# Release Notes for Cisco VPN 3000 Series Concentrator, Release 3.6 Through 3.6.8.A

**CCO Date: February 23, 2004**

Part Number OL-5637-01

## Introduction

**Note** You can find the most current documentation for released Cisco VPN 3000 products at http://www.cisco.com or http://cco.cisco.com. These electronic documents might contain updates and changes made after the hard-copy documents were printed.

These release notes are for Cisco VPN 3000 Series Concentrator Release 3.6 and for its incremental "point" releases through Release 3.6.8.A software. Please note that product release numbers are not necessarily consecutive. These release notes describe new features, limitations and restrictions, interoperability notes, and related documentation. They also list issues you should be aware of and the 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.

## Contents

These release notes describe the following topics:



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

# System Requirements

This section describes the system requirements for Release 3.6.x.

## Hardware Supported

Cisco VPN 3000 Series Concentrator software Release 3.6.7 supports the following hardware platforms:

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

## Platform Files

Release 3.6.7 contains two binary files, one for each of two platforms:

- Files beginning with `vpn3000`- support the VPN Concentrator 3015 through 3080 platforms.
- Files beginning with `vpn3005`- support the VPN Concentrator 3005 platform only.

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

If you are using Internet Explorer, use version 5.0, Service Pack 2 or higher.

# Upgrading to Release 3.6.7

This section contains information about upgrading from earlier releases to Release 3.6.7.

When upgrading VPN 3000 Concentrator releases, you must clear the cache in your browser to ensure that all new screens display correctly when you are managing the VPN Concentrator.

**Note** You must also log in and click "Save Needed" to add new Release 3.6.7 parameters to the configuration file. These new Release 3.6.7 parameters are added to the running configuration immediately, but they are not added to the saved configuration until you click the "Save Needed" or "Save" icon in the VPN Concentrator Manager.

Upgrading to a new version of the VPN 3000 Concentrator software does not automatically overwrite the existing configuration file. Configuration options for new features (for example, IKE proposals) 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.

## 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 for VPN 3000 Series Concentrator, page 15 for a description of using this number to locate a particular caveat.

Release 3.6.7 of the VPN 3000 Concentrator software contains several features that interact with corresponding new features in the Release 3.6.x versions of the VPN Client and VPN 3002 Hardware Client software. To get the full benefit of this release you should upgrade your client software as well as your concentrator software. The VPN 3000 Concentrator software, Release 3.6.7, does operate with VPN Client and VPN 3002 Hardware Client versions 3.0 and higher, but you should upgrade these, too, to take full advantage of the new features.

- To use the VPN Client, Release 3.0 or higher, you *must* upgrade the VPN Concentrator to Release 3.0 or higher. The VPN Client, Release 3.0 or higher, does *not* operate with the VPN 3000 Concentrator version 2.5 or earlier versions.
- Do not update the VPN 3000 Concentrator when the system is under heavy use, as the update might fail (CSCdr61206).
- If you are upgrading from Release 3.0 to Release 3.1 or higher 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**)**.

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

### Backing Up the Existing Configuration to the Flash

1. Go to Administration | File Management | Files.
2. Select the configuration file and click Copy.
3. Enter a name for the backup file (in 8.3 format; for example, name it CON367BK.TST)

You have now backed up the existing configuration to the flash.

### 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 Manager).

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

**Note** After upgrading, be sure to clear the cache on your browser. Release 3.6.7 adds features and enhances HTML page layouts. Clearing your browser cache ensures that everything displays correctly and uses the new features and layout.

## Downgrading from Release 3.6.7

If you need to return to a release prior to Release 3.6.7, do the following:

**Step 1** Reload the firmware for the desired release. (Do not reboot yet.)

**Step 2** Rename the existing configuration (for example, rename it as CON367BK.TST).

**Step 3** Delete “CONFIG”.

**Step 4** Copy the previously saved backup file (for example, CON36BKP.TST) 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.

# New Features in Releases 3.6.3 Through 3.6.7

These releases update the VPN 3000 Series Concentrator software to resolve several outstanding caveats. Refer to the appropriate “Caveats Resolved in Release 3.6.x” section of these Release Notes for details for each release.

**Note** Release 3.6.2 was never externally released.

# New Features in Release 3.6.1

This section describes the new features in Release 3.6.1 of the VPN 3000 Series Concentrator. For detailed instructions about how to configure and use these features, see *VPN 3000 Series Concentrator Reference Volume I: Configuration* and *VPN 3000 Series Concentrator Reference Volume II: Administration and Management.*

## Network Extension Per Group

Network extension per group lets a network administrator restrict the use of network extension mode on the VPN 3002 Hardware Client. You enable the use of network extension mode for clients on a group basis.

## Bandwidth Management

Bandwidth management provides a throttling mechanism to all tunneled traffic that limits the maximum amount of bandwidth allowed per group/user (policing) or provides a minimum amount of bandwidth allowed per group/user (bandwidth reservation).

- A bandwidth management *policing* policy limits users to the policed rate. Traffic received by the VPN Concentrator at or below this rate is transmitted, while traffic above this rate is dropped.
- A bandwidth management *reservation* policy reserves the amount of bandwidth configured in the policy for each user.

Policies containing both bandwidth reservation and policing apply on the interface and group level. You must create a policy before enabling bandwidth management. For an overview of bandwidth management, see Configuration | Policy Management | Traffic Management | Bandwidth Policies | Add or Modify in the *VPN 3000 Series Concentrator Reference Vol. I: Configuration*.

To configure bandwidth policies, go to Configuration | Policy Management | Traffic Management | Bandwidth Policies.

To enable bandwidth management on the public interface, go to Configuration | Interfaces | Public Interface and select the Bandwidth Management tab. Check the Bandwidth Management check box, set the Link Rate, and apply a policy to the interface. The policy applied to the public interface is considered the default or global policy for all groups/users that do not have a bandwidth policy applied to their group.

The defined Link Rate must be based on available Internet bandwidth and not on the physical LAN connection rate. For example, if the Internet router in front of the VPN Concentrator has a T1 connection to the Internet, leave the Link Rate set on the VPN Concentrator at the default value of 1544 kbps.

To configure bandwidth policies on a group, go to Configuration | User Management | Groups | Assign Bandwidth Policy. Select the public interface and apply a policy. This page also has an option to reserve a specific amount of bandwidth per group.

To configure a bandwidth policy for a LAN-to-LAN connection, go to Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN and apply a policy.

# DHCP Relay for Wireless Operation (Includes Microsoft VPN Client Route List via DHCP)

The DHCP Relay feature lets wireless clients obtain a network configuration from the corporate network before creating a VPN tunnel. This may be used with the VPN Client autoinitiation feature to obtain a network configuration and automatically connect to the secure gateway when a configured wireless LAN (WLAN) is detected.

To add DHCP, go to Configuration | System | IP Routing.

To configure DHCP Relay, go to Configuration | System | IP Routing | DHCP Relay.

To enable DHCP Relay, you must also assign proper rules to filters in the Configuration | Policy Management | Traffic Management | Filters screen

# DHCP Intercept

DHCP Intercept uses DHCP to provide a Microsoft L2TP/IPSec Client with a Subnet Mask, Domain Name, and Classless Static Routes.

This feature allows the VPN Concentrator to reply directly to the Microsoft Client DHCP Inform message. This is useful in environments in which using a DHCP server for this purpose is not advantageous.

You configure this feature on a per-group basis on the Client Config tab of either the Configuration | User Management | Base Group screen or the Configuration | User Management | Groups | Add or Modify screen.

# Ratified IPSec/UDP Implementation (NAT Traversal)

Release 3.6.1 adds support for NAT Traversal (NAT-T), the new IPSec over UDP encapsulation IETF IPSec Working Group draft standard specification (draft-ietf-ipsec-nat-t-ike-02).

NAT-T lets IPSec peers establish a LAN-to-LAN connection through a NAT device. It does this by encapsulating IPSec traffic in UDP datagrams, thereby providing NAT devices with port information. Multiple IPSec clients behind a NAT/PAT device can connect to the same VPN Concentrator, except Microsoft L2TP/IPSec clients (as noted in the following list). NAT-T auto-detects any NAT devices and encapsulates IPSec traffic only when necessary.

NAT-T has the following limitations and requirements:

- NAT-T can support only one Microsoft L2TP/IPSec client behind a NAT/PAT device.
- You must open UDP port 4500 on any firewall you have configured in front of a VPN Concentrator. This is the destination port for the inbound direction from any source port.
- Because NAT-T depends on UDP port 4500 being available, if a previous IPSec/UDP configuration is already using that port, you must reconfigure that earlier IPSec/UDP configuration to use a different UDP port.

To configure NAT-T globally, go to the Configuration | System | Tunneling Protocols | IPSec | NAT Transparency screen and check the IPSec over NAT-T check box.

**Note** Versions of the VPN Client prior to Release 3.6.1 do not support NAT-T. If you have an older VPN Client, the VPN Concentrator determines that the client is incapable of NAT-T during tunnel establishment and the NAT-T setting has no effect for that particular tunnel. These clients, therefore, continue to work as they did previously.

## LAN-to-LAN NAT Traversal

With Release 3.6.1, you can also enable NAT traversal for LAN-to-LAN sessions. For a LAN-to-LAN connection, you must also check the IPSec over NAT-T check box in the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add or Modify screen.

LAN-to-LAN NAT Traversal has the following limitations and requirements:

- You must open UDP port 4500 on any firewall you have configured in front of a VPN Concentrator. This is the destination port for the inbound direction from any source port.
- Because NAT-T depends on UDP port 4500 being available, if a previous IPSec/UDP configuration is already using that port, you must reconfigure that earlier IPSec/UDP configuration to use a different UDP port.

## Advanced Encryption Standard (AES)

Release 3.6.1 adds support for Advanced Encryption Standard (AES), which is more secure than DES and more efficient than triple DES. It also adds:

- One active IKE proposal, IKE-AES 128-SHA, to the default proposal list.
- Two inactive proposals, IKE-AES 192-SHA and IKE-AES 256-SHA.
- A new default IPSec SA to support the AES algorithm, ESP-AES128-SHA.

If you configure AES on a VPN 3000 Concentrator group, only clients that support AES (such as the VPN Client, Release 3.6.1) can connect to that group.

To configure AES to the Encryption parameter in Tunneling, go to Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN or Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN.

**Note** The VPN Client and the VPN 3002 Hardware Client no longer support DES/SHA encryption. Existing Connection Entry profiles that use DES/SHA can no longer connect. Redefine the connection to use a different encryption standard. See the *VPN Client Administrator Guide* for a list of these standards.

## Support for Diffie-Hellman Group 5

Release 3.6.1 adds support for Diffie-Hellman Group 5 for use with LAN-to-LAN connections or VPN Client connections with digital certificates. You can use DH Group 5 with 3DES.

To configure DH 5 and AES, go to Configuration | System | Tunneling Protocols | IPSec | IKE Proposals.

To add DH 5 and AES to the Perfect Forward Secrecy parameter, go to Configuration | Policy Management | Traffic Management | Security Associations.

## CRL over HTTP

You can now configure the VPN Concentrator to use the HTTP protocol to retrieve a certificate revocation list (CRL) from a distribution point. If you choose HTTP, you must assign HTTP rules to the public interface filter if you access your distribution points through the public interface. For example, enabling this feature supports the use of public key interfaces (PKI), such as Verisign, that require the use of HTTP.

To configure CRL over HTTP, go to Configuration | System | Management Protocols | HTTP/HTTPS.

