Release Notes for Cisco SSL VPN Client, Release 1.0.2

CCO Date: July 26, 2005

Part Number: OL-7819-02

Introduction

These release notes are for the Cisco SSL VPN Client (SVC), Release 1.0.2, running on the Cisco VPN 3000 Concentrator. The Cisco SVC provides end users running Microsoft Windows XP or Windows 2000 with the benefits of a Cisco IPSec VPN client without the administrative overhead required to install and configure an IPSec client. It supports applications and functions unavailable to a standard WebVPN connection.

These release notes describe new features, changes to existing features, limitations and restrictions, open and resolved caveats, and related documentation. They also include procedures you should follow before loading this release. The section Usage Notes describes interoperability considerations and other issues you should be aware of when installing and using the Cisco SVC. Read these release notes carefully prior to installing this software.

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

Contents

This document includes the following sections:

System Requirements, page 2
Upgrading to Release 1.0.2, page 3
New Features in Release 1.0.2, page 3
New Features in Release 1.0.1, page 4
Installation Notes, page 4
Usage Notes, page 8
Caveats, page 12
Documentation Updates, page 16
Service, Support, and Tips, page 16
Obtaining Documentation, page 16
Obtaining Technical Assistance, page 18
Obtaining Additional Publications and Information, page 19

System Requirements

The following sections describe the system requirements for Cisco SVC Release 1.0.2.

Hardware Supported

Cisco SVC, Release 1.0.2, is supported on the following hardware platforms:

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

Security Appliances and Software Supported

Table 1 shows the supported security appliances and the software that is required in order to use this SVC release.

Table 1 Platform Software Supported

Platform	Required Software
Cisco VPN 3000 Series Concentrators	version 4.7.2 or later
Altiga Networks VPN Concentrators	version 4.7.2 or later

Upgrading to Release 1.0.2

This section contains information about upgrading from earlier releases to Cisco SVC, Release 1.0.2.

Before You Begin

Be aware of the following considerations before you upgrade. These are known product behaviors, and knowing about them at the beginning of the process should expedite the upgrade. Where appropriate, the number of the caveat documenting the issue appears at the end of the item. See the "Caveats" section on page 12 for a description of using this number to locate a particular caveat.

Note To use the SVC, Release 1.0.2, you *must* upgrade the VPN Concentrator to Release 4.7.2 or higher. The SVC, Release 1.0.2, does *not* operate with the VPN Concentrator running versions earlier than version 4.7.2

New Features in Release 1.0.2

This section describes the new features in SVC Release 1.0.2. For detailed instructions about how to configure and use these features, see the documentation associated with the security appliance on which you are installing the SVC software.

SSL VPN Client Keepalive Frequency

The Keepalive Frequency (CSCsa97704) ensures that an SVC connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle.

This feature also ensures that the SVC does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

The Keepalive Frequency defaults to zero (disabled), and can be configured from 5 and 300 seconds.

You can view and configure the Keepalive Frequency from:

Configuration | User Management | Groups

Select a group from the Current Group list, and select Modify. The Manager opens the Configuration | User Management | Groups | Modify (group) screen.

Click the WebVPN tab to view and configure all WebVPN parameters, including the Cisco SSL VPN Client Keepalive Frequency.

New Features in Release 1.0.1

This section describes the new features in SVC Release 1.0.1. For detailed instructions about how to configure and use these features, see the documentation associated with the security appliance on which you are installing the SVC software.

NTLM Proxy Authentication

Windows NT LAN Manager (NTLM) Proxy Authentication is the authentication protocol used on networks that include systems running versions of the Microsoft® Windows NT® operating system earlier than Windows 2000, and on stand-alone systems. NTLM Proxy Authentication is a more advanced challenge/response-based protocol from its predecessor, LAN Manager (LM).

Note The SVC must support NTLM Proxy authentication in the case where there is a proxy server between the SVC (running on a PC) and the VPN 3000 Concentrator, and the proxy server is expecting NTLM Proxy Authentication instead of basic authentication. Therefore, in order for the SVC to operate properly in this scenario, you must be running SVC Release 1.0.1 or later.

Installation Notes

This section describes installation-specific issues and procedures for SVC Release 1.0.2, and contains the following sections:

- Installing SVC Software on a VPN 3000 Concentrator
- Enabling Automatic Installation of SVCs for Non-Privileged Users
- VPN 3000 Concentrator and Automatic Installation of SVCs
- Adding a Security Certificate in Response to Browser Alert Windows

Installing SVC Software on a VPN 3000 Concentrator

To install the SVC software on a VPN Concentrator, follow these steps:

Step 1 Download the sslclient-win*.pkg file to any location on your PC.

