Release Notes for CiscoView Device Manager for the Cisco SSL Services Module 1.1

These release notes are for use with the CiscoView Device Manager for the Cisco Catalyst 6500 Series SSL Services Module (CVDM-SSLSM) running on Windows and Solaris platforms.

These release notes provide:

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

Description

CiscoView Device Manager for the Cisco Catalyst 6500 Series SSL Services Module (CVDM-SSLSM) enables users to configure Secure Socket Layer (SSL) services on their SSL Services Module. CVDM-SSLSM has a small footprint and can be downloaded and installed on the module Flash memory.

CVDM-SSLSM supports several features in SSL Services Module Software Release 2.1(1), such as:

- Initial setup wizards:
  - Configuring certificate Trustpoints
  - Importing certificates from external PKI system
  - Exporting certificates from SSL Services Module
- Certificate Management:
  - Visual indication of certificates expiry
  - Grouping of certificates by CA, enrollment status, and certificate expiry date
- CA pools, certificate access control lists
- Policies
- Proxy services
- VLANs
- Statistics

CVDM-SSLSM enables you to create configurations by responding to a series of questions in wizards, and CiscoView Device Manager designs the command-line interface (CLI) configuration based on those responses. At the end of the process, you view the CLI command syntax created and decide whether to deploy the configurations to the chassis immediately or to save them for future editing.

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Available Formats
ReadMe Document for CiscoView Device Manager for the Cisco Catalyst 6500 Series SSL Services Module (CVDM-SSLSM)	This document is available if you download CVDM-SSLSM from the software download site. You can reach the CVDM-SSLSM download site by clicking the Download Software link from this URL: http://www.cisco.com/go/cvdm **Note** It is important that you read this document before downloading and installing CVDM-SSLSM from the software download site.
User Guide for CiscoView Device Manager for the Cisco Catalyst 6500 Series SSL Services Module (CVDM-SSLSM)	This document is available on Cisco.com at this URL: http://www.cisco.com/go/cvdm
Context-sensitive online help	Click the Help button from any dialog box within the application.

Related Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 2 describes the additional documentation that is available.

Table 2 Related Documentation

Document Title	Description and Available Formats
Readme Document for CVDM-C6500	This document is available if you download CVDM-C6500 from the software download site. You can reach the CVDM-C6500 download site by clicking the Software Center link from this URL: http://www.cisco.com/go/cvdm **Note** It is important that you read this document before downloading and installing CVDM-C6500 from the software download site.
Release Notes for CiscoView Device Manager for the Cisco Catalyst 6500	This document is available on Cisco.com at this URL: http://www.cisco.com/go/cvdm
User Guide for CiscoView Device Manager for the Cisco Catalyst 6500	This document is available on Cisco.com at this URL: http://www.cisco.com/go/cvdm
Readme Document for CVDM-CSM	This document is available if you download CVDM-CSM from the software download site. You can reach the CVDM-CSM download site by clicking the Software Center link from this URL: http://www.cisco.com/go/cvdm **Note** It is important that you read this document before downloading and installing CVDM-CSM from the software download site.
Release Notes for CiscoView Device Manager for the Cisco Content Switching Module	This document is available on Cisco.com at this URL: http://www.cisco.com/go/cvdm

Table 2 Related Documentation (continued)

Document Title	Description and Available Formats
User Guide for CiscoView Device Manager for the Cisco Content Switching Module	This document is available on Cisco.com at this URL: http://www.cisco.com/go/cvdm
Readme Document for CiscoView Device Manager for the Cisco IPSec VPN Acceleration Services Module (CVDM-VPNSM)	This document is available if you download CVDM-VPNSM from the software download site. You can reach the CVDM-VPNSM download site by clicking the Download Software link from this URL: http://www.cisco.com/go/cvdm **Note** It is important that you read this document before downloading and installing CVDM-VPNSM from the software download site.
Release Notes for CiscoView Device Manager for the Cisco IPSec VPN Acceleration Services Module (CVDM-VPNSM)	This document is available on Cisco.com at this URL: http://www.cisco.com/go/cvdm
User Guide for CiscoView Device Manager for the Cisco IPSec VPN Acceleration Services Module (CVDM-VPNSM)	This document is available on Cisco.com at this URL: http://www.cisco.com/go/cvdm