## CRL Caching

You can configure the VPN 3000 Concentrator to store certificate revocation list (CRL) information in volatile memory (RAM). CRL caching can potentially speed up the process of verifying the revocation status of certificates. With CRL caching enabled, when the VPN Concentrator needs to check the revocation status of a certificate, it first checks whether the required CRL exists in the cache and has not expired. Then the VPN Concentrator checks the serial number of the certificate against a list of the serial numbers in the CRL. If a match exists, the authentication fails.

To configure CRL caching, go to Administration | Certificate Management | Configure CA Certificate.

## Backup CRL Distribution Points

You can now configure the VPN Concentrator to retrieve the CRL from the distribution points specified in the certificate being checked, from a user-specified list of up to five static distribution points, or from a combination of these.During IKE negotiation, if CRL checking is enabled, the VPN Concentrator verifies the revocation status of the IKE peer certificate before allowing the tunnel to be established. CRLs exist on external servers maintained by Certificate Authorities. If you configure retrieval of the CRL from a list of distribution points, the VPN Concentrator tries each in turn until it either finds the relevant CRL or exhausts the list.

To configure backup CRL distribution points, go to Administration | Certificate Management and select the Configure option on the appropriate CA certificate.

## SDI Upgrade (ACE/Agent Enhancements)

Release 3.6.1 updates the implementation of the RSA ACE/Agent on the VPN Concentrator to the RSA/ACE Agent 5.0 release. It supports ACE/Server Replicas (a more advanced primary/backup feature than what was in earlier versions), two-step authentication, load balancing, and group-based support for multiple node secrets.

## Split DNS

Split DNS lets an internal DNS server resolve a list of centrally-defined Local Domain Names (LDN), while ISP-assigned DNS servers resolve all other DNS requests. This feature is used in a split-tunneling connection. You configure LDNs on a Base Group/Group basis.

## Dynamic DNS (DDNS Host Name Population)

Dynamic DNS passes the host name to the central site device, which uses that name in the DHCP address request. This feature allows the DHCP server and DDNS to dynamically populate the DNS records.

## L2TP/IPSec Authentication Enhancements (EAP/TLS, EAP/SDI)

Extensible Authentication Protocol (EAP) lets a VPN Concentrator proxy the authentication process to an authentication server. This feature supports additional authentication options for the Microsoft VPN Client (L2TP/IPSec), including CHAP (EAP/MD5), Smartcards (EAP/TLS), and RSA SecurID (SDI).

Supporting EAP pass-through on the VPN Concentrator means that Microsoft native IPSec clients can authenticate users through Smartcards or SDI tokens.

To configure EAP, go to Configuration | User Management | Base Group or Configuration | User Management | Groups.

**Note** In the PC environment, EAP and Cisco's LEAP are not the same. If you are using Cisco LEAP, you need a Cisco WLAN card.

## MTU Interface Configuration

You can now configure the Maximum Transmission Unit (MTU) to be a value in the range from 68 through 1500 bytes. To configure the MTU, go to Configuration | Interface | Ethernet 123, General tab.

## Secure Copy (SCP)

You can now do secure file transfers using the SCP (Secure CoPy) function over an SSH session. To enable SCP, go to Configuration | System | Management Protocols | SSH and check "Enable SCP".

## LAN-to-LAN Filters on the VPN 3000 Concentrator

Release 3.6.1 lets you configure a filter to apply to the traffic that is tunneled through an IPSec LAN-to-LAN connection. To configure LAN-to-LAN filters, go to Configuration | System| Tunneling Protocols | IPSec LAN-to-LAN.

## Management Interface Enhancements

Release 3.6.1 lets you view version and operating system information (when available) for connected clients and connected user session information. You can also sort by any of the columns in the table. To view these enhancements, go to the Administration | Administer Sessions screen and the Monitoring | Sessions screen.

## NAT over LAN-to-LAN

Release 3.6.1 allows LANs with overlapping or same IP addresses between VPN 3000 Concentrators using static, dynamic, and PAT rules. To answer the need for hosts to communicate across overlapping LANs, the private address space must be translated (NATed).

## IPSec Fragmentation

The IPSec fragmentation policy specifies how to treat packets that exceed the MTU setting when tunneling traffic through the public interface. This feature provides a way to handle cases where a router or NAT device between the VPN Concentrator and the VPN Client rejects or drops IP fragments. There are three options:

- Do not fragment prior to IP encapsulation; fragment prior to interface transmission.
- Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP).
- Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit).

To configure this option, go to Configuration | Interface | Ethernet 123 | General tab. *VPN 3000 Series Concentrator Reference Volume 1: Configuration* explains these options and gives an example of their use.

## Certificate DN Group Matching

In release 3.6.1, you can define rules to match a user's certificate to a permission group based on fields in the Distinguished Name (DN). To specify a policy for group matching by rules, you must define the rules and enable each rule for a selected group that already exists in the configuration. For more information, refer to the description of the Configuration | Policy Management | Certificate Group Matching screen in *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

## IPSec Backup Servers Feature Now Applies to the VPN Client

The description of the IPSec Backup Servers feature in the VPN 3000 Concentrator Series Reference documentation indicates that it applies only to the VPN3002 Hardware Client. The feature now applies to the Software Client as well. For information about this feature and how to configure it, on the VPN Concentrator, see *VPN Client Administrator Guide*, Chapter 1. For information about how to configure Backup Servers in the VPN Client, see *VPN Client User Guide* (CSCdy09630).

## Online Help Enhancements

Online help is now easier to use. Release 3.6.1 provides a global help Table of Contents that lets you view and navigate all available help topics. It also offers a search engine, an index, and a glossary.

## "Username@Group" Can Now Be Sent to Authentication Server When Strip Group Is Disabled

Release 3.6.7.F adds the ability to send a "Group Lookup" username to the authentication server during user authentication. This feature restores the ability that was available as a side effect of having "Strip Realm" disabled and "Group Lookup" enabled with "@" delimiter.

In Release 3.6.7 and earlier releases, the strip realm and group lookup feature overlapped when the group lookup delimiter was set to '@'. A side effect of this overlap was the ability to send "username@group" to the authentication server during user authentication. This later was reported as a caveat (CSCea88995), which now has been fixed. Unfortunately, some customers have been taking advantage of this feature and have requested that the capability be added back.

This restored feature applies only to usernames that are in the group lookup format "user@group", "user#group", or "user!group" and only when "Group Lookup" is enabled.

To use this feature, uncheck the "Strip Group" checkbox on the Configuration | System | General | Authentication screen.

- When "Strip Group" is checked and a username contains a group, the group name is stripped off the username during user authentication.
- When "Strip Group" is unchecked and the username contains a group, the group name is not stripped off the username during user authentication.

# Usage Notes

This section lists interoperability considerations and other issues to consider before installing and using Release 3.6.7 of the VPN 3000 Series Concentrator software.

## Online Documentation

The online documentation might not be accessible when using Internet Explorer with Adobe Acrobat, Version 3.0.1. To resolve this issue, upgrade to Acrobat 4.0 or higher. The latest version of Adobe Acrobat is available at the Adobe web site: http://www.adobe.com.

## Disable Group Lock When Using SDI or NT Domain Authentication

This feature is supported only when using Internal or RADIUS authentication. To ensure that you are using this feature properly please refer to the following URL:
http://www.cisco.com/warp/customer/471/altigagroup.html

## Password Expiry Does Not Change User Profile for LAN

You must enable Start Before Logon on the VPN Client and possibly may need to make sure that DNS and WINS servers are properly configured (CSCdv73252).

# Browser Interoperability Issues

The following sections describe known behaviors and issues with the indicated Web browsers.

## VPN 3000 Concentrator Fully Supports Only Netscape and Internet Explorer

Currently, the VPN 3000 Concentrator fully supports only Netscape and Internet Explorer. If you are using Internet Explorer, use version 5.0, Service Pack 2 or higher. 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 return you to the login screen. (CSCdx87630).

## Internet Explorer 4.x Browser Issues

The following are known issues with Internet Explorer 4.X and the VPN Concentrator Manager (the HTML management interface). To avoid these problems, use the latest version of Internet Explorer (at least version 5.0).

- If you encounter a script error when you try to save your configuration file using Internet Explorer 4.0, reinstall Internet Explorer 4.0, or upgrade to a later version of Internet Explorer. Reinstalling Internet Explorer fixes the problem.
- If you plan to upgrade the firmware on multiple VPN Concentrators at the same time from the same PC, use the version of Internet Explorer on the Cisco VPN 3000 software distribution media or newer. Using an earlier version could cause a failure in one or more of the upgrades.
- When connecting to the VPN Concentrator using SSL with Internet Explorer 4.0 (v4.72.2106.8), you might receive a message box saying, “This page contains both secure and non-secure items. Do you want to download the non-secure items?” Select Yes. There really are no *non-secure* items on the page and the problem is with Internet Explorer 4.0. If you upgrade to Internet Explorer 4.0 Service Pack 1 or Service Pack 2, you should not see this error message again.

  After adding a new SSL certificate, you might have to restart the browser to use the new certificate.

# VPN Client Used with Zone Labs Integrity Agent Uses Port 5054

VPN Clients, when used with the Zone Labs Integrity Agent, are put into a “restricted state” upon connection to the Integrity Server if a port other than 5054 is used. The restricted state simply means the VPN Client is able to communicate only with the Integrity Server; all other traffic is blocked (CSCdw50994).

*Workaround*:

Do *one* of the following:

- Configure the VPN Concentrator and the Integrity Server to use port 5054 when communicating with each other.
- Edit the WEB.XML file in the Integrity directory and search for 5054 (the port that Integrity uses/looks for). Change it to 5000, save, and restart the Integrity Server.

## Administer Sessions Screen Shows Data for Wrong Group

When an L2TP/IPSec connection is established, authentication should behave as follows:

1. The Tunnel Group is authenticated (using the OU field in the Certificate or using the Base Group).
2. The User should be authenticated (using the authentication method of the tunnel group.
3. The User's Group (as defined by the group delimiter option) should be authenticated.

This all works properly, but in the Administration | Administer Sessions screen, the Tunnel Group displays instead of the User's Group (CSCdy00360).

## Long Initialization for SNMP Traps in Releases 3.0, 3.5, and 3.5.1

In Releases 3.0, 3.5, and 3.5.1 of the VPN 3000/3002 products, the SNMP task takes 3-5 minutes to complete initialization after a device reboot. Traps being processed during this interval are queued and sent to the SNMP Management station after SNMP task initialization completes.

However, the cold start trap, normally sent as a result of a device rebooting, is never sent.

In Release 2.5.X, the cold start trap is properly sent to the SNMP Manager after a device reboots (CSCdt01583).

## Windows NT Authentication Servers Can’t Follow Other Server Types in the a Prioritized Authentication Server List

If an Windows NT server follows a non-NT server in the prioritized authentication server list, and the non-NT server becomes unavailable for some reason, the VPN 3000 Concentrator detects this and falls back to the Windows NT server. If the tunnel being established is PPTP or L2TP, the authentication attempt to the Windows NT server also fails.

Therefore, when configuring PPTP or L2TP connections, do not place Windows NT authentication servers behind other types of servers in the applicable authentication server list (CSCdy07226).

## Accessing Online Glossary Requires Connection to Cisco.com

The Glossary button at the top of all Help screens tries to contact univercd at www.cisco.com (the Cisco documentation site). This connection requires connectivity to Cisco's main web site. If your PC does not have a corporate Internet connection or your firewall blocks access, the following error appears when you attempt to access the Glossary:

“The page cannot be displayed.”

To access the Glossary, you must be connected to www.cisco.com (CSCdy14238).

