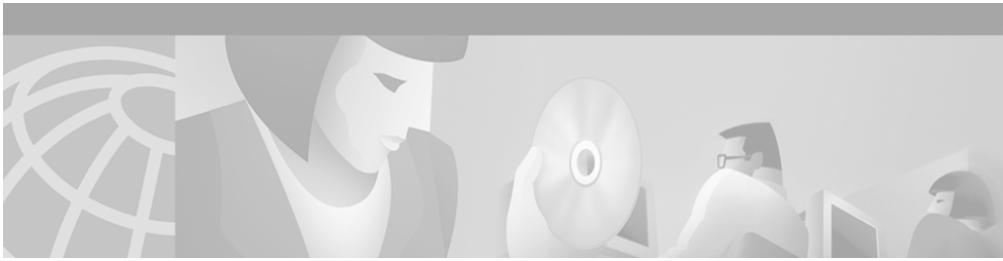

Release Notes for Cisco Emergency Responder 1.1(2)

Updated August 6, 2003

These release notes describe the known problems for Cisco Emergency Responder version 1.1(2).

These release notes provide the following information:

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

What's New in Cisco Emergency Responder 1.1(2)

These are the changes and new features in the 1.1(2) maintenance release for Cisco Emergency Responder. These changes are not reflected in the CER documentation or in the CER online help.

Note Cisco Emergency Responder does not support Cisco CallManager installed on the Cisco Integrated Communications System (ICS) 7750.

Note Cisco ER does not support Cisco ATA. Although Cisco ATA devices support CDP and SCCP, Cisco ER cannot automatically track them. You can add Cisco ATA devices manually and assign them to an ERL and Cisco ER will route calls from Cisco ATA devices based on the assigned ERL.

- **Installation requirement**—You can only install 1.1(2) if 1.1(1) is already installed on the server.
- **New switch support**—You can now use Catalyst 2900XL switches with CER. CER will dynamically identify phones that use the Cisco Discovery Protocol (CDP). Phones that are tracked using CAM tables can only be tracked if they are connected to data or native VLANs; phones connected to auxiliary VLANs cannot be tracked using CAM tables on the 2900XL. Because Cisco IP Softphone uses the data or native VLAN, CER can track it when attached to a 2900XL switch. See the *Cisco Emergency Responder Administration Guide* for an explanation of which phones use CDP or CAM tracking.
- **New Cisco CallManager support**—CER 1.1(2) supports Cisco CallManager 3.1(3a), 3.2(1), and 3.2(2a). During installation, you are asked which version of Cisco CallManager you are using.

  After you install CER, if you later upgrade from Cisco CallManager 3.1 to 3.2, you need to run the C:\Program Files\Cisco Systems\CiscoER\bin\CCM3.2.bat file.

Note that a single CER *group* cannot support a mix of Cisco CallManager 3.1 and 3.2 clusters: it can only support all 3.1 or all 3.2 clusters. However, a CER *cluster* can contain CER groups that support different versions of Cisco CallManager. In this way, CER can support a mix of Cisco CallManager versions in your telephony network.

- **CER clustering**—If you combine CER groups into a CER cluster as described in the *Cisco Emergency Responder Administration Guide*, each group can run different versions of CER. However, within a single CER group, Cisco recommends that both CER servers run the same version of CER. You can only mix CER versions within a CER group if the group is supporting a Cisco CallManager 3.1 cluster.
- **Support for Active Directory**—In CER 1.1(1), you could only use the Cisco CallManager DC directory. CER 1.1(2) adds support for Active Directory. You can now use either the DC directory or Active Directory. However, CER does not automatically transfer data between directory types if you move from one type to another. You must reconfigure CER. To simplify the reconfiguration, export any data that you can export using the CER web interface. Then, when you reconfigure CER, you can import the exported data. See the administration guide for information on the types of data you can export and how to export it; see the "Changing Directories for an Existing CER Group or Cluster" section on page 8 for additional steps you must complete if you change directory types.

