Troubleshoot Cisco Emergency Responder

- Troubleshoot Phone-Related Problems , on page 1
- Troubleshoot Emergency Call Problems , on page 7
- Troubleshoot Licensing, on page 12
- Troubleshoot Email Alerts , on page 13
- Troubleshoot Web Alerts , on page 18
- Troubleshoot Emergency Responder System and Administration Problems , on page 19
- Troubleshoot Emergency Responder System Problems , on page 24
- Troubleshoot Cisco Unified Communications Manager Configuration Problems , on page 25
- Identify Emergency Responder Groups and Servers in Cluster , on page 26
- Manage Emergency Responder Server , on page 26
- Troubleshoot ALI Data Uploads , on page 27
- Call History Logs , on page 30
- Trace and Debug Information , on page 31
- Event Messages , on page 32
- Performance Management , on page 32
- Network Management Systems Integration , on page 32
- Data Backup and Recovery, on page 34
- Troubleshooting Data Migration Assistant, on page 34
- Troubleshoot Linux Upgrades , on page 35
- Troubleshoot SAML Single Sign-On, on page 36
- Troubleshoot IOS Switch Upgrades, on page 36

Troubleshoot Phone-Related Problems

The following sections help you troubleshoot problems related to assigning phones to ERLs and managing the phones.

Check Unified CM SNMP Settings

If Cisco Emergency Responder (Emergency Responder) is not discovering the phones homing to Cisco Unified Communications Manager (Unified CM), check that all Unified CMs are SNMP-reachable and that the SNMP settings are correct. Emergency Responder logs an event if Unified CM is SNMP-unreachable.

Procedure

Step 1 Log in to the Emergency Responder Administration CLI and use the following command to ping the Unified CM server:

```
utils network ping <ipaddress of CUCM>
```

Step 2 If you successfully ping the Unified CM, verify that the SNMP settings are correct on Unified CM, as follows:

- If you are using a Linux-based version of Unified CM (version 6.0 or higher), log in to the Unified CM Serviceability web interface and use the SNMP web pages to check the SNMP community string settings.
- If you are using a Windows-based version of Unified CM, open the services on Unified CM and choose **Start > Settings > Control Panel > Administrative Tools > Services Properties > SNMP > Properties > Security Tab**.

Step 3 Check to see if Unified CM is SNMP reachable by running the following CLI command on the Emergency Responder server:

```
utils snmp get <ccm ip-address/host name> <snmp-read-community-string> 1.3.6.1.2.1.1.2.0
```

If the Unified CM is SNMP reachable, then the output of the preceding command should be similar to the following:

```
Variable = 1.3.6.1.2.1.1.2.0

value = OBJECT IDENTIFIER <sys-oid-of-ccm>
```

Unlocated Phones

Emergency Responder obtains a list of registered phones from Unified CM and tries to locate all phones. If Emergency Responder cannot locate a phone behind a switch port or in any configured IP subnets, and the phone is not a configured synthetic phone, the phone is placed in the list of unlocated phones.

If there are a lot of unlocated phones, first try running the switch port and phone update process to see if Emergency Responder can resolve some of the problems automatically. See Manually Run the Switch-Port and Phone Update Process for more information.

These are some of the situations that can prevent Emergency Responder from locating a phone:

- If more than one switch port reports the phone as a Cisco Discovery Protocol (CDP) neighbor, then the phone is placed in unlocated phones. This condition is corrected in the next phone tracking when only one switch port reports this phone as its CDP neighbor.
- The phone is attached to a switch that is not defined in Emergency Responder. See LAN Switch Identification for information about defining switches.
- The phone is connected to an unsupported device, such as a router port, a hub connected to a router, or an unsupported switch. See Network Hardware and Software Requirements for a list of supported switches. See Manually Define Phones for information about configuring these types of phones if you cannot connect them to a supported device.
- The phone is connected to a hub, which is connected to a supported switch port, but it does not support CDP. Emergency Responder can consistently discover CDP-enabled phones attached to hubs (which are

attached to supported switch ports), but cannot always track non-CDP phones attached in this manner. For non-CDP phones, ensure the phones are attached directly to supported switch ports.

- The switch to which the phone is connected is currently unreachable, for example, it does not respond to SNMP queries. This could be for several reasons:
  - The SNMP read community string on the switch does not match the string configured in Emergency Responder. Correct the Emergency Responder configuration. See Set Up SNMPv2.
  - The phone requires CAM table access, but CAM tracking is not enabled for the switch in Emergency Responder. See LAN Switch Identification.
  - There is a network outage preventing communication between the Emergency Responder server and the switch. Locate and resolve the network outage problem.

    Unreachable switches are not retried until Emergency Responder runs the next full switch port and phone update process, unless you run it against the individual switch.
- The phone has moved to a switch served by a different Emergency Responder group. If this is the case, the Emergency Responder group name is shown for the phone in the unlocated phones list. If the phone is not in the next incremental phone tracking process after it is moved, the phone remains unlocated in any Emergency Responder group until a full switch port and phone update process is run.
- The phone requires CAM-based tracking, but CAM-based tracking is not enabled on the switch to which the phone is connected. Cisco IP SoftPhone and some other phone models require CAM-based tracking. See LAN Switch Identification for information about enabling CAM-based tracking, and Network Hardware and Software Requirements for a list of phones that require CAM-based tracking.