## SNMP Traps VRRPNotifications and cipSecMIBNotifications Are Not Supported

The VPN 3000 Concentrator does not support the VRRPNotifications and cipSecMIBNotifications SNMP traps. You can configure VRRP for these SNMP traps without getting an error message, but the traps themselves are not supported, so no action occurs. The same is true of Cisco IPSec-flow MIB notifications (CSCdx44580).

## RSA Allows a CA to Issue Only One Certificate with any DN

The rekey option to renew an SSL certificate from the RSA CA results in a rejection of the request.

The resubmit/renew feature does work with RSA as long as the certificate being rekeyed or renewed is first deleted from the CA database. RSA does not allow a CA to issue more than 1 certificate with any particular DN (CSCdv27743).

## Rebooting after Installing New Hardware

Delays of about 3-50 seconds in making a VPN connection have occurred on Windows XP Professional Edition and Windows 2000 Professional Edition after adding a new NIC card. If you see problems of this nature, reboot the PC after the initial installation of the NIC card (CSCdv27743).

## Reauthentication on Rekey Interval

If you have enabled the Reauthentication on Rekey feature, the VPN Concentrator prompts you to enter an ID and password during Phase 1 IKE negotiations and also prompts for user authentication whenever a rekey occurs. Reauthentication provides additional security.

If the configured rekey interval is very short, users might find repeated authorization requests inconvenient. In this case, disable reauthentication. To check your VPN Concentrator's configured rekey interval, see the Lifetime Measurement, Data Lifetime, and Time Lifetime fields on the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add or Modify screen.

**Note** At 85% of the rekey interval, the software client prompts the user to reauthenticate. If the user does not respond within approximately 90 seconds, the VPN Concentrator drops the connection.

## Network Lists for CPP Firewall Policy Source and Destination Are Not Supported

The VPN 3000 Concentrator does not support selecting source and destination network lists when defining rules for CPP firewall policy. Instead, you must define the source and destination address in the rule definition (CSCea14152).

## Change to Network List Creation for LAN-to-LAN Configuration

The functionality that allows the administrator to create a network list from within a LAN-to-LAN configuration page has changed.

In previous releases, the administrator could create a network list from within the LAN-to-LAN configuration page. The new method for creating a network list uses a link on the LAN-to-LAN index page to the network list configuration page.

This change was resolves a problem with Reverse Route Injection when the network lists are added from within the LAN-to-LAN page. With the previous method, the routes, corresponding to the network lists that were added via the LAN-to-LAN page, were not present in the routing table (CSCea13002, CSCdz87573).

# Open Caveats for VPN 3000 Series Concentrator

Caveats describe unexpected behavior or defects in Cisco software releases. The following 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.

The following problems exist with the VPN 3000 Series Concentrator, Release 3.6.7.

- CSCds44095

  L2TP over IPSec connections fail if going through a NAT device. During the connection establishment, the VPN Client and the VPN 3000 Concentrator exchange IP addresses. When the client sends what it believes to be the VPN 3000 Concentrator's address (really the NATed address), the VPN 3000 Concentrator releases the connection.

  This is because the address assigned to the interface does not match the address coming in from the client. The same issue exists on the client side. This will not be resolved until the Windows 2000 MS client supports UDP encapsulation.

- 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.

- CSCdt96500

  Multiple simultaneous connections from users behind a PAT (Port Address Translation) device can work, but only if the PAT device uses a unique source port for each simultaneous user's IKE session.

  Some PAT devices use UDP source = 500 for all IKE sessions even if there are multiple simultaneous sessions. This will only allow 1 session to work since the second connection brought up from behind this PAT device will cause the first session to be torn down.

  This is unrelated to whether a PAT device supports "ESP" PAT or whether you are using the IPSec/UDP (NAT) functionality.

*Workaround*:

- Use a PAT device that maps each additional simultaneous session to use unique UDP source ports.
- Connect to different destination Concentrators from behind the PAT device for additional users.
- Use IPSEC over TCP (cTCP) or IPSEC over UDP with NAT-T instead of simple IPSEC over UDP. In order to use either option, the feature needs to be enabled on the concentrator side. NAT-T and cTCP are available in 3.6(1) and later of the VPN Client and VPN 3000 Concentrator code.

- CSCdv26372

  If the phase 2 SA has a lifetime set to 60 - 119 seconds, the VPN Client connection is automatically disconnected. A phase 2 SA lifetime of 120 seconds and higher rekeys properly. This is an issue in the SW client. LAN-to-LAN and hardware Clients work fine.

- CSCdw36613

  In some cases, the Zone Labs Integrity Agent may not properly update on the Windows NT version 4.0 operating system while the VPN Client is connected, policy is changed and re-deployed, and the connection is up. Specifically, if you “Block Internet Servers” under the Firewall Security Rules in the Policy and then Deploy that new policy, a PC running Windows NT version 4.0 receives the updated policy, but it might not put the “Block Internet Servers” setting of that policy into effect.

  *Workaround*:

  Reboot the operating system.

- CSCdx41742

  You cannot reserve group bandwidth based on a percentage.

- CSCdx47596

  Due to a Microsoft bug, 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 Concentrator may display the following events during a VPN Client connection. These events were found to be 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 Concentrator. The problem is more prominent if LZS compression is used.

  *Events*:

  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.

  *Workaround*:

  Although no workaround currently exists, disabling LZS compression on the Concentrator helps reduce the number of events. To disable LZS compression on the 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.

- CSCdy51295

  When specifying the link rate for bandwidth management on an interface, the VPN 3000 Concentrator only permits specifying the range 1544000 - 100000000 bps.

  This renders the feature difficult to use properly when the Internet link is less than T1 speed. We should permit the full range of speeds to allow this feature to be deployed in all environments.

- CSCdy51319

  On the VPN 3000 Concentrator running version 3.6 code, a bandwidth management policy is created with a reservation included, and this is applied to a group. No aggregation is applied to the group (left at 0). Interface bandwidth management is enabled and link rate is set to 1.544 Mbs, and a different group is applied for default users with a reservation only.

  If the reservation amount is then changed on the policy the following error occurs in the log:

  31 11/27/2000 15:43:48.360 SEV=4 BMGT/47 RPT=7

  The Policy [ ADCUsers ] with Reservation [ 102000 bps ] being applied to Group [ ADC ] on

  Interface [ 1 ] exceeds the Aggregate Reservation [ 0 bps ] configured for that group.

  This error does not occur if the policy is first removed from the group, then the reservation is changed and the policy re-applied. No users are connected at the time of the error.

  The reservation should be checked against the aggregate only if aggregation is enabled.

- CSCdy51333

  On a VPN 3000 Concentrator running Release 3.6 code, a bandwidth management policy is created and applied to a group reserving some portion of the link bandwidth using an aggregate reservation. If this reservation is then changed, the previous committed bandwidth is not freed up first when calculating whether enough bandwidth is available for use.

  So, if 600 kbps is reserved from a link of 1544 kbps to start with, and this is then modified to reserve 1000 kbps, an error is generated and the modification is refused. The error shown is as follows:

  83 11/27/2000 16:30:44.620 SEV=4 BMGT/31 RPT=7

  Attempting to specify an Aggregate Group reservation [ 1000000 bps ] on Group [ ADC ] Interface [ 1 ] which added to the current reservation of the interface [ 600000 bps ] exceeds the link rate [ 1544000 bps ] to which it is being applied.

  No bandwidth is reserved by any other policy.

  *Workaround*:

  Remove the aggregate reservation from the group first, and then to apply the new setting.

- CSCdy55175

  When a customer who is using the NT domain for user authentication and has the group name that is defined in the Concentrator the same as the user name in the NT domain server, the VPN Client can no longer connect to the Concentrator after upgrading the Concentrator to Release 3.6.1.

- CSCdy59580

  Cannot perform xauth with a PDC emulator in an Active Directory (AD) environment, when NT is the authentication method from a VPN 30000 Concentrator. In a MIXED MODE environment for Windows 2000 AD setup, using a PDC emulator in the domain for authentication from a VPN 3000 Concentrator does not allow a user to authenticate from a PDC emulator if the length of password is more than 14 characters.

  *Workaround*:

  Do *one* of the following:

  – Use a password shorter than 15 characters

  – Use Radius server for Xauth, and let Radius talk to Active Directory

- CSCdy67982

  The LAN-to-LAN tunnel might drop and get re-established, but the IKE session doesn't get cleared out of the administer sessions screen.

- CSCdy71688

  The VPN 3000 Concentrator does not send the ZoneLabs Integrity Server properly formed markup characters. Ampersands – as well as angle brackets (<,>), apostrophes ('), and double-quotes (") – should be escaped, because they are markup characters. For example: The "&" is not escaped. The result is that a login name of "L&nc&" is sent included in all messages the VPN Concentrator sends Integrity. (The username should be sent as "L&nc&".) Integrity rejects the session, and the VPN Concentrator drops the tunnel.

- CSCdy76967

  Attempting to delete a file from an ftp session into the VPN3000 fails and terminates the ftp session.

  *Workaround*:

  The file can be deleted from the VPN3000 Web Management screen at Administration | File Management.

- CSCdz04141

  After setting up the "config" user in Administration | Access Rights | Administrators | Modify Properties as being able to Read/Write File, this user can't access Administration | File Management. The following message appears:

  > You do not have sufficient authorization to access the specified page.

- CSCdz12638

  In all versions prior to Release 3.6, the Concentrator asked the Client to provide a Domain Name field for Native NT Domain authentication. Since it was believed that this field was not used for anything, this field was removed in Release 3.6.

  To establish a connection in Release 3.6, use:

  > DOMAIN\username
  > password

  instead of the construction used in earlier releases:

  > username
  > password
  > DOMAIN

- CSCdz30124

  The Client might fail to establish an IPsec session if the Concentrator has a larger certificate. TCP encapsulation is used and there is a PAT router between the Concentrator and the Client.

- CSCdz32718

  If CPP, which allows local LAN access, is pushed from Concentrator, the Client allows any traffic from/to the Internet.

- CSCdz34686

  With multiple authentication servers defined, if any are defined by DNS name, and the system fails to resolve any of the servers, all incoming authentication requests will be held off for approximately 45 seconds. For example, the first server in the list was defined as an IP address and was working, the second and third servers were defined as DNS names and did not exist on my network (testing with a customer config). When trying to make a VPN Client IPSec connection, the first and second connection attempts time out, the next 10 or so work, then repeat the time out cycle.

  Testing with servers only defined by IP address did not exhibit this behavior. In fact, servers defined by IP address that did not exist were recorded as being on-line in the event log

  *Workaround*:

  Remove the servers defined by DNS name.

- CSCdz44060

  VPN 3000 Concentrator version 3.6.3 sometimes leaves the RRI route in the Concentrator's routing table, even though the client is no longer connected.

- CSCdz45586

  When connecting a VPN 3015 Concentrator with Cisco VPN Client Software, the VPN connection fails.

- CSCdz66368

  Windows XP becomes unreachable over IP after returning from standby mode if the "Stateful Failover (Always On)" is enabled.

  *Workaround*:

  Disable "Stateful Failover (Always On)".

- CSCea04137

  There is a problem with IPSEC SAs reestablishing after checkpoint initiates a soft reset.

- CSCea07260

  After the public IP address and default gateway have been changed, the VPN 3000 Concentrator does not allow incoming data packets encapsulated by UDP(10000), even if an IPsec session is being established correctly. If you use TCP encapsulation or no encapsulation the problem does not occur.

  *Workaround*:

  Reload the VPN 3000 Concentrator after IP address modification.

- CSCea08566

  Many "IPSEC ESP bad pad length (8) >= buffer length (8)" messages were logged in a syslog.

  Using VPN3000 and PIX EzVPN:

  -Phase 2 SA recreation after an expiration of a SA because of an idle timeout (30min)

  -35 sec after a creation of a new SA after an old SA lifetime Expiration. (Duplicate of CSCdz33769.)

