



Release Notes for Cisco Emergency Responder 1.3(1a)

June 1, 2006

These release notes describe the feature enhancements and caveats for Cisco Emergency Responder (Cisco ER) 1.3(1a). Use these release notes along with the Cisco ER 1.3(1) documentation at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/voice/respond/res13/index.htm>

Contents

These release notes discuss the following topics:

- [New and Changed Information, page 2](#)
- [Installation Notes, page 6](#)
- [Caveats, page 7](#)
- [Obtaining Documentation, page 9](#)
- [Documentation Feedback, page 11](#)
- [Cisco Product Security Overview, page 11](#)



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

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

- [Obtaining Technical Assistance, page 13](#)
- [Obtaining Additional Publications and Information, page 16](#)

New and Changed Information

This section highlights the new features for Cisco ER 1.3(1a):

- [What's New in Cisco ER 1.3\(1a\), page 2](#)
- [Cisco ER 1.3\(1a\) Feature Enhancements, page 3](#)
- [New Software and Hardware Support, page 3](#)
- [BARS Compatibility Message, page 5](#)

What's New in Cisco ER 1.3(1a)

Resolution of DDTs, including the following:

- **Resolution of CSCsd64154**—With Cisco ER 1.3(1a), any ERL association that is configured for a switchport on a Cisco Catalyst 3750 device or a Cisco Catalyst 3750 stack is maintained when you upgrade to Cisco ER 1.3(1a).
- **Resolution of CSCsd82684**—With Cisco ER 1.3(1a), Cisco ER is able to track phone movement from one location to another when incremental phone tracking is used when debug tracing is disabled for the phone tracking component.

For a complete list of resolved DDTs, see the [“Resolved Caveats” section on page 8](#).

Cisco ER 1.3(1a) Feature Enhancements

Cisco ER Cluster DB Host—Cisco ER 1.3(1a) stores cluster details in a cluster database on a Cisco ER server. A cluster database is created on all Cisco ER servers; you select one of the Cisco ER servers to be the Cluster DB Host for a cluster. For more information, see the “Understanding Cisco Emergency Responder Clusters and Groups” in *Cisco Emergency Responder Administration Guide 1.3(1)*.

IP Subnet Import and Export Capability—Cisco ER 1.3(1a) allows you to import and export IP Subnet data. In Cisco ER 1.3(1a) administration, select **ERL Membership > IP Subnets > Find and List IP Subnets**. For more information, see “IP Subnet Search” in *Cisco Emergency Responder Administration Guide 1.3(1)*.

New Software and Hardware Support

For a complete list of required and supported software and hardware for Cisco ER 1.3(1a), see “Network Hardware and Software Requirements” in *Cisco Emergency Responder Administration Guide 1.3(1)*.

The following sections highlight new support provided by Cisco ER 1.3(1a).

Cisco Unified CallManager Support

Cisco Emergency Responder 1.3(1a) supports Cisco Unified CallManager versions 4.2(1), 5.0(2) and previously-supported Cisco Unified CallManager versions 4.1, 4.0, and 3.3.



Note

Cisco ER 1.3(1a) does not support Cisco Unified CallManager 5.0(1) because of [CSCsd64154](#).
CSCsd64154 is resolved in Cisco Unified CallManager 5.0(2).

Supported Operated System

Cisco ER 1.3(1a) supports Version 2000.2.7 as the minimum supported version; Cisco ER 1.3(1a) also supports OS2000.4.1; OS2000.4.1(a); OS2000.4.2; and OS2000.4.3.

Backup and Restore System

Use the Cisco IP Telephony Backup and Restore System (BARS) version 4.0(9) for back up and restore of Cisco ER 1.3(1a).

Cisco Security Agent

Cisco ER 1.3(1a) supports Version 4.5.1.639 for the Cisco Security Agent (CSA) policy version 3.0(3) for Cisco CallManager.

Cisco ER 1.3(1a) has not been tested with CSA Version 5.

New Phone Support

Cisco ER 1.3(1a) adds support for the following Cisco Unified IP Phones running SCCP protocol:

- 7961G/7941G, 7961G-GE/7941G-GE
- 7911G

Cisco ER 1.3(1a) supports the following Cisco Unified IP Phones running SIP protocol:

- 7970G, 7971G-GE
- 7961G/7941G, 7961G-GE/7941G-GE
- 7960G/7940G
- 7912G/7905G
- 7911G

Cisco ER 1.3(1a) supports third-party SIP phones if they are configured as IP subnets.

New Router Support

Cisco ER 1.3(1a) adds support for the following routers:

- Cisco 2811 Integrated Service Router
- Cisco 2821 Integrated Service Router
- Cisco 2851 Integrated Service Router
- Cisco 3825 Integrated Service Router
- Cisco 3845 Integrated Service Router

MCS Platform Support

Cisco ER 1.3(1a) supports the MCS platforms shown in [Table 1](#).

