Release Notes for Cisco Enhanced Device Interface 2.0.1

September 23, 2007

These release notes support the release of Cisco Enhanced Device Interface 2.0.1.

Contents

This document includes the following topics:

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

Introduction

Cisco E-DI provides a comprehensive management interface for configuration of Cisco devices.

Cisco E-DI offers interfaces for two categories of users - the human user interacting with network devices through the command line interface (CLI), and management applications interacting with network devices through an XML programmatic interface (see *Cisco Enhanced Device Interface Programmer's Guide, 2.0.1*).

Cisco E-DI 2.0.1 is a maintenance release that includes enhanced security features. It includes device authentication which allows the administrator to choose between a centralized credential model (non session based device authentication) and a per user-session credential model (session based device authentication).

Cisco E-DI 2.0.1 supports reception and processing of syslog messages from a syslog relay.

Cisco E-DI 2.0.1 supports SSHv2 in addition to SSHv1 which is present in Release 2.0.

Cisco E-DI 2.0.1 can automatically identify the management interface address of an NE where it has multiple IP addresses scenarios. Only one of NE's IP addresses is used for management.

Cisco E-DI 2.0.1 supports NETCONF protocol draft07. Cisco E-DI 2.0.1 also supports Licensing capability.

Cisco E-DI 2.0.1 includes an FTP server, and provides additional commands to create and extract tar files.

Installation

Refer to the *Cisco E-DI Quick Start Guide 2.0.1* for details to install, configure and start using Cisco E-DI.

Incremental Device Updates

IDUs allow Cisco E-DI to be updated with support for new device packages.

The device packages listed in Table 3 are included in this build.

To add device packages from CCO, the Cisco E-DI administrator can login to CCO, specify the Cisco E-DI version, and download the files for the device packages. See http://www.cisco.com/kobayashi/sw-center/sw-netmgmt.shtml. Once the required device package files are downloaded, they can be copied to Cisco E-DI, and installed using the maintenance shell. Refer to *Cisco E-DI Quick Start Guide 2.0.1* for details of the installation process.

Important Notes

Forbidden Commands

Administrator can restrict certain native device commands that can be executed on the device using the **exec-cmd** command. These commands can be added to /user/admin/forbiddenCommands file. Each command must be entered on a separate line. Users will not be allowed to execute any command that matches or starts with the commands entered in the file. Use **edit** command to edit this file. Only the Administrator is allowed to edit. The default content of forbiddenCommands file is as follows: **er** <cr> **erase** <cr> **wr** <cr> **write** <cr> **re** <cr> **reload**.

Known Caveats With This Release

Open Caveats

Table 1 Open Caveats

Identifier	Title	Impact	Workaround
CSCeh27856	Recreating the config archive label after deleting a label with the same name would not succeed.	Cannot reuse label name after deleting it.	Use a different label each time.
CSCeh59930	The editor process (opened using the edit command) or the perl process are not closed when the user session times out.	This might affect the performance of Cisco E-DI if too many sessions are opened.	None.
CSCeh67305	Startup config is retrieved even though it has been erased on device. The configuration is retrieved from the archives on Cisco E-DI.	None.	None.
CSCeh77656	In group config mode, interface selection behavior is inconsistent.	Interface selection is not allowed in group config mode, except in the interface configuration.	Do the same operation on individual devices.
CSCeh94947	The device status shows offline when SNMP connectivity fails but Telnet connectivity exists.	Device status is misleading.	Check SNMP credentials on Cisco E-DI configuration and on the NE.
CSCin88776	Unable to close editor in Telnet and SSH.	The editor cannot be closed in Telnet or SSH sessions when opened through certain clients like MS-DOS.	Use applications such as Putty.
CSCin93495	Cisco E-DI does not support concurrent connections beyond 64.	A user cannot open more than 64 concurrent sessions to Cisco E-DI.	None.
CSCjh00074	File System operations (manipulating files and or directories) performed using Perl scripts bypass the authorization checks on Cisco E-DI.	A Cisco E-DI perl script user with less privileges can perform operations that the user is not authorized to.	Limit the usage of perl scripts for manipulating the Cisco E-DI file system.