- CSCea08995

  A VPN 3000 Concentrator fails rekey with Microsoft's L2TP/IPSec client for Windows 95 or Windows 98 (oem'd from Safenet).

**Note** NOTE: This does not apply to the “native” MS L2TP/IPSec client, which is included with Win2000, XP, etc.

  This was determined to be a bug in the Microsoft client. The Concentrator always initiates rekeys. When phase 1 rekeys, we send the first main mode packet to the MS client. The Microsoft client responds with a malformed main mode packet.

  The packet that Microsoft sends contains a final payload that has the Next Payload fields set to “vendor-id”. Since the packet does not actually contain a next payload, we fail on the packet and thus fail the rekey. This caveat is a placeholder to track the issue.

  *Workaround*:

  The only workaround is currently to increase phase 1 rekey time(s) to a value that will not be hit. Because IKE will negotiate the lower of the proposed rekey times, this requires a registry change on the client PC(s), as well as a change on the concentrator.

  The registry key is:

  HKLM\Software\IRE\Safenet\Soft-PK\ACL\1\PH1PROPOSAL_xx, where “xx” is the number of the proposal. The default value of these keys is 28800 (seconds) or 8 hours. This value should be changed to a value that is high enough that users will not run into it.

- CSCea11658

  After working for 2 weeks, the following messages can appear on the Concentrator:

  Concentrator memory resources are critical

  It might fail, or you might have to reload the Concentrator manually to free the memory.

- CSCea21796

  The VPN3000 Concentrator will transmit data to exceed the negotiated Max Window Size. If going through a PIX edge firewall, the PIX shuts down the session when the window size is exceeded.

  This occurs only when the ACKs coming back are delayed in transit.

  The default window size for cTCP is 64K. The VPN Client and VPN3002 Hardware Client both generate ACKs at 8K intervals to avoid window issues. In this case the delays in ACK transport are significant enough that the window size is exceeded.

- CSCea41370

  When split-tunnel configured, Windows XP machines with firewall enabled are not able to pass VPN traffic to the central-site concentrator, even though Internet traffic is passing through.

  The Internet Connection Firewall is incompatible because the firewall blocks IPC communication from the VPN Client to the VPN Device Driver. In the firewall log, the log consistently blocks UDP 62515; this is the port used to establish the IPSEC SA.

- CSCea48242

  With the Release 3.6.3.C VPN Client connected to a Release 3.6.7.B VPN 3000 Concentrator, a static route pointing to the exit interface (Ethernet) does not route IPSec traffic to the connected VPN Clients, although it can route cleartext traffic just fine. The route has to point to an exit interface instead of a next-hop router.

- CSCea48668

  A VPN 3060 Concentrator running software Release 3.6(7)Rel:

  failed with Exception Type: 0x00000300/DSI.

  The Concentrator recovered itself after a while with no intervention.

- CSCea50566

  You can access the web admin GUI interface using a MAC OSX machine running IE 5.5 with all updates and java installed. You can get around and configure the device as usual; however, when you click on the live event log link from the left-hand menu options | Monitoring | Filterable Event Log | Live Event Log, the following error appears:

  java.lang.ClassNotFoundException eventlog.class

- CSCea51198

  The VPN Client can connect to the VPN 3005 Concentrator, but cannot reach to a network when the packet matches “tunnel default gateway” route. But when the packet matches “static” route, the VPN Client can reach to the network.

- CSCea52841

  When applying a filter to a vpn group the filter settings don't apply to users of this group when connected.

  *Workaround*:

  Apply the filter to the individual user.

- CSCea55221

  A VPN3005 fails frequently.

- CSCea64917

  A VPN 3000 Concentrator running Release 3.6.7.C fails to generate a full XML file if the Concentrator has more than 15 LAN-to-LAN tunnels configured.

- CSCea65125

  Network Autodiscovery does not work if the VPN 3000 Concentrator is behind a NAT device and the NAT-T feature is in place.

  *Workaround*:

  On the VPN 3000 Concentrator behind the NAT device, do the following steps:

**Step 1** Modify filter rules created for public-to-public. Replace the local address with the NATed address

**Step 2** Enable L2L-NAT

**Step 3** Add static L2L NAT entry: public/0.0.0.0:NAT/0.0.0.0->peer/0.0.0.0,

where 'public' is public IP of the Concentrator behind NAT device, 'NAT' is the public address of the NAT device and 'peer' is the public address of the remote Concentrator.

*Explanation of Workaround:*

Step 1 updates the filter rules that are used to establish the Public-To-Public IPSec SA. The addressing in the rules must be consistent on each side of the tunnel.

This tunnel is used to sent the autodiscovered networks (via RIP). Steps 2 and 3 tell the Concentrator to NAT packets (to the NAT device's public interface) between the peer's public to its public. This is necessary because the peer directs its RIP packets to what the peer believes to be its peer (the NAT device).

Since the filter rule was modified, the NATed Concentrator needs to NAT its RIP packet to match the modified filter rule.

- CSCea68888

  The VPN Concentrator is not accepting client connections.

  After re-booting the VPN 3000 Concentrator, it accepts client connections for some time, then stops accepting client connections.

  *Workaround*:

  Re-boot the VPN concentrator.

- CSCea70412

  You cannot use Split Tunnel with ICF on Windows XP. Microsoft does not allow adding an appropriate filter rule to allow the specific ports needed to use for VPN Client communications.

- CSCea74611

  The VPN 3000 Series Concentrator mibs are improperly posted and do not conform to Cisco standards.

- CSCea79588

  With Cisco Integrated Client Firewall and CPP, when you define (on the Concentrator) a filter with “Default Action” set to “Drop & Log”, the policy looks good on the VPN Client “Firewall” tab, but the default action (drop) is not correctly enforced.

  *Workaround*:

  Choose “drop” as the default action.

- CSCea81088

  Using VPN 3000 Concentrator software Release 3.6.5 or 3.6.7.A, a CRL check fails if the received CRL is empty.

- CSCeb06719

  A VPN 3030 Concentrator froze when telnetting on it. Then it rebooted.

- CSCeb06896

  The circumstances initiating this set of failures are unclear and at this point unreproducible. The customer network had been running for some time without incident. Suddenly, the system crashed several times within a few days. The initial failure occurred when running Release 3.6.7.A, but upgrading to Release 3.6.7.D made no improvements. The customer environment requires tunnels to be terminate on all three interfaces. At some point IPSec compression was enabled for all groups. It's unclear whether this configuration change was made at the time of the crashes. It is clear that disabling IPSec compression restored stability in the customer network.

- CSCeb07283

  A VPN 3000 Concentrator using EAP-TLS and L2TP compression stops encrypting traffic after 2-3 hours, connection stays up.

  The user can connect to the VPN 3000 Concentrator (running Release 3.6.7.Rel) without any problem, using L2TP over IPSec /w EAP-TLS authentication, but after 2-3 hours of traffic passage, the VPN 3000 Concentrator stops encrypting traffic, but doesn't drop the connection.

*Workaround*:

Disable L2TP compression and/or EAP-TLS Auth.

- CSCeb08162

  Clicking apply on any LAN-to-LAN SA causes all LAN-to-LAN sessions to drop.

- CSCeb09587

  If you have a client user and an admin user with the same name, the client user might not be able to connect when the admin user is logged in and the client user has a simultaneous logins set to 1.

  This caveat has been closed because the VPN 3000 Concentrator has a flat namespace. The administrator names should be different from the username for security reasons.

  *Workaround*:

  Do *one* of the following:

  – Use different users name for web and vpn client connection.

  – Set the simultaneous logins on the group to more than 1.

  – Connect from a vpn client before making web connection using the same user.

- CSCeb13767

  In the LAN-to-LAN NAT rules, the VPN Concentrator accepts network/mask rules such as 192.168.1.0/255.255.0.0.

  It should consider this as a typo and either modify it to be 192.168.0.0/255.255.0.0 or it should reject it and warn the user.

- CSCeb36140

  After some period of time the concentrator will fail to take any new connections. Each new incoming connection fails with a time-out in building IKE Main Mode Message 6.

  *Workaround*:

  Reboot the Concentrator.

- CSCeb48289

  VPN3000 crash due to a malformed PPP IP Control Protocol message.

# Caveats Resolved in Release 3.6.8.A

Release 3.6.8.A resolves the following issues:

- CSCec62519

  L2TP and PPTP connections to VPN 3000 running Release 3.6.8 or Release 4.0.2 cause the device to fail.

- CSCec67748

  The following problem occurred on both Release 3.6.8 and Release 4.0.1.C. The primary VPN 3000 Concentrator's interfaces are still primary after being rebooted, even though one of the interfaces is Down.

# Caveats Resolved in Release 3.6.8

Release 3.6.8 resolves the following issues:

- CSCea29828

  HTTP Software Updates sometimes fail with “Software Update Error”. Retrying the operation does not update the image.

- CSCeb30226

  Using a VPN 3060 Concentrator running Release 3.5.5 or 3.6.7.F, when we set VRRP and Master VPN's private interface fails, switchover delay happens at Backup VPN, hence we cannot communicate end-to-end.

- CSCeb72217

  The VPN 3000 Concentrator has a minimum password requirement of 8 characters. This requirement can be bypassed and a local user password can be set to blank by editing the username and removing the password at the same time on the VPN 3000 Concentrator, despite the error about the password not meeting minimum length requirements.

# Caveats Resolved in Release 3.6.7.H

Release 3.6.7.H resolves the following issues:

- CSCdz17373

  A customer is connecting from a 3002 hardware client configured as a PPPoE client to a VPN 3000 Concentrator using an Internet Service Provider. According to the customer, this configuration was working fine until recently when ISP made a change on their side to use PAP instead of MS-CHAP v1 for PPPoE authentication. The customer sees same behavior whether they use 3.6.3, 3.6.1 or 3.5.5.

- CSCeb18649

  VPN Client can't connect using cTCP to the virtual address in the VPN 3000 Series Concentrator using load balancing following a reboot. This issue occurs only in Releases 3.6.7.F, 3.6.7.G, 4.0.1.Rel and 4.0.1.A

- CSCeb22460

  VRRP and IPSec over TCP might not work in Releases 3.6.7.F and 4.0.1., but they work in release 3.6.3.

# Caveats Resolved in Release 3.6.7.G

Release 3.6.7.G resolves the following issues:

- CSCea50428

  A VPN 3000 Concentrator might leak message buffers under the following conditions. This could prevent new connections and possibly cause the device to fail.

  Conditions:

  – DHCP relay is configured.

  – The external interface is used as the public interface.

  - Routing from the DHCP server to the Concentrator's external interface is not through the Concentrator's private interface (that is, the Concentrator is not the default gateway).

- CSCea81010

  When using multiple static CRL servers, if the first server fails without being taken off-line, the subsequent searches also fail.

- CSCea83433

  With authentication set to Radius with Expiry, the user is prompted for username, password and domain name when connecting. The ACS authentication report shows “domain\username”, but the ACS accounting report page shows only the “username”.

- CSCea91878

  The VPN 3000 Concentrator, Releases 3.6.7C, 3.6.7D, and 4.0, sends VRRP messages on the public interface after system shutdown.

# Caveats Resolved in Release 3.6.7.F

Release 3.6.7.F resolves the following issues:

- CSCea45131

  VPN 3002 Ethernet ports might hang intermittently when connected to a Centercom hub.

- CSCea74732

  Changing from DHCP to STATIC on an interface will not stop IP event logs 29 and 34 from showing in the filterable event log.