  Active Directory imposes a size limitation on the number of entries that can be processed. Although the default limit is larger than Cisco's recommended limitations for CER, you might need to modify your Active Directory configuration depending on your CER configuration. See the "Understanding and Resolving Active Directory Size Limitations" section on page 9 for more detailed information.
- **Manual phone definition changes**—The CER web interface has been improved to make it easier to define and manage a large number of manually-defined phones. Manually-defined phones are those that CER cannot support directly, such as analog phones.

  In CER 1.1(2), when you select **Port/Phone > Add/Modify Phones**, you are now presented with a new page: Find and List Manually Configured Phones. From this page, you can search for phones based on extension, which makes it easier to find a phone you need to modify. To add phones manually, click **Add a new phone** on this page. You can then follow the manual phone procedure described in *Cisco Emergency Responder Administration Guide*.

Note that the Add/Modify Phones page no longer lists manual phones; manual phone lists are only available on the Find and List Manually Configured Phones page. To delete a manually-defined phone, you must first list it; then, you can click the delete icon for the phone.

See the administration guide for more detailed information about manual phones and their use.

- **Fixed problems**—Table 1 lists the bugs that were fixed in the 1.1(2) maintenance release. See the "Cisco Emergency Responder Known Problems" section on page 21 for a current bug list.

Table 1 Fixed Problems in Cisco Emergency Responder 1.1(2)

Bug ID	Summary
CSCdv68753	The server name is not shown in the control center (**CER Group > Control Center**). CER now shows the server name (as defined in CER) as well as the IP address or DNS host name.
CSCdw64139	On the CER Group Settings page (**CER Group > CER Group settings**), the Source Mail ID field does not allow email addresses longer than 30 characters. CER now allows longer email addresses.
CSCin00333	The CTI Manager address is not printed in the log when it unregisters the 912 route point. CER now includes the CTI Manager address in the log file kept in the CER root directory when the CTI Manager unregisters a route point.
CSCin00390	If you specify the wrong password for the CTI Manager Password when configuring the Cisco CallManager settings (**Phone Tracking > Cisco CallManager Details**), CER continues to try to log into Cisco CallManager using the wrong password even after you fix the password and CER successfully logs in using the updated password. CER now ends the errant login process gracefully.
CSCin01831	When you modify ERL details, the modification is not reflected in the standby CER server. CER now reflects the modification in both the primary and standby servers.

Table 1 Fixed Problems in Cisco Emergency Responder 1.1(2) (continued)

Bug ID	Summary
CSCin02022	After adding an ERL, when you list ERLs from a remote CER group, you cannot see the route point-ELIN or onsite alert information for the remote ERLs. CER now displays correct information when listing ERLs from remote CER groups.
CSCin02052	Under some conditions, the top frame of the Switch Port Details Find tab (**Port/Phone > Switch Port Details**) displays old search criteria when you return to the tab from the Configure tab. CER now always displays the search criteria used to generate the list in the bottom frame of the Find tab, if any, when you return to the Find tab from the Configure tab.
CSCin02063	If you enter the wrong server name in the email address for an onsite alert person, no email is sent to any onsite alert personnel assigned to an ERL configured with the misconfigured onsite alert person, even if the other email addresses are correct. CER now sends email to all correct email addresses, even if one is incorrect.
CSCin02177	When listening to a security alert message, if the listener presses more than one key, there is a 10 to 15 second pause before continuing the message. CER now handles multiple DTMF entries more gracefully.
CSCin02207	If CAM tracking is enabled for a switch, under some conditions a single MAC address might be duplicated such that it is on both the associated and unassociated tables. CER now ensures that MAC addresses do not get duplicated between the associated and unassociated tables.