Table 1 Open Caveats (continued)

Identifier	Title	Impact	Workaround
CSCjh00139	In connect exec mode the write commands do not ask for confirmation.	It is possible to inadvertently perform destructive operations through connect exec mode.	Exercise caution when using the connect exec mode.
CSCsb54924	If the terminal setting is not appropriately set for different client types e.g. putty, xterm, the display of the cursor position on the screen is occasionally random.	It can cause confusion when the user is typing CLI commands or erasing part of the command.	The terminal settings should be appropriately configured depending on the terminal type using the **terminal cursor-wrap**, and **terminal width** commands.
CSCsb66082	Occasionally, the device configuration's status is displayed as dirty (i.e. configuration copy is not up-to-date) even after a successful synchronization.	It gives the incorrect status of the configuration state to the user.	None
CSCsb67138	When the mgmt IP address is different from the source IP address in a trap, the trap is not processed.	Some traps may not be shown in the Cisco E-DI trap list.	Change the source IP address to the mgmt IP address
CSCsb72283	While importing a device that has the management IP Address different from discovered IP address, the user must choose an option of Y/N/Q.	Not choosing an option explicitly could hang the session.	Choose a valid option.

Resolved Caveats

Table 2 lists the caveats that were resolved between Cisco Enhanced Device Interface 2.0 and Cisco Enhanced Device Interface 2.0.1.

Table 2 Resolved Caveats

Identifier	Title
CSCeh73442	The utility command **snmp oidlookup** fails with an **internal error** message.
CSCei09354	A user with netoperator privileges cannot view locks acquired.
CSCei10176	**http-raw-request** command is handled incorrectly on XML PI.
CSCei17032	Download of files from ftp-server works only for anonymous users.
CSCin93297	The derived credential set will inherit the credentials from a parent set when it is re-created after deletion.

Known Limitations with IDUs

Cisco IOS Devices

The following are known limitations with the Incremental Device Updates (IDUs) for the Cisco IOS devices listed in Table 3:

1. Implicit support provides a super-set/sub-set CLI of what is supported on a particular device type.
2. The following commands are not supported in network config mode:
   a. do
   b. define
   c. interface range
   d. default
   e. help
3. Only the following commands are supported in network exec mode:
   a. clear
   b. clock
   c. erase
   d. show
   e. write
4. Complete syntax checking for some commands in the following scenarios may be not be available:
   a. access-list (syntax checks available to depth 7)
   b. redistribute (syntax checks available to depth 5)—The user will see a customized node WORD with description Command Parameters. This node will accept any syntax, and will recurse to an infinite depth.
5. Some commands may not have a <cr>. This can occur for deprecated commands or any Cisco IOS commands that need special handling.
6. Hidden commands supported by Cisco IOS will not be supported through Cisco E-DI.

CatOS Devices

The following are known limitations with the Incremental Device Updates (IDUs) for the Cisco CatOS devices listed in Table 3:

1. Implicit support provides a super-set/sub-set CLI of what is supported on a particular device type.
2. Only the following commands are supported in network config mode:
   a. set
   b. clear
   c. commit

3. Only the following commands are supported in network exec mode:
   a. show
   b. history
   c. disconnect
   d. reconfirm
   e. reset
   f. slip
   g. switch
   h. rollback
4. Complete syntax checking for some commands in the following scenarios may not be available:
   a. set vlan <vlan> name
   b. set security acl—The user will see a customized node WORD with description Command Parameters. This node will accept any syntax and will recurse to an infinite depth.
5. Some commands may not have a <cr>. This can occur for deprecated commands or any CatOS commands that need special handling.
6. Hidden commands supported by CatOS will not be supported through Cisco E-DI.
7. Interactive commands that require user input after a carriage-return is typed will not be not supported. For example:
   – issc-6509-2> (enable) set password
   – issc-6509-2> (enable) set enablepass

Devices Supported by Cisco E-DI

The device packages listed in Table 3 are included in this build.

Note When additional device packages are supported, they will be made available through CCO.