# Caveats Resolved in Release 3.6.7.E

Release 3.6.7.E resolves the following issue:

- CSCea70449

  The User [user], Group [group] event log message for a VPN Client disconnect is now separated by comma in Release 3.6.7 and later code. In the code before 3.6.7, this comma was not present and the User [user] Group [group] event log message was separated with a space tab format.

# Caveats Resolved in Release 3.6.7.D

Release 3.6.7.D resolves the following issues:

- CSCdu83085

  Autoupdate continues to retry even when tunnel fails.

- CSCdv51097

  The IPSec terminating interface is the External Interface, and the Inside Interface is the Private Interface. The Ethernet 2 (Public) interface has the Public Interface checkbox checked. but the Interface is set to “NOT CONFIGURED”. When this happens, all the IPSec/NAT connections fail by giving the error:

  Could not register UDP port for NAT enabled IPSec!

Unchecking the public Interface checkbox when its not configured or giving it any bogus IP Address resolves the issue, and IPSec/NAT starts working fine.

- CSCdz85885

  The load balance notify packet arrives at the VPN Client before the certificate packet, and this results in a failed connection attempt. The VPN Client sees this as a malformed packet, and the entire negotiation fails.

  The VPN Client does not have the ability to inspect the certificate when it arrives after the load balanced notify packet from the VPN Concentrator. This causes the phase 1 main mode negotiations to fail.

- CSCea47443

  The VPN 3000 Concentrator running 3.6.7 randomly fails after changing LAN-to-LAN rules.

- CSCea58142

  A VPN 3000 Concentrator running Release 3.6.7 is not able to decode the objects in the CA certificate or in the VPN Client certificate.

  The VPN 3000 Concentrator accepts the CA certificate and the certificate for the Concentrator, but in Subject and Issuer, it shows Unknown. When the VPN Client connects, it always ends up in the base group, not in the group matching the OU or group match config.

- CSCdv87793

  If the DHCP Server address pool on the VPN 3002 is modified, it will still renew IP Address from the previous address pool.

- CSCea41973

  After upgrading to Release 3.6.7.A from 3.6.7 Rel, a VPN 3000 Concentrator does not redirect any traffic coming in from a VPN Client to across LAN-to-LAN tunnel.

- CSCea48892

  PIX-to-PIX spoke connectivity when each PIX is connected LAN-to-LAN to a VPN 3015 Concentrator running Release 3.6.7.A is broken.

# Caveats Resolved in Release 3.6.7.C

Release 3.6.7.C resolves the following issues:

- CSCdx27114

  An administrative user who has “Stats Only” permission and who attempts to view users filtered by “Group” on the Monitor | Sessions screen, sees *all* logged-in users instead of a filtered list.

- CSCdz39114

  If a L2L tunnel is initially configured with Auto Discovery then the routing field in the tunnel configuration is changed to 'none' the L2L:AutoDiscovery stays in the network list. If you attempt to remove the entry from the network list, the concentrator goes to 100% CPU.

  The following error message appears in the log file:

  564520 09/06/2002 12:05:47.830 SEV=1 L2TP/60 RPT=3 pSOS q_send failed

- CSCdy40481

  A stable system suddenly started to crash - when removed from the network, the system no longer crashed. The crash dump seems to lead to autodiscovery for LAN-to-LAN tunnels. When autodiscovery is used, each route learned eats up memory by having to create custom (hidden) filters.

- CSCdy79954

  When configuring a load balanced configuration, the shared secret can be set to cisco123. Under the VCA L2L, session a preshared key of ALTIGA is listed. Changing this preshared key results in an error:

  Error updating group for LAN-to-LAN connection (Not Writable Error).

- CSCdy82294

  Cisco 3030 VPN Concentrator running 3.6.1 fails when SDI sockets are depleted. The Concentrator is leaking sockets when the SDI server responses time out (see CSCea08807). This failure is another symptom of that problem.

- CSCdz72398

  Even when the master Concentrator is shutdown, VRRP messages are still sent out. As a result, the backup Concentrator never assumes the master role.

- CSCdz78203

  The following code Assertion might occur on a system using the SEP-E as tunnels are connecting and disconnecting.

  Assertion: “sa->refCnt >= 0" failed, in file fsmact.c, line 4462

- CSCdz82620

  Cisco 501 with Individual User Authentication to Cisco ACS fails. The log message on the VPN 3005 Concentrator is:

  56 01/16/2003 18:55:24.480 SEV=4 AUTH/9 RPT=52
  Authentication failed: Reason = No active server found
  handle = 232, server = (none), user = user

- CSCea00667

  The VPN 3000 Concentrator might fail if you are viewing bandwidth management statistics from the HTML management interface.

- CSCea11996

  If RRI (Client and/or Net extension mode) is enabled or disabled in configuration/system/ip routing/reverse route injection, and generate hold down routes is clicked before apply, the enable/disable changes that were made fail to survive. The changes revert back to what they were set to when you entered the page as soon as gen hold down routes is clicked. If you are observing closely, you may realize that your settings were blown away, before clicking apply. Otherwise, you may be confused as to why the routes are not showing up in the routing table.

- CSCea12413

  A problem can occur with a VPN 3000 Series Concentrator that is authenticating against a Windows 2000 server via RADIUS w/ Expiry option. If a user's password expires, the Cisco Client prompts user for change of password. If the new password meets password requirements, then the rest goes well. If not, then subsequent attempts also fail.

- CSCea12933

  This happens only in Release 3.6.1, but not in 3.0.3, which has also been tested. Release 3.6.1 also works correctly if @ is used as group delimiter.

  If Group Delimiter is selected; for example, #, the external authentication request is sent with the whole UsernameDelimiterGroupname instead the Username only.

  This means no strip-off from Group Delimiter for external authentication. The authentication fails because the Authentication server authenticates based on Username. For example:

  user: Cisco
  group: Test
  Group Delimiter: #
  UsernameDelimiterGroupname: Cisco#Test

  This means that the VPN 3000 Concentrator sends Cisco#Test to the Authentication server instead of Cisco.

- CSCea19992

  Under Monitoring | Statistics | Authentication, the Requests column never gets updated and shows 0. The Accept, Reject columns counter get updated properly.

- CSCea37929

  When using Unit Authentication for 3002s connecting into a Load Balancing Cluster the connection will fail. Connecting to the individual concentrators within the cluster functions properly. This problem only occurs when connecting to the cluster address.

- CSCea37992

  The VPN 3002 cannot establish an IKE tunnel to a central-site PIX.

- CSCea39673

  Incorrect port number is displayed via CLI for VPN 3002 NAT-T connections.

- CSCea42622

  On the VPN Concentrator's group configuration for the VPN 3002, if you have AES-256 and PFS Group 2 configured in the IPSec SA and the 3002 is using NAT-T, PHASE 2 fails to negotiate, and the tunnel never comes up.

- CSCea44988

  When group lookup is enabled and the user enters username<delimiter>group, the group is not stripped off the username before sending it to the accounting.

  For example, "User#MyGroup" would be sent to the accounting server instead of just "User".

- CSCea45176

  A VPN 3002 Hardware Client fails to pass data across a cTCP tunnel for one way streams. This problem occurred because of a TCP windowing issue. The TCP ACKs piggy-back on the ESP data packets. Since data was only going one way, the TCP acks were not being sent. This caused the VPN 3002 Hardware Client to drop new packets (including Dead Peer Detection), and the connection would terminate.

  The peer sends a gratuitous ACK for every 8K of data received. This ACK was getting processed but did not adjust the window. This problem was introduced in Release 3.6.7.B when exceeding window size prevention was added.

- CSCea45961

  The password for the Accounting server will reset when you modify the server data but not the password field. This happens when you select Modify Accounting Server and press apply (without changing any fields).

# Caveats Resolved in Release 3.6.7.B

Release 3.6.7.B resolves the following issues:

- CSCdz01769

  OSPF updates are not populating the routing table on the VPN Concentrator.

- CSCdz48332

  If you add and delete filters through the GUI interface (Configuration | System | Policy Management | Traffic Management | Filters), there is a very small memory leak for each filter created and deleted.

- CSCdz80292

  If the 3002's configuration is changed from DHCP to PPPoE, and the PPPoE username or password is configured incorrectly, after 3 attempts to contact the PPPoE Access Server the 3002 will reboot.

- CSCdz83301

  If a simple password is configured under the OSPF tab in any of the interface configuration pages, the deleted entry reappears, even after deleting the password, selecting none for OSPF authentication, and clicking apply.

- CSCdz84481

  When a user fails authentication due to a restriction placed on the account at the Active Directory server, the Concentrator Events do not display the reason for the failure. Some restrictions on the account could be Account Expired, Account Disabled, Account Locked-Out, Not within Logon Hours and Password Change required. For most of these restrictions you will see the following Events:

  124 01/20/2003 11:12:55.590 SEV=10 AUTHDECODE/43 RPT=4

  Kerberos: Error type: Client's creds have been revoked

  130 01/20/2003 11:12:55.590 SEV=4 AUTH/9 RPT=9 70.139.1.5

  Authentication failed: Reason = Invalid response received from server handle = 196, server = 198.133.219.25, user = myuser

- CSCdz87573

  When a LAN-to-LAN connection is added and the “Create Network List” feature is used, then the routing table fails to get populated with the remote list entries, as it should when Reverse Route Injection (RRI) is enabled.

  If the network lists are constructed first, then the LAN-to-LAN is constructed via the wizard using these lists, then when RRI is applied to the LAN-to-LAN, all entries show up as they should.

- CSCea02277

  When the customer, using VPN3030 with 3.6.5 software, assigns IP addresses, the addresses are allocated on a group basis under the Configuration | User Management | Groups | “hilite the group” Modify Address Pool option. When an entry is deleted from the list, multiple entries are deleted. If you try to enter the second erroneously deleted entry, the VPN Concentrator complains that the network exists in the lists. Rebooting does not solve the problem.

- CSCea02294

  When receiving IKE packets with missing payload(s), events currently only state that the packet had invalid payload(s).

- CSCea07383

  When using split tunneling and routing large frames in-the-clear through the public interface over PPPoE, frames that require fragmentation due to the additional 8 bytes for PPPoE overhead will be dropped. This problem seems to affect only PPPoE connections.

- CSCea25668

  Statically assigned filters take precedence over dynamically assigned filters. It should be the other way around.

- CSCea28425

  Using Kerberos authentication, if you attempt a VPN Client connection and type the username incorrectly or enter an unknown username, the Client simply disconnects and the Concentrator Event Log shows:

  122 02/25/2003 08:08:06.690 SEV=4 AUTH/9 RPT=1 192.168.1.24

  Authentication failed: Reason = Invalid response received from server handle = 19, server = 10.10.0.10, user = IsThisUserHere

  To help troubleshoot Kerberos authentication problems, enable AUTHDECODE up to SEV=10, and you also see this Event:

  117 02/25/2003 08:08:06.690 SEV=10 AUTHDECODE/43 RPT=8906

  Kerberos: Error type: Client not found in Kerberos DB

# Caveats Resolved in Release 3.6.7.A

Release 3.6.7.A resolves the following issues:

- CSCdy09630

  The description of the IPSec Backup Servers feature in the VPN 3000 Concentrator Series Reference documentation indicates that it applies only to the VPN3002 Hardware Client. The feature now applies to the Software Client as well. For information about this feature and how to configure it, on the VPN Concentrator, see *VPN Client Administrator Guide*, Chapter 1. For information about how to configure Backup Servers in the VPN Client, see *VPN Client User Guide*.

- CSCdy12056

  If a LAN-to-LAN tunnel between a VPN 3000 Concentrator and an IOS device is misconfigured and repeatedly fails to establish, then the VPN 3000 Concentrator could enter a state where a reboot is required.