Step 2 Install a VPN Concentrator Release 4.7.2 image on your VPN Concentrator.

Step 3 Navigate to the Configuration | Tunneling and Security | WebVPN | SSL VPN Client screen in the VPN Concentrator Manager.

Step 4 Click **Install a new SVC.**

Step 5 Click **Browse** and highlight the sslclient-win*.pkg file.

Step 6 Click **Apply**.

Step 7 Save the configuration.

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

Enabling Automatic Installation of SVCs for Non-Privileged Users

Users must have Administrator privileges on client PCs that use SVC. Clients connecting without Administrator privileges cannot receive and install an SVC. However, Cisco provides an Install Enabler utility to pre-load a client service that lets non-privileged users load SVC. This utility (STCIE.EXE) is useful if you do not typically configure client PC users with Administrator privileges. It is available within the sslclient-win-1.0.2.127.zip file on your distribution media or on the VPN 3000 Concentrator download area on Cisco.com.

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

To set up the client service, unzip the sslclient-win-1.0.2.225.zip file and the start the STCIE.EXE executable file. It creates or updates the SVC in the Program Files\Cisco System folder, which the VPN 3000 concentrator pushes to the client.

The following command line switches are available:

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

VPN 3000 Concentrator and Automatic Installation of SVCs

The following recommendations and caveats apply to the automatic installation of SVC software on client PCs:

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

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

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

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

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

1. Go to Tools | Internet Options | Trusted Sites.

   The Internet Options window opens.
2. Click the Security tab.
3. Click the Trusted Sites icon.
4. Click the Sites button.

   The Trusted Sites window opens.
5. Type the host name or IP address of the VPN Concentrator. Use a wildcard such as https://*.yourcompany.com to allow all VPN Concentrators within the yourcompany.com domain to be used to support multiple sites.
6. Click the Add button.
7. Click the OK button.

   The Trusted Sites window closes.
8. Click the OK button in the Internet Options window.

Adding a Security Certificate in Response to Browser Alert Windows

This section explains how to install a self-signed certificate as a trusted root certificate on a client in response to the browser alert windows.

In Response to a Microsoft Internet Explorer "Security Alert" Window

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

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

Install the certificate as a trusted root certificate as follows:

1. Click the View Certificate button in the Security Alert window.

   The Certificate window opens.
2. Click the Install Certificate button.

   The Certificate Import Wizard Welcome opens.

3. Click the Next button.

   The Certificate Import Wizard – Certificate Store window opens.

4. Select the “Automatically select the certificate store based on the type of certificate” option.
5. Click the Next button.

   The Certificate Import Wizard – Completing window opens.

6. Click the Finish button.

   Another Security Warning window prompts “Do you want to install this certificate?”

7. Click the Yes button.

   The Certificate Import Wizard window indicates the import is successful.

8. Click OK to close this window.
9. Click OK to close the Certificate window.
10. Click the Yes button to close the Security Alert window.

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

In Response to a Netscape, Mozilla, or Firefox “Certified by an Unknown Authority” Window

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

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

Install the certificate as a trusted root certificate as follows:

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

   The Certificate Viewer window opens.

2. Click the “Accept this certificate permanently” option.
3. Click OK.

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

Usage Notes

This section lists the following interoperability considerations and other issues to consider before installing and using SVC Release 1.0.2:

- NTLM Authentication
- WINS and DNS
- Internet Explorer Proxy With SVC
- Setting the Secure Connection (Key) Icon
- Cisco Secure Desktop and the SVC
- Cisco Security Agent Version Requirements
- PC Wireless Client Configurations
- Hosts File Recovery
- Certificate Revocation List Processing
- Zyxel Modem SSH Incompatibility

NTLM Authentication

If there is a proxy server between the SVC (running on a PC) and the VPN 3000 Concentrator, and the proxy server is expecting NTLM authentication instead of basic authentication, the SVC must support NTLM Authentication. Therefore, you must use SVC Release 1.0.2 or later.

WINS and DNS

The SVC supports group configured primary and secondary Windows Internet Naming Services (WINS) or Domain Naming Services (DNS). In general, the IPSec Group-based parameters apply to the SVC. The exception is the Authentication, Authorization, and Accounting configuration, which is always global. The following table summarizes the group and global settings that the SVC supports.

Parameter	Group	Global/System-wide
Authentication	No	Yes[1]
Authorization	No	Yes
Accounting	Yes	Yes[2]
DNS and WINS	Yes	N/A
MSIE Proxy Server Setting	Yes	N/A
Default Domain	Yes	N/A
Split DNS	Yes	N/A
Split Tunneling	Yes	N/A
Local LAN	Yes	N/A

1. In this release WebVPN does not support RADIUS with Expiry authentication.
2. If no accounting servers are defined in the group, the system servers apply.