Table 1 Fixed Problems in Cisco Emergency Responder 1.1(2) (continued)

Bug ID	Summary
CSCin02253	Misdirected emergency calls when using Extension Mobility and shared lines. If you are using Extension Mobility on a phone, emergency calls might get misdirected if the user makes an emergency call before CER has run an incremental phone tracking process. For example, you have two phones, X and Y, that use the same extension, 2000. A user logs into phone X to get extension 3000, and makes an emergency call before CER runs phone tracking. CER still sees phone X as having extension 2000, and matches the ERL based on this information (thus, routing the call based on the ERL assigned to phone Y). During the next phone tracking process, CER recognizes the new extension on phone X. CER 1.1(2) eliminates this problem.
CSCin02370	If you associate a phone in the unlocated phones list (**Port/Phone > Unlocated Phones**) to an ERL, and then add a line to the phone, emergency calls from the new line are routed based on the default ERL rather than the assigned ERL. CER now uses the assigned ERL for every line configured for a phone on the unlocated list.
CSCin02388	There is a typographical error on the Server Settings page, where "ECS" is used instead of "CER." The typographical error is now fixed.
CSCin06702	Although you can configure Port Name information for a port (when configuring ports during switch configuration, not through CER), Port Name is not included in the information sent to onsite alert personnel in a web alert. CER now includes the Port Name information in web alerts. Tell the onsite alert personnel to click the alert to see the information.
CSCdw10852	CER does not allow you to configure Gigabit Ethernet ports. Any phone directly attached to a Gigabit Ethernet port is not tracked. CER now allows you to configure Gigabit Ethernet ports.

Table 1 Fixed Problems in Cisco Emergency Responder 1.1(2) (continued)

Bug ID	Summary
CSCdv65059	CER does not handle duplicate CDP entries properly (thus, a phone with duplicate entries is identified as being attached to two switch ports). CER now places phones that have duplicate CDP entries on the unlocated phones list. CER then tries to rediscover the phone on the next switch-port and phone update process or phone tracking process. Typically, one of the duplicate entries will expire from the CDP cache before the next CER update.
CSCin10038	If the Cisco CallManager server is unavailable during a CER phone tracking process, CER continues to see the server as unavailable even after it becomes available again, thus preventing phones from being tracked. To get around this problem, you could delete and then re-add the Cisco CallManager server to the CER configuration, or restart CER. CER now sees the correct current status of the Cisco CallManager server for every phone tracking process. You do not have to restart CER or alter the Cisco CallManager configuration in CER.
CSCin09716	If you do not enter a value for CER Group Name when configuring a CER group, CER uses the directory server's host name or IP address as the CER group name. Now, CER uses the primary Cisco CallManager server name as the default CER group name. Rather than accepting the default name, Cisco recommends that you specify a CER group name to ensure it is meaningful to you. Note that this change will not overwrite any existing CER group names, whether they were chosen by default or explicitly entered.
CSCdw05656	Cisco IP Softphone sends the wrong IP address in requests to CER if you change the IP address on the machine running the phone after you start the phone. You must restart the phone to get the correct address. Now, as long as you select Automatic for IP address configuration, Cisco IP Softphone sends the correct IP address on requests to CER. If you do not use Automatic address selection, you still must restart Cisco IP Softphone if you change the IP address on the machine.
CSCdv83837	CER does not include the port Location field in email alerts. CER now includes the Location field. When you configure switch ports in CER, you can add specific location information for each port to help onsite alert personnel more quickly locate an emergency caller.

Changing Directories for an Existing CER Group or Cluster

If you change the Cisco CallManager directory that a CER group or cluster is using, you must make some changes for CER to see the new directory. This is necessary if you have a working CER setup and you change the type of directory that Cisco CallManager is using (for example, you change from DC Directory to Active Directory.

Before You Begin

This procedure does not transfer data between directories. You must transfer the data manually. See the documentation for the directory for more information.

Procedure

Step 1 Update the E911Bootstrap.properties file on all CER servers in a CER group that use the changed directory. Table 2 describes the relationship between the registry key on the Cisco CallManager directory server and the parameters in the E911Bootstrap.properties file. Change the E911Bootstrap.properties parameters so that they are the same as the equivalent registry keys on the Cisco CallManager directory server.