  One way to encounter this problem is to try to set up IOS to handle both LAN-to-LAN tunnels and Remote Access tunnels on the same interface, without breaking the IOS interface into V-LANs. This is a misconfiguration and is not supported by IOS, and it can lead to problems with the VPN 3000 Concentrator.

  This configuration is not supported because IOS does not allow the same crypto map to be used to terminate both LAN-to-LAN tunnels and Remote Access tunnels. In addition, IOS only allows one crypto map to be applied per interface.

Consequently, if both types of tunnels must be terminated on a single physical interface, that interface must be broken out into V-LANs. Dividing the physical interface in this way enables a different crypto map to be applied to each virtual interface. This in turn enables both types of tunnels to be terminated on the same physical interface while maintaining a valid configuration.

- CSCdy26296

  When viewing bandwidth management statistics via the CLI, with Bandwidth Management enabled and multiple users connected, all user sessions scroll through on the screen without the user being prompted to press space to continue or Q to quit.

- CSCdy28464

  Documentation for the Bandwidth Management feature in Release 3.6.1 refers to a configuration option in which bandwidth aggregation is automatically applied to a LAN-to-LAN connection when a bandwidth reservation policy is applied to a LAN-to-LAN connection. This feature is not available in Release 3.6.1.

  To ensure that bandwidth is always available for a LAN-to-LAN connection via the HTML interface, navigate to Configuration | User Management | Groups. Highlight the LAN-to-LAN group, and select the Assign Bandwidth Policies button. Select the public interface, and next to the Bandwidth Aggregation parameter, enter the amount of bandwidth to reserve from the total available bandwidth for this connection.

  If bandwidth aggregation is not set for a LAN-to-LAN connection, a situation might occur where there is not enough bandwidth available for the tunnel to be established.

- CSCdy42970

  The VPN 3002 IPSec tunnel fails to establish if using Perfect Forward Secrecy and NAT Traversal.

- CSCdy67970

  The customer cannot set the filter in a LAN-to-LAN connection to NONE. When we set it to NONE and save the configuration, then go back to LAN-to-LAN and apply a filter, NONE is no longer set. It appears that it inherits the filter from a VPN Group that has that filter applied.

- CSCdy76174

  After upgrade the CVPN3002 from 3.5.2 to 3.6.1, every user gets a script error message, and some users are no longer able to use the Outlook email application.

- CSCdy81949

  When using Certificate Group Matching as described in:

  http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/3_6/config/polmgt.htm#xtocid145

  it appears that in the instance of having a number of distinguished names to match on, such as multiple OUs, we only try to match the rules on the last attribute (OU). Earlier OU's are ignored.

  This occurs when you are using Certificate Group Matching and have multiple OUs in the same certificate.

  If you have a Client certificate with multiple OUs under the “Subject”, such as:

  OU=12345678
  OU=http://www.cisco.com

  and you have defined rules like this:

  ou*12345678
  ou*http

  then messages similar to these appear in the Concentrator logs (class=CERT):

1 10/02/2002 12:10:21.510 SEV=5 IKE/21 RPT=18 192.168.1.1
No Group found by matching IP Address of Cert peer 192.168.1.1

2 10/02/2002 12:10:21.510 SEV=5 CERT/110 RPT=19
Group match for cert peer 192.168.1.1 failed using rule ou*“12345678”

3 10/02/2002 12:10:21.510 SEV=5 CERT/110 RPT=20
Group match for cert peer 192.168.1.1 succeeded using rule ou*“http”

4 10/02/2002 12:10:21.510 SEV=5 CERT/105 RPT=4
Group [TEST-GROUP] found for cert peer 192.168.1.1 by group match rule ou*“http”

If you remove the first rule, you also (trivially) succeed, matching “http” against the second OU.

If you remove the second rule, the connection fails, because 1234578 is not a pattern inside the last OU (http://www.cisco.com)

- CSCdz08568

  If an IPsec policy containing DES appears after policies containing AH, the DES policy is not found. The Concentrator appears to stop matching policies once one containing AH is found.

- CSCdz23351

  VPN 3000 Concentrator may not successfully authenticate users that are externally authenticated with SDI to an RSA ACE Server when the number of retries for the SDI server is configured to 0 on the Concentrator.

  In Configuration | User Management | Groups | Authentication Servers, “Retries” must be set to zero for the problem to occur.

  The problem has been reported in Releases 3.5.5, 3.6.2 and 3.6.4 so far. The problem is confirmed NOT to be present in Release 3.5.2.

  When the Concentrator has not yet received the Node Secret from the ACE, it also fails to install it.

  On the ACE though, you see the messages “Passcode Accepted” and “Node Secret Sent” to the Concentrator.

- CSCdz25612

  When a default gateway is configured, the XML > export > outputs a “dummy” <Route> record with ip/netmask = “0.0.0.0”. This issue occurs when using VPNSC download console to download configuration to the VPN 3000 Concentrator.

- CSCdz25627

  The VPN 3000 Concentrator does not take an empty string for the shared secret. This issue occurs when downloading a full configuration to the device.

- CSCdz31629

  LAN-to-LAN tunnels fail with Null encryption after having tunnelled with AES. LAN-to-LAN, which attempts to negotiate P1 = RSA Cert - SHA1 - AES256, P2 = MD5 - Null or SHA1 - Null, cannot be brought up. This happens only after a previous tunnel has come and gone, using AES.

- CSCdz34486

  During connection establishment, the VPN Concentrator received a framed IP netmask that was not consistent with the address pool defined on the VPN Concentrator. User authentication was via RADIUS, with address assignment being done via internal local pools. The netmask received from RADIUS is being acted upon and used in the computation for determining valid addresses to be issued from the local pool. When the broadcast address, based on the received netmask, was to be issued to an incoming client connection, the connection was rejected.

- CSCdz38146

  The VPN30xx Concentrator tries to interpret ISAKMP/IPSec packets that arrive on the Public interface even if those packets are not specifically destined for it. This occurs only when trying to build a new tunnel over an existing tunnel built with VPN30xx's.

- CSCdz43263

  The Group Delimiter feature is currently not working with a software VPN client. The groupname is not stripped off and the Concentrator tries to authenticate UsernameDelimiterGroupname instead of just Username.

- CSCdz43286

  You cannot use the HTML interface to set the IPSec Encryption to Null on the SA configuration page.

  If you set it to Null, then click Apply, it reverts to the previous value.

  You *can* set it to Null using the console CLI interface. It then appears on the web page as Null.

- CSCdz57202

  HTTP data does not cause a VPN 3002 Hardware Client to initiate a tunnel if cTCP is enabled. ICMP (ping) data does, however, cause the VPN 3002 to initiate the tunnel.

- CSCdz57411

  The VPN 3000 Concentrator sends larger DHCP release packets than RFC 2131 specifications. This causes the external DHCP server drop the packets with “Malformed packets” error messages. In turn, the IP addresses are exhausted in the external server, and nobody is then able to obtain IP addresses from the DHCP server.

- CSCdz59827

  The rollover text boxes do not appear over the SEP and SEP-E on the Monitoring | System Status screen when moving the cursor over the SEPs in the graphic. This works fine for Netscape 4.x and I.E. 5.x. It does not work for Netscape 6.2.1.

- CSCdz62450

  VPN Client connections using cTCP fail to connect after upgrading the client. Changes in the nature of the cTCP code on both the VPN Client and VPN 3000 Concentrator require a concerted upgrade in order to function properly.

  To connect using cTCP, VPN Clients upgraded to Release 4.0 and higher require VPN 3000 Concentrator code Release 3.6.7.a and higher.

- CSCdz62471

  A VPN 3002 in split-tunneling mode does not pass ICMP error messages from the Internet back to the inside host. This may stop functions such as traceroute from working.

- CSCdz63397

  If you attempt to add an existing rule that has been used previously into an existing filter, then click Done, then the Save icon, you might see a crash. Instead of getting the OK box to confirm the save, you may be presented with the outline of the box, after which the Concentrator reboots itself and produces a crashdump.txt file.

- CSCdz72903

  Using the Microsoft L2TP/IPSec VPN Client v1.0 for Windows98 SE, the VPN 3000 Concentrator rekeying phase 2 SA drops the tunnel. When testing with 3.6.3, rekeying phase 2 SA generates a second IPSec session under Administration | Admin Sessions | Remote Access, but the tunnel is still working fine.

- CSCdz79050

  The VPN3000 is not properly supporting the IP NOP and EOL options. It might reject packets that contain these options. These options have a length of 1 and do not contain a length field.

- CSCdz85796

  The VRRP password fails to survive a reboot if the configuration file is encrypted using RC4. Everything works fine if “no encryption” *or* “DES” encryption is used to encrypt the file.

- CSCdz87316

  No connections are accepted when Concentrator reboot is scheduled. When a load balancing Concentrator is scheduled for a reboot, the Concentrator is switched to a secondary role. This causes a problem when all Concentrators in the cluster are scheduled for a reboot, because this leaves no Concentrator as the master.

- CSCdz88326

  An SNMPv2 trap generated by a Cisco VPN 3080 Concentrator does not contain the standard format sysUpTime.

- CSCea04761

  A VPN Concentrator with VPN Group configured with Radius with Expiry and “Simultaneous Logins” set to “1” allows more than one connection.

- CSCea08807

  SDI Servers go off line and do not recover. SDIN sockets remain open. This is a frequent but intermittent problem.

- CSCin30722

  Any text When the MIB variable alSepModuleStatsSlotNum is queried on a VPN 3000 Concentrator with a SEP card, it returns a “No Such Instance” SNMP error.

# Caveat Resolved in Release 3.6.7

Release 3.6.7 resolves the following issue:

- CSCdz23343

  A defect was introduced in the 3.6.6 Release of the VPN3000 Concentrator that causes the Concentrator to stop accepting new connections after 40 cumulative connection failures. On the 3005 & 3015 platforms, the threshold is 15 cumulative failures.

  Once the cumulative failure total is hit, no more IKE requests are processed. Current sessions are not immediately affected, but are not be able to rekey. A system reboot is required to reset the cumulative counter.

# Caveats Resolved in Release 3.6.6

Release 3.6.6 resolves the following caveats.

- CSCdv72688

  When using Quick Config on the VPN3002 to change IP address and enable DHCP, the user is locked out from management access as soon as the IP address is changed.

- CSCdw42380

  When you use the Monitoring Sessions screen or the Administer Sessions screen to configure a VPN 3000 Concentrator with a LAN-to-LAN tunnel to any device through the Private Interface, the tunnel shows up under the MANAGEMENT SESSIONS as VCA/IPSEC, rather than under the LAN-to-LAN Tunnels, as should be the case. The tunnel works fine, as expected.

- CSCdx87630

  Using the Mozilla 1.0 Web Browser to manage the VPN 3000 Concentrator, clicking any of the links always returns you to the login screen. Currently, the VPN 3000 Concentrator only fully supports Netscape and Internet Explorer.

- CSCdy42182

  The VPN 3000 Concentrator failed while freeing memory after telnet session was closed.

- CSCdy51051

  New Pin authentication works correctly when authenticating directly to RSA. If RADIUS is used as a proxy for RSA authentication, then new pin mode fails. This failure occurs when RSA's RADIUS server is used. There is no problem when a Cisco Secure ACS server is used.

- CSCdy55655

  When using Netscape 7.0 with the VPN 3000 Concentrator, after logging in and then trying to configure something, you are returned to the login screen.

- CSCdy74252

  For a VPN 3002 Hardware Client, v3.6 & v3.6.1, you can change PPPoE settings (for example, password) from Quick Configuration, but the changed setting cannot be saved. When you make the PPPoE change and return to the PPPoE setting screen, the Static IP Addressing is checked.