Downloading the Application

You can download CVDM-SSLSM, any published patches, and their readme files from the Download Software site. You can reach the CVDM-SSLSM download site by clicking the Download Software link from this URL: http://www.cisco.com/go/cvdm

Refer to *Readme Document for CiscoView Device Manager for the Cisco Catalyst 6500 Series SSL Services Module (CVDM-SSLSM)* for the following information:

- Hardware and software requirements
- Information on coexistence with other CiscoView Device Managers
- Installation/uninstallation instructions
- Launch instructions

Known and Resolved Problems

Installation and launching problems with CVDM-SSLSM can occur because of known problems with:

- Lack of available VTY lines
- Netscape installation support for Java plug-in
- Lack of SSH or Telnet access
- Lack of flash: space
- Previously installed versions of CVDM

To avoid problems, please do the following:

- Ensure that at least two VTY lines are available. CVDM-SSLSM will not launch if all Telnet lines are being used. Instead, you will see a “Page cannot be displayed” error.
- Manually download the Java plug-in if you do not have Java Plug-in 1.4.2_06, or use Internet Explorer to download the Java plug-in automatically. Sometimes Netscape does not prompt you to download the Java plug-in.
- If there is not enough space in flash:, back up your files on the flash memory card by copying them to an external server, delete them from the flash memory card and issue the **squeeze flash:** command.

- If you have the previous version of CVDM-SSLSM installed on the flash:, you should delete the CVDM files, then install CVDM-SSLSM 1.1; see *Readme Document for CiscoView Device Manager for the Cisco Catalyst 6500 Series SSL Services Module (CVDM-SSLSM)* for uninstallation instructions.

Table 3 describes problems known to exist in this release. Table 4 describes problems resolved in this release.

Note To obtain more information about known problems, access the Cisco Software Bug Toolkit at http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl. (You will be prompted to log into Cisco.com.)

Table 3 Known Problems in CVDM-SSLSM 1.1

Bug ID	Summary	Explanation
CSCee13487	CVDM-SSLSM does not allow you to create names that contain a space.	Unlike CLI, CVDM-SSLSM does not support the creation of names that contain white space characters for Trustpoints, key pairs, proxy services, policies, certificate ACLs, and CA pools. To work around this problem, do not use spaces in the names for these items.
CSCee16213	Certificate Trustpoint wizard does not determine TFTP transfer status of certificate request.	When a certificate Trustpoint is enrolled using TFTP enrollment method, the Certificate Trustpoint wizard does not determine whether the TFTP transfer of the certificate request has succeeded or failed. The wizard displays *Request sent to Server* as the status even if the TFTP transfer was unsuccessful. To work around this problem, verify the TFTP server and confirm that the certificate request was successfully transferred from the SSL module.

Table 3 Known Problems in CVDM-SSLSM 1.1 (continued)

Bug ID	Summary	Explanation
CSCee31054	Proxy service configuration fails if any CLI session is in ssl-proxy configuration submode.	Proxy service configuration fails if any CLI (Telnet or SSH) session is in ssl-proxy configuration submode. This applies to policy, NAT pool, CA pool and VLAN configurations (all the configurations that use the ssl-proxy command). To work around this problem, ensure that there are no CLI sessions in ssl-proxy configuration submode when using CVDM-SSLSM.
CSCee48552	Some fields look compressed in Solaris 2.8.	When using Netscape on a Solaris system, some of the dialogs may appear squeezed if the font is set to a small size. To work around this problem, go to Tools > Desktop Controls > Font Style Manager. Increase the Font size and restart the Workspace Manager. A medium-sized font should work in most cases.
CSCee57848	Sometimes, a new browser window is not displayed in the foreground when you use Netscape on Windows.	From a CVDM page, after you click a button or link that opens a new browser window, the window does not appear in the foreground. To work around this problem, bring the new browser window to the foreground by clicking the window's title bar. **Note** Netscape browser brings a new window to the foreground of all windows belonging to the browser process only, not to the foreground of the entire desktop. CVDM belongs to a separate process and remains in the foreground.
CSCee58122	On exiting the CVDM-SSLSM, the splash screen and Java console are not closed.	When using Netscape 7.1, if you select **File > Exit** from the menu bar, the splash screen and Java console are not closed. To work around this problem, close the splash screen and Java console manually.