Internet Explorer Proxy With SVC

If you have Internet Explorer configured with a proxy, you must activate the "Use HTTP 1.1 through proxy connections" setting to use the SVC. If this option is not set, the SSL VPN connection does not come up.

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

Setting the Secure Connection (Key) Icon

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

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

Cisco Secure Desktop and the SVC

To ensure proper operation of the SVC, follow the instructions of the DSL or cable router manufacturer to upgrade to the latest available firmware revision.

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

Cisco Security Agent Version Requirements

Cisco Security Agent (CSA) Version 4.5 and higher is the only version compatible with the SVC. The appropriate CSA policy ships with CSA and is attached to the group "Remote desktops and laptops." These policies are not enabled by default; you must select them to prevent the SVC from failing with CSA version 4.5.

PC Wireless Client Configurations

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

Hosts File Recovery

If Application Access fails to terminate correctly when using the SVC, the hosts file may not be recovered to its previous condition. This can result from any of the following actions:

- Terminating the browser using the Task Manager
- Terminating Java processes using the Task Manager
- Shutting down the PC without closing the browser
- Logging out without closing the browser

Manually restore the hosts file to its original condition by copying the contents of *webvpn.hosts* to the hosts file. This restores network connectivity. The *webvpn.hosts* file is in the C:\WINNT (or C:\WINDOWS) \system32\drivers\etc directory.

Certificate Revocation List Processing

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

- `CRL server is offline`

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

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

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

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

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

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

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

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

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

- Click on the Restore Defaults button near the bottom of the window.

  This option restores all of the options under the Advanced tab to the original settings. To avoid doing so, use the second option.

- Insert a check mark next to “Check for server certificate revocation (requires restart),” click Apply, click OK, and restart Windows.

Zyxel Modem SSH Incompatibility

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

Caveats

Caveats describe unexpected behavior or defects in Cisco software releases. The open caveats in Release 1.0.2 appear first in this list. The second section lists caveats that have been resolved in Release 1.0.2, followed by sections describing caveats in previous releases. Each list is sorted by identifier number. Both lists include any workarounds that are available.

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.

Open Caveats in the Cisco SSL VPN Client Release 1.0.2

Cisco SSL VPN Client (SVC) Release 1.0.2 has the following known caveats:

- CSCeh37813

  The SVC connection fails when connecting to the secure gateway via a proxy server and the Microsoft Internet Explorer proxy settings are configured for autoconfiguration.

  Workaround: Use the static configuration of the proxy settings option.

- CSCei67188

  If a proxy server requires authentication, and that proxy server supports only Basic authentication, the SVC fails, displaying error messages indicating that no proxy authentication scheme is supported.

  Workaround:

  Configure the proxy server to support more than just Basic authentication.

- CSCsa99041

  The SVC may not authenticate with a transparent (implicit) proxy server.

  When a proxy server is configured to use authentication (Basic, NTLM, etc.) and is also configured in a manner that it is transparent to the client, the authentication may fail. A transparent proxy server is one that the client has no knowledge of. This deployment is usually done by redirecting traffic to a proxy server via a router.

  For example, the following configuration of a NetCache server would not work with the SSL VPN Client: http://www.netapp.com/tech_library/3336.html#4.2

  In this configuration, the proxy server uses a non-standards-based implementation to appear like a web site instead of a proxy server with respect to authentication. The proxy server responds with a 401/WWW-Authenticate instead of the usual 407/Proxy-Authenticate that would occur in explicit proxy configurations.

  Workaround: Do not use non-standard authentication mechanisms when deploying a proxy server (e.g. don't deploy a transparent proxy server and then require authentication via that proxy server).

Resolved Caveats in the Cisco SSL VPN Client Release 1.0.2

The following caveats were resolved in Cisco SSL VPN Client (SVC) Release 1.0.2:

- CSCeh88091

  If the client configuration of the Cisco VPN 3000 Concentrator contains more than 26 split tunneling entries, the SVC fails to connect and displays the following message:

  ```
  The SSL VPN HTTP response received from the gateway is invalid, contact your
  administrator.
  ```

- CSCei33496

  If you establish an SVC connection with a remote computer running Windows XP using the DHCP Alternate Configuration, the SVC fails to connect and fails to update the routing table.

- CSCei33502

  After a minor install error occured, the Installer Enabler utility continued to install sucessfully. However, users without administrator privileges failed to establish SVC connections.