Table 2 CER Group and Cisco CallManager Directory Key Equivalents

CER ServerGroup Directory Details Settings	Cisco CallManager Directory (Used by CER Group) Key Settings
E911Bootstrap.properties	**\\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Directory Configuration**
LDAPURL=	LDAPURL
MGRDN=	MGRDN
MGRPW=	MGRPW
DS=	DIRTYPE
CISCOBASE=	CISCOBASE
CCNBASE=	**OU=CCN,** *CISCOBASE*

Step 2 Update the E911Bootstrap.properties file on all CER servers in a CER *cluster* that use the changed directory as the CER cluster directory server. Table 3 describes the relationship between the registry key on the Cisco CallManager directory server and the parameters in the E911Bootstrap.properties file. Change the E911Bootstrap.properties parameters so that they are the same as the equivalent registry keys on the Cisco CallManager directory server.

Table 3 CER Cluster and Cisco CallManager Directory Key Equivalents

CER Cluster Directory Details Settings	Cisco CallManager Directory (Used by CER Cluster) Key Settings
E911Bootstrap.properties	**\\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Directory Configuration**
PRIMARY_LDAP_URL=	LDAPURL
PRIMARY_USER_DN=	MGRDN
PRIMARY_USER_PWD=	MGRPW
PRIMARY_CISCOBASE=	CISCOBASE
PRIMARY_CCNBASE=	**OU=CCN,** *CISCOBASE*

Step 3 Restart all CER services on the CER servers whose E911Bootstrap.properties file you changed.

Understanding and Resolving Active Directory Size Limitations

If you use Microsoft Active Directory, be aware that the MaxPageSize setting limits the number of certain types of entries that CER can process. This limitation includes the number of LAN switches (but not switch ports), ERLs, unlocated phones, and manually-defined phones.

The default MaxPageSize limit is 1000. If this limit is reached, CER does not process any of those entries that exceed the limit (for example, if you define 1001 switches in CER, CER only manages 1000). CER logs this error in the CER logs and in Windows Event Viewer.

The default MaxPageSize limit is larger than the number of entries Cisco recommends that you use with CER, so this should normally not be a problem. However, if you need to exceed this limit, you should change the Active Directory settings to increase the limit using this procedure.

Procedure

Step 1 Log into the Active Directory server using an administrator account and open a command prompt.

Step 2 Enter **NTDSUTIL**.

The command prompt should change to `ntdsutil:`.

Step 3 Enter **LDAP Policies**.

The command prompt should change to `Ldap Policies:`.

Step 4 Enter **connections**.

The command prompt should change to `server connection:`.

Step 5 Enter this command, where *DNS-name-of-this-AD-server* is the DNS name of the Active Directory server on which you are entering the command.

connect to server *DNS-name-of-this-AD-server*

You should be bound to the Active Directory server.

Step 6 After binding to the server, enter **q**.

The command prompt should change to `Ldap Policies:`.

Step 7 Enter **Show Values** and look for MaxPageSize to determine the current setting.

Step 8 To increase the MaxPageSize limit, enter this command, where *limit* is the new limit you want to set.

Set MaxPageSize to *limit*

Step 9 Enter **Commit Changes** to save your change.

Step 10 Enter **Show Values** and confirm the change to the MaxPageSize setting.

Step 11 Enter **q** until you return to the original Windows command prompt.

Step 12 Restart all CER services.

CER should now be able to process entries up to your new limit.

Documentation Roadmap

Use these publications to learn how to install and use CER. All CER documents are available online at:

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

- *Cisco Emergency Responder Administration Guide* (DOC-7813718=)—Describes how to plan for, install, configure, manage, and use the CER application. An Adobe Acrobat (PDF) version of this manual is available in the CER administration online help.
- CER Administration online help—Contains all of the information available in *Cisco Emergency Responder Administration Guide*. This ensures you have complete information even if you do not have the manual readily available while using CER.
- *Cisco Emergency Responder User's Guide*—Describes how to use the end-user interface, used by onsite alert (security) personnel to obtain information about emergency calls. This guide is built into the end-user interface as the online help system. The online help includes a PDF version you can use to print the guide for distribution.

Important Notes

This section includes important information that did not get included in the CER manuals. Use this list in conjunction with the "What's New in Cisco Emergency Responder 1.1(2)" section on page 2.