Table 3 Known Problems in CVDM-SSLSM 1.1 (continued)

Bug ID	Summary	Explanation
CSCsa15820	Sometimes, when using Internet Explorer on a Windows system, CVDM-SSLSM cannot be launched after installing the Java plug-in.	To work around this problem, remove the proxy setting in the browser.
CSCsa15984	CVDM-SSLSM is not launched if a nondefault password prompt is configured on a device.	CVDM-SSLSM works on devices that have default prompts. If you change the default password prompt for a device using CLI commands, then CVDM-SSLSM cannot be launched.
CSCsa45867	Unable to launch the CVDM-SSLSM if SSH is not enabled on SSLSM.	CVDM-SSLSM does not launch for either of the following conditions: • SSH is not enabled on the SSLSM. Or • A non-existing key pair is assigned for SSH ("ip ssh rsa keypair-name <*ssh_key*>") To work around this problem try one of the following: • Generate the key pair assigned for SSH using CLI • Assign an existing key pair for SSH using CLI. • Remove the SSH key configuration ("no ip ssh rsa keypair-name").

Table 3 Known Problems in CVDM-SSLSM 1.1 (continued)

Bug ID	Summary	Explanation
CSCsa50843	CVDM-SSLSM does not launch on a Windows 2000 machine with multiple versions of the Java Plug-in installed.	The problem occurs on machine with the following configuration: • Operating system—Windows 2000 Professional with Service Pack 4 • Java Plug-in versions installed—1.4.2_04 and 1.4.2_06 • Active browser—Netscape 7.0 or Internet Explorer 6.0 with SP1 Workaround: Uninstall Java Plug-in 1.4.2_04.
CSCsa50848	Cannot launch CVDM-SSLSM in Internet Explorer running on a Windows 2000 machine when Java Plug-ins 1.4.2_06 and 1.5 are installed.	Problem occurs on machine with the following configuration: • Operating System—Windows 2000 Professional with SP4 • Java Plug-in versions installed—1.4.2_04, 1.4.2_06, and 1.5 • Active Browser—Internet Explorer 6.0 with SP1 Workaround: To launch CVDM-SSLSM with Internet Explorer, you must first uninstall Java Plug-in 1.5.

Table 3 Known Problems in CVDM-SSLSM 1.1 (continued)

Bug ID	Summary	Explanation
CSCsa54308	When CVDM-SSLSM is launched with unsupported plug-in, it does not point to the correct download location of the supported Java plug-in (1.4.2_06).	When CVDM-SSLSM is launched with unsupported plug-in: • Netscape 7.1 (Windows 2000), does not point to the download location of the Java plug-in 1.4.2_06. The splash screen appears, but no error message is displayed. • Firefox 1.0 (Windows 2000), begins installing Java plug-in 1.5. • Netscape 7.0 (Solaris 2.8 and 2.9), does not point to the download location of the Java plug-in 1.4.2_06. Workaround: Install Java plug-in 1.4.2_06 manually.

Table 3 ***Known Problems in CVDM-SSLSM 1.1 (continued)***

Bug ID	Summary	Explanation
CSCsa55533	Certificate Export wizard does not close the connection to a redundant SSLSM.	When exporting certificates to a redundant SSLSM with a single VTY available for connection, the Certificate Export wizard does not close the connection after completing the certificate installation. To work around this problem: Clear the VTY used by the Certificate Export wizard on the redundant SSLSM using CLI.
CSCsa64995	Launching CVDM-SSLSM using HTTPS reloads the module if any certificate is not available in the module.	If the SSL module does not have any certificates installed, launching CVDM-SSLSM using HTTPS reloads the module. To work around this problem, try one of the following: • Make sure that at least one certificate for HTTPS access is present on the module. By default, a test PKCS12 file (test/testssl.p12) is embedded in the SSL software on the module. You can install the certificate from CLI, following the steps mentioned in the SSLSM configuration. • Use HTTP to launch CVDM-SSLSM.

Table 4 ***Problems Resolved in CVDM-SSLSM 1.1***

Bug ID	Summary	Explanation
CSCsa11679	On Windows, Netscape 7.1 does not prompt you to install the supported Java plug-in version again if you cancelled the installation the first time.	To work around this problem, go to http://java.sun.com/products/archive/j2se/1.4.1_05/index.html and download and install the JRE from J2SE v1.4.1_05.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

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 Ordering tool:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.

- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. 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/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

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