  Changing PPPoE settings is not possible. However, if you change the PPPoE settings from Configuration -> Interface, then you have no problem changing the PPPoE setting.

- CSCdy74667

  The Linux Web browser Mozilla is not compatible with the VPN 3000 Concentrator or the VPN 3002 Hardware Client Web interface.

- CSCdz20934

  If an EZVPN Client does not properly disconnect its tunnel to a VPN3000 Concentrator, its IKE SA is not cleared from the Concentrator. The result is that each lingering IKE SA retains an address out of the address pool.

  This occurs only if the Client connects without xauth authentication.

- CSCdz22107

  When using a Windows XP client connecting to a VPN 3000 Concentrator using split tunneling with EAP, the networks specified in your network list are not passed down and installed into the client computer.

- CSCdz25644

  The XML import did not accept an OSPF router ID of 0.0.0.0, even though OSPF was not enabled. This issue was found when downloading a full configuration to a device via an XML config file import.

- CSCdz29498

  The VPN3000 Concentrator might return fragments of Ethernet packet data within PPP reject messages. This behavior occurs only when a decryption error occurs. The reject message might contain data fragments from other Ethernet packets processed by the VPN 3000 Concentrator.

- CSCdz40860

  The VPN 3000 Concentrator failed when exporting XML file under File Management with L2L with Auto discovery configured.

- CSCdz48220

  The VPN 3000 Concentrator continually requests the node secret from the RSA server. These requests are considered as failed login attempts by the RSA server; therefore, the user's account is disabled. This problem occurs under the following conditions:

  – The 3000 does not have the node secret stored locally.

  – The client provides an incorrect passcode.

# Caveats Resolved in Release 3.6.5

Release 3.6.5 resolves the following caveats.

- CSCdy86096

  A VPN 3000 Concentrator, upon a DHCP renewal, sends the request to the router's address instead of the IP address of the DHCP server.

- CSCdz18271

  Potential buffer overrun in MPPC decompression. MPPC decompression requires additional error handling.

- CSCdz21459

  A VPN 3000 Concentrator crashes when a new virtual interface is created for L2TP and PPTP connections.

  This issue was introduced by the fix for CSCdv71158 (Disabling VRRP on a VPN 3000 Concentrator does not refresh the interface MAC address).

# Caveats Resolved in Release 3.6.4

Release 3.6.4 resolves the following caveats.

- CSCdt54337

  Load Balancing Cluster Address should reply to pings for troubleshooting purposes.

- CSCdv71158

  When a VPN 3000 Concentrator is configured for redundancy (VRRP), and then the IP address of an interface is changed, and VRRP disabled afterwards, then the MAC address of the changed interface remains the VRRP address instead of changing to the physical MAC address.

  To avoid this issue, disable VRRP before changing the IP address of an interface, and re-enable it afterwards.

- CSCdw09946

  If a default gateway is not defined on the VPN 3000 Concentrator, the following event is generated:

  73 10/18/2001 11:53:52.430 SEV=4 IKE/2 RPT=13 82.171.0.5

  Filter missing on interface 0, IKE data from Peer xx.xx.xx.xx dropped

  This may not be the only thing that causes this event to be generated, but it is one of the scenarios.

- CSCdw72102

  If you create a rule with TCP port of 138 NetBIOS, then you save the rule, and then go back and in and view the rule, you will see that the rule has changed the port to TCP Port 137 NetBIOS Name Service.

- CSCdy18645

  AAA authentication for an admin account fails using TACACS+ if Simultaneous Logins in the Base Group is set to “0”. It works fine if it is set to any positive number. The default is 3.

- CSCdy40109

  When a VPN Client (version 3.6) connects to a VPN 3000 Concentrator (running 3.6 code as well), using Entrust Entelligence (version 6.0) certificates, the username is not displayed under Administration | Administer Sessions and/or Monitoring | Sessions.

  This behavior occurs only when using a certificate serial number with a name in the CN field. For example, CN=First Lastname + serial number...

  If the CN field includes only the Name (without a serial number), the username is displayed correctly under Administration | Administer Sessions and/or Monitoring | Sessions.

- CSCdy74304

  Rare, intermittent VPN 3000 Concentrator failures without any patterns occur during IKE negotiation.

- CSCdy88797

  After upgrading VPN3000 Concentrator to release 3.6.3, tunnels do not negotiate to AES.

- CSCdy80300

  VPN Client logon to a VPN 3000 Concentrator running Release 3.6.1, using RADIUS for authentication, fails when the VPN 3000 Concentrator assigns the IP address, and the RADIUS server passes back a Framed-IP-Netmask of 255.255.255.255. The error message is:

  “Bad refCnt (1) or invalid assigned ip address received (x.x.x.x).”

  Hardware clients are able to connect. Local authentication works.

  All address allocation is via static pools configured for each group, no addressing comes from the RADIUS server. Under 3.6.x, the user is phase2 authenticated, but then authentication fails.

- CSCdy87378

  Cisco VPN 3000 Concentrator can not connect with some third-party devices; for example: Furukawa Denko FITELnet-F40. The VPN 3000 Concentrator required that the third Aggressive mode packet be encrypted. In versions prior to 3.6.Rel, this was not required. The VPN 3000 Concentrator now accepts the third Aggressive mode packet, either encrypted or unencrypted.

# Caveats Resolved in Release 3.6.3

Release 3.6.3 resolves the following issues:

- CSCdu74128

  SNMPv2 traps miss the standard snmpTrapOID.0 object.

- CSCdv89254

  The VPN Client might fail to connect to a load-balanced VPN 3000 Concentrator if it receives out-of-order packets from the VPN 3000 Concentrator.

- CSCdx12383

  With local authentication or split-tunneling enabled, a VPN 3002 stops passing voice traffic after about 9-15 hours of normal operation. All other traffic passes through without a problem.

- CSCdx67737

  In VPN 3000 Concentrator software, v3.5, the word “VPN” can not be used as group name. The tunnel fails to establish. There is no such problem in the v3.0 software. Any other name, even one using “Vpn” or a similar upper/lower case variant works.

- CSCdx74374

  Release 3.5.2/3.5.3 of the VPN 3000 Concentrator does not work with the NETWARE DHCP server. In 3.5.x, when the VPN 3000 Concentrator receives the same IP address from the DHCP server, it never sends the reject; it just fails the connection. On the other hand, in Release 3.02, when the VPN 3000 Concentrator receives the same IP for the second client, it sends a reject to the DHCP server and successfully retrieves a second, unique IP address.

- CSCdy09539

  When obtaining an IP address and DNS server attributes via PPPoE, the VPN 3002 might fail to resolve DNS host names, causing the VPN 3002 PING utility to fail, and IPSec VPN tunnels to fail to negotiate.

- CSCdy15762

  A view-only administrator session can lock the configuration on a VPN 3000 Concentrator, not allowing an administrator with authority to make a change for a certain time period. To avoid this issue, reboot the VPN 3000 Concentrator or locate the view-only session and log it off.

- CSCdy18819

  Maximum connect timeout value does not work.

  After setting the maximum connect tim out value to 6 hours, the VPN Client connections do not terminate. They are seen to be live for more than 6 hours.

  The maximum connect timeout applies only to each SA. This leads to the issue where SAs started at different times (for example, during split-tunneling) would prevent the connection from terminating. The connection terminates only when the last SA is torn down.

  The code has been adjusted to reduce an SAs lifetime by the current uptime for the connection, so no new SAs are permitted after max connect is exceeded. This causes all SAs to expire at max connect.

- CSCdy26332

  The VPN 3002 might ignore some Cisco Discovery Protocol (CDP) messages because of checksum errors. The VPN 3002 uses the CDP messages to detect IP Phones on its private network.

  This occurs because of an error in the checksum algorithm in the CDP packet with respect to odd length packets.

  The error checksum algorithm is now part of the standard, so the VPN 3002 should be updated to this algorithm.

- CSCdy26579

  An HTTP 401 Unauthorized error appears on the console when trying to access the VPN 3000 Concentrator through a web browser using admin access, even when administrative rights are given to admin user.

  The two events HTTP/9 and HTTP/10 might appear when a user connects to the login page. These are not errors but HTTP status information. As a result, their severity will be lowered from warning(3) to informational(5).

- CSCdy29543

  Automatic backup of log files through FTP is failing to a 3COM FTP/TFTP server. The resolution for caveat CSCdy20464 did not solve the problem. Customer is using 3COM 3CDAEMON version 2.0 release 10 and the FTP server is still rejecting the binary command.

- CSCdy35638

  IP Phone_a is talking to IP Phone_b. When IP Phone_a mutes the conversation, it stops transmitting packets as the codec goes into receive-only mode. IP Phone_b continues to transmit to IP Phone_a. However, after 5 seconds, IP Phone_b can no longer be heard at IP Phone_a, because the PIX firewall has stopped transmitting packets from the outside to inside interface, and this was caused by the TCP windows being exceeded.

- CSCdy36342

  The range displayed in the error message for IPSec SA Lifetime Time is wrong. It displays “IPSec Time Lifetime out of range. (10 - 2147483647)”.

  The range should be “IPSec Time Lifetime out of range. (60 - 2147483647)”. It was displaying Lifetime KB range.

- CSCdy36609

  IKE rekey may fail if IKE rekey is set to 60 seconds.

- CSCdy37701

  In very rare situations, when connecting via HTTP or HTTPS (SSL) management session, LAN to LAN sessions and Remote Access Sessions are not displayed under Administration | Administer Sessions and/or Monitoring | Sessions. This appears to happen for sessions with SINGLE QUOTES (') in the name.

  Telnet, SSH, or console connections successfully display the remote access and LAN to LAN sessions. Remove the SINGLE QUOTE (') from the site name.

- CSCdy37743

  With the Mac OS X IE browser, when looking at logged in users under the session management screen, 127.255.255.255 is seen instead of the correct IP address in some cases.

- CSCdy38726

  VPN Hardware Client 3002 with version 3.6 does not negotiate the correct MRU that is configured in the interface configuration. It always tries to adjust the MRU to 1492.

- CSCdy38856

  When a VPN 3002 is placed behind a PIX firewall with IPSec over TCP connection to a VPN 3000 Concentrator, we cannot bring the connection up once the VPN 3002 is rebooted.

This occurs because PIX firewall has an active TCP connection which was never reset; when the 3002 comes up it uses the same source and destination port number to make the new connection. The sequence number for the packets does not match the previously active connection, and PIX drops the packets. To avoid this issue, clear the connection on the PIX using the clear xlate command.

- CSCdy39675

  When users try to enroll a VPN 3000 Concentrator or VPN 3002 Hardware Client to a Verisign Onsite CA using a file-based method, the Verisign enrollment application complains about the PKCS10 request generated by the VPN 3000 concentrator (the error ID on Verisign enrollment page is 105).

  The issue is reported only in versions 3.5.4 and 3.6. Downgrading the VPN 3000 Concentrator or VPN 3002 Hardware Client to a version earlier than 3.5.4 and enrolling to the CA works fine. After the enrollment, the VPN concentrators then can be upgraded to higher version if needed.

- CSCdy41307

  Internet Explorer does not display any remote access users in the admin or monitoring session tables if any user specifies a domain upon connecting.

  The table is displayed in Netscape but the separating '\' is not displayed.

  For example: User: test Domain: Lab.com

  should be displayed in the table as Lab.com\test, but Netscape displays it as Lab.comtest.

- CSCdy49334

  The VPN 3000 Concentrator might fail with an out-of-memory error during heavy memory usage. During heavy memory usage, memory was not being properly freed.