- Before deploying CER throughout your enterprise, test the ALI submission process with your service provider, and with your service provider's help, test that the PSAP can successfully call back into your network using the ALI data. Each service provider and ALI database provider can have slightly different rules concerning ALI information. CER allows you to create ALI data according to the general NENA standards, but your service provider or database provider might have stricter rules.
- Cisco CallManager supported version is 3.1(3a) or higher.

- During installation, CER resets the Administrator local user's password to blank. At the end of installation, you are prompted to change the password. If you leave the password blank, you will encounter the problem described in Table 7 for CSCdu76987.
- The manual mentions how to open the CER web administration interface in a browser. You can also open the interface from the Start menu by selecting **Start > Programs > Cisco Emergency Responder > CER Web Administration**.
- The MCS servers listed in the manual are not the correct servers for CER. Table 4 lists the correct servers.

Table 4 Supported Media Convergence Server Platforms

Component	MCS-7835-1266	MCS-7825-1133
Processor	Intel Pentium III, 1.266 GHz	Intel Pentium III, 1.133 GHz
Cache	512-KB Level 2 ECC cache	256-KB Level 2 ECC cache
Memory	1-GB 133-MHz Registered ECC SDRAM	1-GB 133-MHz Registered ECC SDRAM
Network Connectivity	Two Fast Ethernet NIC Embedded 10/100 Wake On LAN (WOL).	Two Fast Ethernet NIC Embedded 10/100 Wake On LAN (WOL).
Storage	• Dual 18.2-GB Ultra3 SCSI hot-plug drives • Integrated Smart Array 5i Controller (Ultra3 SCSI)	• Single 40-GB Ultra ATA/100 7200 RPM non-hot-plug drive • Integrated Ultra ATA/100 Controller Module
Floppy Drive	1.44-MB diskette drive	1.44-MB diskette drive
CD-ROM Drive	24X Max IDE CD-ROM Drive	Removable CD-ROM/Diskette drive assembly
Power Supply	Hot-plug redundant 400-watt power supply	180-watt PFC Power Supply
Video	Integrated ATI Rage XL Video Controller with 8MB Video Memory	Integrated ATI Rage XL Video Controller with 4 MB video memory
Backup Drive	Optional 20/40-GB DAT (digital audio tape) hot-plug drive	Not available

- The administration guide mentions many of the conditions in which an emergency call is routed using the Default ERL. The Default ERL is also used for all emergency calls when the CER server is first started (or restarted when there is no standby CER server) until the initial switch-port and phone update process is finished (this process is started immediately).
- When you configure the SNMP strings for your switches (as described in the administration guide), you must also configure the SNMP strings for your Cisco CallManager servers. CER must be able to make SNMP queries of all Cisco CallManager servers that it supports.
- The administration guide lists the switches that CER supports. This list includes the Catalyst 4200 series; however, this switch is not supported.

  Note that hub topologies are not supported. Also note that DSL, VPN, ISDN, and other remote or dial-in technologies are not supported, which means that CER cannot support telecommuters who have phones linked into your network over these types of lines.
- CER does not support survivable remote site telephony (SRST). If you deploy CER over a WAN link, the link must be active for CER to work correctly.
- The administration guide explains how to create a Cisco CallManager user for CER's use, and lists the types of CTI ports and route points that need to be assigned to the user. This information must be complete before CER tries to create a provider with the CER cluster. CER only registers the CTI ports and route points that are associated with the user when the provider is created. Thus, any devices you add to the user after starting CER will not be registered by CER.

  If you add devices to the CER user in Cisco CallManager, you can force CER to recreate the provider using any of these techniques:

  – Restart the CER server.

  – Delete the Cisco CallManager server from the CER configuration and re-enter it.

  – Change the backup CTI Manager setting for the Cisco CallManager server in the CER configuration and click **Update**. This forces CER to log off the provider and recreate it.

  – Change the name of the user in Cisco CallManager, or create a new user, and associate all devices with it. Then update the CER configuration to use the new user.