- CSCei34401

  Signing Certificate Renewal—The code signing on the client build machine requires updating.

- CSCsa97704

  A configurable 'heartbeat' is needed to keep proxy connection open.

  For a description of this new feature, see "SSL VPN Client Keepalive Frequency" in the "New Features in Release 1.0.2" section.

- CSCsb19268

  A remote computer, with an SVC connection to a secure gateway, and multiple network interface controllers connected to other networks, is unable to access the other networks even though they are configured in the list of networks allowed to bypass the tunnel.

- CSCsb36296

  The SVC component Agent.exe causes remote computers running Windows XP (Service Pack 2) to experience long delays in logging off and shutting down.

Resolved Caveats in the Cisco SSL VPN Client Release 1.0.1

The following caveats were resolved in Cisco SSL VPN Client (SVC) Release 1.0.2:

- CSCeh32010

  Need to handle URL type of proxy server configuration in Windows because the tunnel client software does not interpret URL formats like the following:

  The SVC software does not support a URL-type proxy server configuration. Therefore, the SVC does not interpret URL formats like the following:

  - http://proxy1.cisco.com
  - https://proxy2.cisco.com/index.html:88
  - ftp://10.1.1.1:8080

- CSCeh36363

  The Microsoft Internet Explorer browser does not display the restored client proxy configuration.

- CSCeh40800

  When a proxy server and one or more exception addresses that contain some wildcard characters are configured on the client PC, the SVC sometimes bypasses the proxy server to connect directly to the gateway. If the direct connection fails, the client connects via the proxy server.

- CSCeh42709

  On some PCs running Windows XP, SP1 or SP2, the SVC fails to obtain the proxy configuration from Windows. The client attempts to connect directly to the VPN gateway and fails to setup the connection.

- CSCeh50731

  The VPN client may not send an address renewal request to the VPN gateway before the lease duration has expired. The gateway may close the connection if the same address is no longer available.

- CSCeh52036

  The SVC fails to connect when the SVC configuration, pushed down by the VPN concentrator, contains split tunneling route definitions that conflict with existing routes defined on the client PC. Other conditions may also cause this problem. When this problem occurs, the following message appears:

  ```
  The SSL VPN Client was unable to modify the IP forwarding table. An SSL VPN
  connection will not be established.
  ```

- CSCeh52212

  If the user modifies the SVC Virtual Network Adapter IP address via the Network Connections settings in the control panel, the VPN connection will most likely no longer function, even after the VPN connection has been re-established.

- CSCeh52222

  Under-privileged users are able to un-install the Install Enabler.

- CSCeh52948

  After an SVC has been disconnected, some ending characters in the client proxy configuration may be missing. This may occur if the original proxy configuration is longer than 128 characters, and has been saved, modified and restored by the SVC.

- CSCeh66776

  The SVC fails when NTLM authentication is enabled on ISA proxy server in the following configuration:

  [Client] ---> [ISA] ---> [VPN3K] ---> [Web Server]

- CSCeh68269

  The client computer may bluescreen or freeze during an SVC session when the SVC is experiencing heavy network traffic with multiple applications (e.g. multiple ftp sessions). This problem is more likely to occur on multi-cpu or hyper-threading PCs.

- CSCsa70251

  The Cisco VPN 3000 Concentrator reports the following message, even though it actually registers the session as active:

  ```
  login failed, Cisco SSL VPN Client required
  ```

- CSCsb01423

  When a client PC establishes an SVC connection to a Cisco VPN 3000 Concentrator through a NetCache Proxy Server, intermittent disconnects occur.

- CSCsb02263

  When a proxy server is configured on the client PC, and that proxy server follows the specification for persistent connections as described in RFC2616, the proxy server may disconnect the client PC from a persistent connection.

- CSCsb08657

  The SVC connection does not pass data through a proxy server when it is 1 or more hops away from the proxy server.

Documentation Updates

The Cisco VPN 3000 Series Concentrator documentation set has not been revised for this release. It is available online through Cisco Connection Online (CCO) and www.cisco.com.

Service, Support, and Tips

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.

The Cisco Technical Support home page includes technical tips and configuration information for the VPN 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 Support website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco Technical Support website. Cisco.com registered users have complete access to the technical support resources on the Cisco Technical Support website, including 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

Cisco Technical Support

Cisco Technical Support is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco Technical Support website and the Cisco Technical Support 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 Technical Support 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 Technical Support Website

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

http://www.cisco.com/techsupport

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco Technical Support website. Some services on the Cisco Technical Support 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 Technical Support website, you can open a case online at this URL:

http://www.cisco.com/techsupport and select "Open a case (service request)" and follow the instructions from there.

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.