getting Started*
- *VPN 3002 Hardware Client Reference*
- *VPN 3002 Hardware Client Quick Start Card*
- *Cisco Secure Desktop Configuration Guide*

# 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

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 the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<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/>

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/>
- Instructions for ordering documentation using the Ordering tool are at this URL:  
[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

# 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](mailto: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.

## Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips,

configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- 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/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

[http://www.cisco.com/en/US/learning/le31/learning\\_recommended\\_training\\_list.html](http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.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 © 2005 Cisco Systems, Inc. All rights reserved.