- CER directs emergency calls based on the ERL assigned to the phone from which a call is made. Most of the time, the ERL is determined based on the switch port to which the phone is connected. However, if the switch port is not assigned to an ERL, or if the call comes from a phone attached to the network in an unsupported manner, CER determines the ERL for the phone in this order:
  - If the phone number is defined as a manual phone, the call is routed based on the manual entry.

    If you are sharing a line between an analog phone and an IP phone, and you define the analog phone manually, calls from the shared phone number might be routed based on the manual definition even if the call is from the IP phone. This will occur if the IP phone cannot be located by any CER group in the cluster.
  - If the phone is assigned an ERL on the unlocated phones list, and it has not been located in another CER group in the CER cluster, the call is routed based on this ERL.
  - If the phone is on the unlocated phones list but has been located by another CER group in the CER cluster, the call is routed to the other CER group, which handles the emergency call routing.
- If CER cannot direct an emergency call using the route patterns assigned to an ERL, CER tries to use the route patterns assigned to the Default ERL. If this also fails, CER routes the emergency call to the security numbers assigned to the ERL (thus directing the emergency call to the onsite alert personnel assigned to the ERL).

Troubleshooting ALI Data Uploads

Periodically, you must export your ALI data and submit it to your service provider. The ALI data is used to route emergency calls from your network to the correct PSAP, and provide the PSAP with information about the location of the emergency call.

CER lets you export the ALI data in a variety of NENA formats. Ask your service provider which format you should use.

During the upload process, you might find that some ALI data records did not upload correctly. Your service provider should be able to provide you with a list of errors, or you might see these when using your service provider's data upload software. You must fix any mistaken records and resubmit the ALI data export file. To fix the records, you might need to manually edit the records in error.

These sections describe the general procedure for fixing ALI data records, and explain how to edit the various types of NENA formatted files:

- Fixing ALI Data Records, page 15
- Editing NENA 2.0 and 2.1 File Formats, page 16
- Editing NENA 3.0 File Formats, page 18

Fixing ALI Data Records

If you receive data errors when uploading ALI records to your service provider, use this procedure to correct the errors.

Before You Begin

Obtain NENA Doc 02-010, *Recommended Formats and Protocols for Data Exchange*, from NENA or your service provider. This document explains the various NENA formats in detail.

Procedure

Step 1 Look through the error reports to determine the problems you encountered. Using the CER GUI, change the fields that were in error for the ERL/ALI records that failed. For example, if the Street Suffix was an unacceptable abbreviation, change it to an acceptable one. Save all of your changes.

Step 2 Export the ALI data again (see the online help).

Step 3 If any of the records in error were new, you must change the database function for the records. Because CER has already exported these records, CER will label them as updates rather than new insertions. However, because these records failed on upload, the service provider's database will view them as new.

Open the ALI export file in a text editor and change the function code for the records that you are fixing. Use an editor that will not add formatting or other extra characters. See these sections for details about editing the files:

- Editing NENA 2.0 and 2.1 File Formats, page 16
- Editing NENA 3.0 File Formats, page 18

Step 4 Submit the edited file to your service provider.

Editing NENA 2.0 and 2.1 File Formats

The NENA 2.0 and 2.1 file formats have these characteristics:

- Fixed-length records
- Fields are in a specific order
- Unused fields are filled with blanks
- End of record is indicated by an asterisk (*)

Use NENA Doc 02-010, *Recommended Formats and Protocols for Data Exchange*, to determine the byte location and length of each field. When you edit the file, ensure that you are not lengthening the records. Delete any extra spaces that get added. If the length of an item is less than the length of a field, pad the field with blanks. Depending on the field, padding might be on the right or the left.

The file contains one header and one trailer record. The ALI data records are contained between these records.

Table 5 describes the fields you are most likely to edit. You should use the CER GUI to change the other fields.