Table 1 **Supported MCS Platforms**

MCS-7815	MCS-7825
MCS-7815-I1-IPC3	MCS-7825-H1-IPC1
MCS-7815I-3.0-IPC1	MCS-7825-I1-IPC1
MCS-7815-I2	MCS-7825-I2
MCS-7815I-2.0-EVV1	MCS-7825H-2.2-EVV1
	MCS-7825H-3.0-IPC1
	MCS-7825I-3.0-IPC1
MCS-7835	MCS-7845
MCS-7835-H1-IPC1	MCS-7845-H1-IPC1
MCS-7835-H1 retrofit	MCS-7845-HI retrofit
MCS-7835-I1-IPC1	MCS-7845-I1-IPC1
MCS-7835-I1 retrofit	MCS-7845-I1 retrofit
MCS-7835H-2.4-EVV1	MCS-7845H-2.4-EVV1
MCS-7835I-2.4-EVV1	MCS-7845H-3.0-IPC1
MCS-7835H-3.0-IPC1	
MCS-7835I-3.0-IPC1	

BARS Compatibility Message

When viewing BARS log files, you will see this message:

```
The version of CER installed—CER 1.3(1a) has not been verified to
function with BARS 4.0.9000. You should upgrade the BARS software to
ensure complete compatibility otherwise you could experience data loss
during restore.
```

You can disregard this message. The BARS backup will not be affected and no action is required from you.

You can ignore this message can be ignored for Cisco ER 1.3(1a). Refer to the archive build status message at the end of the BARS backup/restore run to determine if the backup or restore was successful.

Installation Notes

This section discusses the following topics

- [Supported Installation and Upgrade Paths, page 6](#)
- [Important Upgrade Notes, page 7](#)

Supported Installation and Upgrade Paths

If you are installing Cisco ER 1.3(1a) as a new installation, use the Cisco ER 1.3(a) installation CD.

For upgrades to Cisco ER 1.3(1a), download **CER-fmr.1-3-1a.exe** from the following URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cer>

You can upgrade to Cisco ER 1.3(1a) from the following Cisco ER versions:

- Cisco ER 1.2(1)
- Cisco ER 1.2(2)
- Cisco ER 1.2(3a)

See also the [“Important Upgrade Notes” section on page 7](#).

For detailed information about installing or upgrading to Cisco ER 1.3(1a), refer to Chapter 2, “Installing Cisco Emergency Responder 1.3(1)” in *Cisco Emergency Responder Administration Guide 1.3(1)*.

Important Upgrade Notes

Be aware of the following Cisco ER 1.3(1a) upgrade requirements:

- You must uninstall all Cisco ER Service Packs and Service Releases before using this upgrade, except for the MSDE 2000 SP4 patch, which is provided by Cisco for Cisco ER servers. To uninstall all Service Patches or Service Releases, use the Add/Remove Programs in the Windows Control Panel.
- You must uninstall all Service Patches or Service Releases such as Cisco ER 1.2(3)sr2 before performing the upgrade. To uninstall all Service Patches or Service Releases, use the Add/Remove Programs in the windows control panel.
- All Cisco ER servers must be upgraded to Cisco ER 1.3(1a). In a Cisco ER cluster, Cisco ER 1.3(1a) server will not operate with previous versions of Cisco ER servers.
- Data migration from Cisco ER 1.1(4) to Cisco ER 1.3(1a) is not supported. To upgrade from Cisco ER 1.1(4), you must first upgrade to Cisco ER 1.2(3a). To upgrade from Cisco ER 1.1(4) to 1.2(3a), see *Cisco Emergency Responder Administration Guide 1.2(3)* at this URL: <http://www.cisco.com/univercd/cc/td/doc/product/voice/respond/res12/res123/index.htm>.

Caveats

Known problems (bugs) are graded according to severity level. These release notes contain descriptions of:

- All severity level 1 or 2 bugs.
- Significant severity level 3 bugs.

You can search for problems by using the Cisco Software Bug Toolkit.

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Software Bug Toolkit, follow these steps:

Procedure

-
- Step 1** To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.
- Step 2** Log on with your Cisco.com user ID and password.
- Step 3** Click the **Launch Bug Toolkit** hyperlink.
- Step 4** To look for information about a specific problem, enter the bug ID number in the “Enter known bug ID” field and click **Search**.
-

This section includes these topics:

- [Resolved Caveats, page 8](#)
- [Cisco.com, page 10](#)

Resolved Caveats

[Table 2](#) describes the problems that are resolved in Cisco ER 1.3(1a).

Table 2 *Resolved Caveats for Cisco ER 1.3(1a)*

Bug ID	Summary and Bug Toolkit Link
CSCsb16653	Cisco ER alerts if CTI link is broken http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb16653
CSCsc33312	On finishing the installation, selecting Yes does not reboot server http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc33312
CSCsd29918	With a newly installed Cisco ER Subscriber, no GUI is shown http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd29918&

Table 2 *Resolved Caveats for Cisco ER 1.3(1a) (continued)*

Bug ID	Summary and Bug Toolkit Link
CSCsd64154	Lost ERL association for switchport after Cisco ER upgrading http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd64154
CSCsd82684	IP subnet configuration does not discover Cisco IP Unified Phone 7920 on incremental discovery http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd82684

Open Caveats

Table 3 describes the problems that are known to exist in Cisco ER 1.3(1a).

Table 3 *Open Caveats for Cisco ER 1.3(1a)*

Bug ID	Summary and Bug Toolkit Link
CSCsdc09114	Manual backup is required for Cisco ER call data http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsdc09114

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](#), page 10
- [Documentation DVD](#), page 10
- [Ordering Documentation](#), page 10

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 web sites at this URL:

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

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 webbiest 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

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>. If you require further assistance please contact us by sending email to export@cisco.com.

See the “[Reporting Security Problems in Cisco Products](#)” section on page 12 for additional information.

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.

See the following sections for additional information:

- [Cisco Technical Support & Documentation Website, page 14](#)
- [Submitting a Service Request, page 14](#)
- [Definitions of Service Request Severity, page 15](#)

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>

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

© 2006 Cisco Systems, Inc. All rights reserved.