  The crashdump exhibits the following symptoms:

  – ASSERT >> Malloc() failed

  – Memory corruption detected with TID = [0x00000000] and Size = [0]

- CSCdy52196

  VPN 3000 Concentrator can fail with cTCP client and a large network list.

- CSCdy52938

  Cannot Set Access Session Timeout to 0, although the error message says that 0 is within the acceptable range.

- CSCdy57163

  The VPN 3000 Concentrator fails to install CA chains if any two of the certificates are identical in the first 4 bytes of their serial numbers.

- CSCdy58124

  Given the following setup:

  NT PDC---vpn3k---Internet

  When we configure a group with the same name as a domain username and then test the authentication against the NTPDC, it fails.

  This is not a valid configuration. Users and groups cannot share common names.

CSCdy62382

When the administrator enters username/password after configuring TACACS authentication for Administrator access to the GUI, the VPN 3000 Concentrator fails.

This occurs if other TACACS attributes are assigned besides “priv-lvl”.

- CSCdy64996

  A VPN 3000 Concentrator, renewing DHCP, sends the request to the broadcast address (255.255.255.255) instead of the IP address of the DHCP server.

- CSCdy73188

  In version 3.6, int_12, under session details (3060) for a remote access session (Hardware or software client), the Auth mode for the IKE session displays “other” when it should be “Preshared Keys - XAUTH”. The session details under CLI correctly displays 'Pre-XTH.

# Caveats Resolved in Release 3.6.1

Release 3.6.1 addresses multiple vulnerabilities for the VPN 3000 Series Concentrators and VPN 3002 Hardware Client. Please refer to the following URL for the details on the vulnerabilities addressed.

http://www.cisco.com/warp/public/707/vpn3k-multiple-vuln-pub.shtml

Release 3.6.1 contains the same fixes as Release 3.6, listed in the following section.

# Caveats Resolved in Release 3.6

This section lists caveats resolved since Release 3.5. If you have an account on CCO you can check the status of any caveat by using Bug Navigator II.

To reach Bug Navigator II on CCO, choose Software & Support: Online Technical Support: Software Bug Toolkit or navigate to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

- CSCdt41281

  Packets coming through a tunnel from a client to a host on the public interface network exit through the Public Interface.

- CSCdv86906

  When using RADIUS authentication, if you are running RIP routing on the Private network, the NAS-IP-Address in the RADIUS Authentication is the IP address of the Private Interface on the Concentrator.

  If you are running OSPF Routing on the Private network, the NAS-IP-Address in the RADIUS Authentication is the IP address of the Public Interface on the Concentrator.

  If you are using OSPF, the NAS-IP-Address is set to the interface with the IP address that has the highest numeric value. For example, if the Private Interface of the VPN Concentrator has the IP address 192.168.10.1, and the Public interface has the IP address 193.111.20.8, the NAS-IP-Address is set to the public interface.

- CSCdx05024

  The phase 1 rekey interval is missing from session management on the VPN3000 series concentrator for Site-to-Site tunnels that are established against IOS devices, if the IOS Device initiates the tunnel.

- CSCdx26088

  Older versions of Netscape (v4.xx) might not properly display the session table from the Monitoring | Sessions link.

- CSCdx26360

  The session management tables might display slowly if there are thousands of users in the VPN Concentrator. HTML pages might take up to a minute or more to display. We are attempting to improve this performance prior to release.

- CSCdx39665

  Full bandwidth availability to a single user (bandwidth stealing) does not yet function to full capacity. User will only be given the amount of bandwidth reserved or policed in their policies.

- CSCdx54510

  The HTML management interface allows an administrator to enter an invalid Router address when configuring Static Routes. The administrator should verify addressing when entering Static Route information.

- CSCdx59201

  Full implementation of bandwidth management statistics has not been completed for this first beta release and should not be tested.

- CSCdx60280

  Bandwidth management statistics for a PPTP user are set to all zeros if bandwidth management is disabled.

- CSCdx60297

  Using Auto-initiate to connect the client before logging into a domain on Windows 95 may result in no VPN Client tray icon appearing (yellow padlock). The client is connected and can be launched from the start menu to view status or disconnect.

- CSCdx61539

  When sorting the session table from HTML management, the Web-browser sometimes stops responding if there are a lot of sessions in the table. (>1000) This behavior may require restarting the browser or, in rare instances, rebooting the management PC.

- CSCdx61917

  The concentrator may assert in memory.c line 554 during a very heavy load of calls connecting and disconnecting while using CRLs and doing a dial-hang test.It is unlikely that a beta site will see this unless the load on the box is very high.

- CSCdx61924

  In version 3.6.1, disabling DHCP Proxy from the following VPN Concentrator management page will also disable the Concentrators ability to retrieve an address off the network using DHCP.

  Configuration | System | IP Routing | DHCP Proxy

  If the Concentrator is using DHCP on any of its interfaces do not disable DHCP Proxy at this page. If DHCP Proxy must be disabled, simply uncheck the “Use DHCP” option form the Address Assignment page located at.

  Configuration | System | Address Assignment | Assignment

- CSCdx62695

  A very heavy load of calls connecting and disconnecting while using CRLs and doing a dial-hang test might cause the Concentrator to fail. It is unlikely that a beta site will see this unless the load on the box is very high.

- CSCdx63294

  Starting and stopping FTP Proxy sessions over LAN-to-LAN-NAT tunnels may cause the VPN 3000 to reset, if using static and dynamic rules.

- CSCdx63962

  If you set the reserved bandwidth for a group equal to the link rate, the result is that no tunnels are established to the VPN Concentrator for that group.

- CSCdx65133

  Interface NAT rule configuration via CLI doesn't automatically disable FTP Proxy when disabling TCP Proxy. Use HTML to disable TCP/FTP Proxy.

- CSCdx66535

  The VPN concentrator reboots if an L2TP connection is attempted to the concentrator with Bandwidth management enabled.

- CSCdx66566

  When the sorting tabs are clicked on in admin/sessions, while both RAS and LAN-to-LAN sessions are being displayed, the LAN-to-LAN summaries table appears distorted. Specifically, the LAN-to-LAN entries lose the Bytes Received column and the “Action” entries are shifted two columns to the left.

- CSCdx69618

  HTML quick config allows the administrator to configure DHCP address pool assignment without specifying a DHCP server. This does not work, because DHCP broadcasts are not supported. All DHCP requests must be directed.

- CSCdx70385

  The session management tables may show very large summary statistics at the top of the html page after a reset of statistics followed by a refresh. The number is in the vicinity of 4.3 billion. This is due to the fact that the number of calls has gone down after resetting the counter to zero. We do not currently display negative numbers for current call count statistics, so negative numbers are erroneously being displayed as large positive numbers.

  of the route; if more are configured they are not be sent.

- CSCdx70496

  Occasionally a client connects and cannot receive any data back from the concentrator. If you see this problem, it usually clears when the client disconnects and reconnects.

- CSCdx72825

  If you change the default pre-fragmentation setting on the public interface on the VPN Concentrator, pre-Release 3.6.1 clients (Unity and 3002) fail to pass large packets after a Phase 1 followed by a Phase II rekey. To correct this problem, disconnect and re-establish the tunnel.

- CSCdx83474

  The remote access session table is not properly displayed when using Netscape 4.78 or 6.2 and viewing the admin sessions table.

- CSCdx85695

  In Release 3.6.1, the VPN 3000 Concentrator software implementation changed the way that the VPN 3000 Concentrator sends its phase 1 ID. This ID consists of a bundle of information including IP address, protocol and port number. The change is that the port is now set to ZERO, whereas before, it was set to 500.

Technically, this is legal because it is up to the peer's policy to enforce whether a port=0 (ignore) is allowed.

- CSCdx86604

  Enabling bandwidth management with client tunnels already established is not supported in the Beta 2 release.

- CSCdx88812

  You may see the following message on the Concentrator console when a VPN client is attempting a connection:

  "RMLogError: bad state=5/event=4 combination".

- CSCdy08702

  When a RADIUS server is configured to Authenticate a Group and return Group attributes, the VPN 3000 Concentrator does *not* check for illegal characters in the attribute "Split-DNS-Names". So, when configuring multiple Split-DNS-names in the RADIUS server, you *must* separate multiple names with a comma without any spaces or other illegal characters.

# Documentation Updates

The Cisco VPN 3000 Series Concentrator documentation set has been revised for this release and is available online through Cisco.com. This section contains any changes and corrections to the documentation that occurred after the documentation was published.

## Documentation Changes

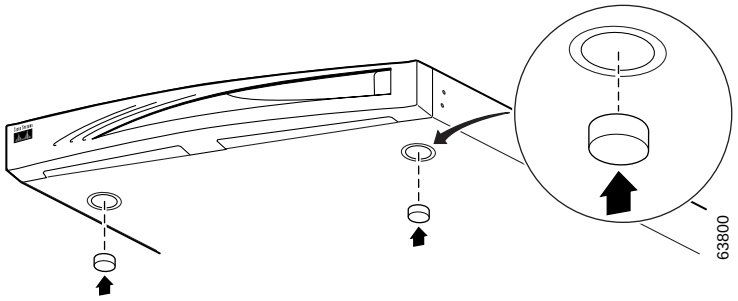
The following documents require modifications, reflecting product changes, as noted in the following sections:

- *VPN 3000 Series Concentrator Getting Started*
- *VPN 3000 Series Concentrator Reference Volume I: Configuration*
- *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring*

### Change to *VPN 3000 Series Concentrator Getting Started*

The method of attaching the feet to the VPN 3000 Series Concentrator has changed. The following illustrations replace those in Figure 2-3, page 2-7 of the VPN 3000 Series Concentrator Getting Started book, version 3.6.

**VPN 3005**




**VPN 3015 - 3080**

## Change to *VPN 3000 Series Concentrator Reference Volume I: Configuration*

The VPN 3000 Concentrator now supports syslog servers on both Windows and UNIX (Linux and Solaris) operating system platforms. In *VPN 3000 Series Concentrator Reference Volume I: Configuration,* Chapter 10, "Events," and in the corresponding online Help, the text and the screen captures refer to UNIX syslog servers. This restriction on the type of syslog server operating environment no longer exists.

## Changes to *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring*

Add the following text under Administration | Access Rights | Access Settings:

DES = Encrypt sensitive entries in the CONFIG file, using DES encryption. A CONFIG file that is encrypted with DES can be used only by the VPN Concentrator that encrypted it. This option prevents the sharing of encrypted configuration files across different VPN Concentrators.

**Note** Note: If a VPN Concentrator that is using a DES encrypted CONFIG file totally fails, all encrypted information is lost

## VPN 3000 Concentrator Documentation Updates

In addition to these Release Notes, the following documents are new or have been updated for Release 3.6. They have not been changed for the subsequent "point" releases (such as 3.6.6):

- *VPN 3000 Series Concentrator Reference Volume I: Configuration*
- *VPN 3000 Series Concentrator Reference Volume II: Administration and Management*
- *VPN 3000 Series Concentrator Getting Started*
- Online Help

## Related Documentation

- *VPN Client User Guide for Windows*
- *VPN Client Administrator Guide*
- *VPN 3002 Hardware Client Getting Started*
- *VPN 3002 Hardware Client Reference*
- *VPN 3002 Hardware Client Quick Start Card*

# Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in "Service and Support" in *Cisco Information Packet* shipped with your product.

**Note** If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems' primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

## Software Configuration Tips on the Cisco TAC Home Page

The Cisco TAC home page includes technical tips and configuration information for the VPN 3000 Concentrator and client. Find this information at:

http://www.cisco.com/warp/public/707/#vpn3000.

# Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

## Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

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

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

We appreciate your comments.

# Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

## Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.

- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

### Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

### Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

## 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

- 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

- 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

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.