Table 5 NENA 2.0 and 2.1 Common Fields

Field	Description
Function Code	**Location:** Byte 1. **Length:** 1 character. **Description:** The database function for the record. One of: • **I**—Insert new ALI record • **C**—Change existing record. You must have successfully uploaded the record once before you can use C. If you are correcting a record that has never been successfully uploaded, change the C to an I. • **D**—Delete the record. CER only generates a deletion record once, in the export file created after you deleted the ALI from the CER configuration. If you need to regenerate the record, cut and paste it from the previous export file (and adjust the record count), or recreate the ALI in CER, save it, export the data, then delete the ALI and export the data again.
Cycle Counter (sequence number)	**Location:** Byte 62 to 67. **Length:** 6 characters. **Description:** The sequence number of the file you are submitting to the service provider (for example, 1, 2, etc.) The number is right-aligned with leading spaces. Your service provider might ignore this field.
Record count	**Location:** Byte 62 to 70 in the trailer record. **Length:** 9 characters. **Description:** The total number of records in the file you are submitting to the service provider (for example, 1, 2, etc.) The number is right-aligned with leading spaces.

Editing NENA 3.0 File Formats

The NENA 3.0 file format has these characteristics:

- Variable-length records.
- Fields are a tag and data combination, and can be in any order.
- Unused fields are not included. The presence or absence of a tag has this effect:
  - If the tag is not included, the previous value of the element, if any, is left unchanged.
  - If the tag is included with a blank value, any previous value for the element is removed.
  - If the tag is include with a non-blank value, the value of the element is changed to the new value.
- Tags are separated by a vertical bar (|).
- End of record is indicated by a pre-defined character.

Use NENA Doc 02-010, *Recommended Formats and Protocols for Data Exchange*, to determine tag name and values for each field. Ensure that your values do not exceed the maximum length for the field. You do not need to pad fields with extra blanks.

The file contains one header and one trailer record. The ALI data records are contained between these records.

Table 5 describes the fields you are most likely to edit. You should use the CER GUI to change the other fields.

Table 6 NENA 3.0 Common Fields

Field	Description
Function Code	**Tag:** FOC. **Description:** The database function for the record. One of: • **I**—Insert new ALI record (FOCI) • **C**—Change existing record (FOCC). You must have successfully uploaded the record once before you can use C. If you are correcting a record that has never been successfully uploaded, change the C to an I. • **D**—Delete the record (FOCD). CER only generates a deletion record once, in the export file created after you deleted the ALI from the CER configuration. If you need to regenerate the record, cut and paste it from the previous export file (and adjust the record count), or recreate the ALI in CER, save it, export the data, then delete the ALI and export the data again.
Cycle Counter (sequence number)	**Tag:** CYC. **Description:** The sequence number of the file you are submitting to the service provider (for example, CYC1, CYC2, etc.) Your service provider might ignore this field.
Record count	**Tag:** REC in the header and trailer records. **Description:** The total number of records in the file you are submitting to the service provider (for example, REC1, REC2, etc.)

Documentation Errata

This section lists mistaken information in the printed version of the *Cisco Emergency Responder Administration Guide*. Some of these errors have been corrected in the CER online help and on the cisco.com web site. This list does not include errata due to changes made in maintenance releases; see the "What's New in Cisco Emergency Responder 1.1(2)" section on page 2 for that information.

- Chapter 4, section "Creating Emergency Responder Users," the list of Windows group names is correct. However, step 6 uses incorrect names for two of these groups. Instead of "E911SystemAdmins," read "CERSystemAdmin." Instead of "E911Users," read "CERUser."
- Chapter 6, section "Collecting System Logs with Syslog," steps 2 and 3 are reversed. You must first enable Syslog before you can enter the name of the syslog server.
- Appendix A, section "Telephony Settings," the description for UDP Port Begin incorrectly states that you must enter an even-numbered port. In fact, you can use an even or odd number, and CER uses the ports in sequence (for example, if you select 32000, CER uses 32000, 32001, 32002, and so forth).
- Appendix A, section "Cisco CallManager Details," the description for the Cisco CallManager field says that clicking **CCM List** will show you the version running on the Cisco CallManager server, and whether that version is supported. In fact, this information is not shown.
- Appendix A, section "CER Group Settings," these items are incorrect:
  - Minimum Heartbeat Count is 3 (not 1)
  - Minimum Heartbeat Interval is 30 (not 10)
  - Minimum Active Call Timeout is 30 (not 1)
  - The SMTP Mail server can also be entered as an IP address (as well as using the fully-qualified domain name)

Cisco Emergency Responder Known Problems

Known problems are unexpected behaviors or defects in the product. They are graded according to severity level. These release notes contain information about some of the known problems that you might encounter.