Table 3 IDUs Available on Cisco E-DI Product CD-ROM and CCO

IDU	OS Version	IDU Version
Cat 2950	Cisco 12.1(13)EA1c	1.1
Cat 3550	Cisco 12.1(14)EA1a, 12.1(22)EA2	1.2
Cat 3750	Cisco 12.1(19)EA1a	1.1
Cat 4000	Cisco 12.1(19)EW1	1.1
Cat 6500	Cisco 12.1(11b)E1, 12.2(17d)SXB6	1.2
Cat 6500 CatOS	Cisco 7.6(6)	1.1
Cisco 12000	Cisco 12.0(27)S5	1.1
Cisco 1700	Cisco 12.2(15)T14, 12.3(8)T6	1.3
Cisco 1800	Cisco 12.3(11)T5	1.1

Table 3 IDUs Available on Cisco E-DI Product CD-ROM and CCO (continued)

IDU	OS Version	IDU Version
Cisco 2600	Cisco 12.1(17), 12.2(24a)	1.3
Cisco 3700	Cisco 12.3(6e)	1.1
Cisco 3800	Cisco 12.3(11)T3	1.1
Cisco 7200	Cisco 12.2(13)T14	1.2
Cisco 7600	Cisco 12.2(18)SXD4	1.1
Cisco 800	Cisco 12.3(8)T7	1.1
Cisco AP350IOS	Cisco 12.3(4)JA	1.1
IDUBase	N/A	1.3

Devices Not Supported by Cisco E-DI

Not all the devices in a customer network may have IDU support. An asterisk (*) next to the device IP address in the **show devices** output indicates that IDU support is not available for that device.

Documentation Updates

This section of the Release Notes includes the following updates to the Cisco Enhanced Device Interface documentation set:

- Example Use Case
- Viewing Security Features

Example Use Case

The Example Use Case is provided in the *Cisco Enhanced Device Interface Programmer's Guide, 2.0.1*, Chapter 1. The following details include the operations that should be used in each step, for example <**get-config**>.

Applications can use the NETCONF primitives to build more complex management scenarios.

1. The application establishes a NETCONF session with Cisco E-DI for the device to be managed—Cisco E-DI provides various ways of establishing a NETCONF session. See Appendix B, "NETCONF Client GUI" for more details.
2. Get the running configuration using a filter on the username—Applications use the standard <**get-config**> operation. In the filter, to express the command for the username, application refers to the device specific XSD. Alternatively, application can use CLI commands.
3. Make sure that the user does not already exist—This is done in the application's code.
4. Add a username to the candidate configuration—Application uses the <**edit-config**>operation with the candidate as the target data store.
5. Validate the candidate configuration—Application uses the <**validate**> operation.
6. Get a lock on the running configuration—Application uses the <**lock**> operation.

7. Commit the configuration change—Application uses the <**commit**> operation.
8. Check the running configuration with a filter on the username—Applications use the standard operation. In the filter, to express the command for the username, application refers to the device specific XSD. Alternatively, application can use CLI commands.
9. Make sure that the username is now returned—This check is done by the application in its own code.
10. Release the lock on the running configuration—Application uses the <**unlock**> operation.
11. Close the session—Application uses the <**close-session**> operation.

Viewing Security Features

Viewing Security Features is in the *Cisco Enhanced Device Interface User's Guide, 2.0.1*, Chapter 12.

Table 4 details how to check the transport method, either SNMP Write or Telnet/SSH, and the credential set.

Table 4 Commands to View Security Setup

Action	Command
To view the IP address of Cisco E-DI and the users' login ID.	`[SRV:/server]#` **`show line`**
To view the syslog messages on the devices.	`[NET:/network]#` **`show events`**
To check the status of management operations in Cisco E-DI	`[NET:/network]#` **`show devices manageability`**

Related Documentation

Refer to the following publications for additional information:

- Cisco *Enhanced Device Interface Quick Start Guide, 2.0.1*
- Cisco *Enhanced Device Interface User's Guide, 2.0.1*
- Cisco *Enhanced Device Interface Programmer's Guide, 2.0.1*
- Cisco *IDU Read-me Files*

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

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

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- Nonemergencies—psirt@cisco.com

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

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

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 linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

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, documentation, 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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- 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 "Related Documentation" section.