You can search for additional known problems on the Cisco bug tracking system tool, called Bug Toolkit. To access Bug Toolkit, enter http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl in your web browser.

Table 7 describes restrictions or other known issues for using CER 1.1.

Table 7 Cisco Emergency Responder Known Problems

Bug ID	Summary	Explanation
CSCdu76987	Domain user can log into CER with an invalid password.	If you install Service Pack 2 on Windows 2000 Server, a domain user identified in one of the CER user groups can log into CER using an invalid password if the domain user's password is blank. To avoid this problem, ensure that all domain users added to CER groups have non-null passwords.
CSCdw04143	IIS (inetinfo) can crash if there are more than 500 IP Softphones.	IP Softphones advertise themselves to CER on a periodic basis. If more than 500 IP Softphones happen to advertise themselves at the same time, inetinfo (IIS) does not handle this many requests gracefully and shows some erratic behavior. We recommend you do not have more than 500 IP Softphones per CER group. If you run into this problem, restart IIS and the CER Admin server.

Table 7 Cisco Emergency Responder Known Problems (continued)

Bug ID	Summary	Explanation
CSCdw04518	Change of switch families does not discover ports.	If you add a switch to the CER configuration, then reuse that switch's IP address for a switch of a different model, CER cannot discover the ports on the new switch. For example, if you add 10.10.10.12 to CER for a Catalyst 3500, then reassign 10.10.10.12 to a Catalyst 6000, CER cannot discover the ports on the Catalyst 6000. To avoid this problem, if you reassign an IP address to a different switch model, remove the switch from the CER configuration, then add it back to the CER configuration. This allows CER to identify the changed switch model.
CSCdw05627	If the LDAP directory is unavailable when an emergency call is made, no call history records are generated.	CER saves call history information in the Cisco CallManager LDAP directory. Therefore, if the directory is unavailable, call history information for emergency calls made during the LDAP down-time is lost.
CSCdw23712	Issues when transferring a call to the emergency number.	If you transfer a caller to the emergency call number (such as 911), the call is successfully transferred to the PSAP. However, there are some limitations to this: • The call is routed to the PSAP based on the ERL for your phone, not the caller's phone. Thus, the call might be routed to the wrong PSAP. • The PSAP receives callback information for your phone extension, not the extension of the caller who you transferred. • The notification sent to onsite alert personnel contains information about your phone, not the caller's phone.

Table 7 Cisco Emergency Responder Known Problems (continued)

Bug ID	Summary	Explanation
CSCin02233	Unexpected behavior when moving a phone used with Extension Mobility	If you move a phone that is used with Extension Mobility (that is, so that users can log into the phone and receive calls to their own phone number), emergency calls might be misdirected if the phone moves between Cisco CallManager clusters that are supported by different CER groups. For example, you move phone X from one CER group ABC to group DEF, but the phone still homes to the Cisco CallManager supported by group ABC. A user logs into the phone with extension Y and makes an emergency call. The call is routed using the wrong ERL in CER group DEF. After CER performs a phone tracking process in group ABC, extension Y will show up as an unlocated phone in CER group DEF's GUI, with nothing listed in the remote server field. Now, if an emergency call is made from extension Y, it is routed based on Y's ERL in CER group ABC. This behavior is the result of MAC addresses not being transferred across inter-cluster links. To avoid these problems, run a full switch-port and phone update process on both CER server groups, or wait for the incremental phone tracking process to run on both CER server groups.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following 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 is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

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

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

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

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **Email** option under the "Leave Feedback" at the bottom of the Cisco Documentation home page.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- 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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires 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 the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; 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 will automatically open a case.

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

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

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

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