After fixing the problems that are preventing Emergency Responder from locating phones, run the switch port and phone update process on the affected switches, or on all switches:

- To run the process on a specific switch—Select **Phone Tracking > LAN Switch Details** and select the switch in the left-hand column; then click **Locate Switch Ports**.
- To run the process on all switches—Select **Phone Tracking > Run Switch-Port & Phone Update**.

Related Topics

Identify Unlocated Phones
IP Subnet Phones
Cisco Unified OS CLI Commands

Phones Not Located with SMNPv3

Check if the SNMP V3 settings on the **SNMPv3** page match the Cisco Unified Communications Manager settings on the **Serviceability** page. Select **Phone Tracking > SNMP V3 Settings**. For more information, see Set Up SNMPv3.

Check if the **Use SNMP V3 for Discovery** check box is enabled on the **LAN Switch Details** page. Select **Phone Tracking > Cisco Unified Communications Manager** and **Phone Tracking > LAN Switch Details** .

Check if the Unified Communications Manager and switch added in Emergency Responder are SNMP reachable by executing a **SNMP Walk** command. Use the CLI and follow one of these examples:

- `snmpwalk -v3 <CUCM IP Address> -u <USERNAME> -l AuthPriv -a <AUTH PROTOCOL> -A <AUTH PASSWORD> -x <PRIVACY PROTOCOL> -X <PRIVACY PWD> 1.3.6.1.4.1.9.9.156.1.1.2.1.7`
- `snmpwalk -v3 <CUCM IP Address> -u <USERNAME> -l AuthNoPriv -a <AUTH PROTOCOL> -A <AUTH PASSWORD> 1.3.6.1.4.1.9.9.156.1.1.2.1.7`
- `snmpwalk -v3 <CUCM IP Address> -u <USERNAME> -lNoAuthNoPriv 1.3.6.1.4.1.9.9.156.1.1.2.1.7`
- `snmpwalk -v3 <SWITCH IP Address> -u <USERNAME> -lAuthPriv-a <AUTH PROTOCOL> -A <AUTH PASSWORD> -x <PRIVACY PROTOCOL> -X <PRIVACY PWD> 1.3.6.1.4.1.9.9.23.1.2.1.1.3`
- `snmpwalk -v3 <SWITCH IP Address> -u <USERNAME> -lAuthNoPriv-a <AUTH PROTOCOL> -A <AUTH PASSWORD> 1.3.6.1.4.1.9.9.23.1.2.1.1.3`
- `snmpwalk -v3 <SWITCH IP Address> -u <USERNAME> -lNoAuthNoPriv1.3.6.1.4.1.9.9.23.1.2.1.1.3`

If you notice a SNMPReqTimeOut or SNMP Unreachable issue in the event logs or the phone tracking logs, then increase the Timeout and Maximum Retry Attempts value under **Phone Tracking > SNMP V3 Settings** page and run a Major Discovery.

If the issue continues, then try the following:

1. Log in to Cisco Emergency Responder from CLI and enter the **command utils network capture eth0 file** <"filename"> **count 10000 size ALL port 161**.
2. Navigate to **Phone Tracking > Run Switch-Port & Phone Update** and run a Major Discovery.
3. When the Major Discovery is completed, stop the CLI command by pressing **CTRL-C**.
4. Download the packet capture file. The packet capture files will be stored in `activelog platform/cli/` location on the server. You can transfer the files through CLI to an SFTP server using the command **file get activelog platform/cli/packets.cap**. Alternatively to collect all .cap files stored on the server, use 'file get activelog platform/cli/*.cap'. See the Command Reference guide for more information.

   Open it and examine the file for the error codes; take the appropriate actions, if needed.

Table 1: Common Error Messages

SL No	Error message	Occurrence
1	usmStatsUnsupportedSecurityLevel (.1.3.6.1.6.3.15.1.1.1.0)	This is set when the security level (AuthPrivAuthNoPriv/NoAuthNoPriv) specified is not supported by the agent. This error is reported by the agent with its first varbind containing the OID .1.3.6.1.6.3.15.1.1.1.0".

SL No	Error message	Occurrence
2	usmStatsNotInTimeWindows (.1.3.6.1.6.3.15.1.1.2.0)	This is set when the engineTime specified is not within the timeWindow of agent. The engineTime is considered not within the timeWindow if any of the following is true: • If the agent's snmpEngineBoots value is equal to 2147483647. • If the request's snmpEngineBoots value differs from that of the agent. • If the difference between the SNMP request's snmpEngineTime and that of the agent is greater than 150.
3	usmStatsUnknownUserNames (.1.3.6.1.6.3.15.1.1.3.0)	This is set when the user name specified is not present in the agent. This error is reported by the agent with its first varbind containing the OID .1.3.6.1.6.3.15.1.1.3.0.
4	usmStatsWrongDigests (.1.3.6.1.6.3.15.1.1.5.0)	This is set when the password specified is not correct. So check if both Auth and Priv passwords are correct if configured. This error is reported by the agent with its first varbind containing the OID .1.3.6.1.6.3.15.1.1.5.0.
5	usmStatsDecryptionErrors (.1.3.6.1.6.3.15.1.1.6.0)	This is set when the packet is unable to decrypt on the agent side. This error occurs while querying an AuthPriv user. So check if the Auth and Priv Protocol specified are correct. This error is reported by the agent with it's first varbind containing the OID .1.3.6.1.6.3.15.1.1.6.0".

IP Subnet Marked as Non-trackable

The IP Subnet Phones page appears when you choose **ERL Membership> IP Subnets**. The Tracked column shows if the phones under the IP subnet are tracked or not. For IP subnets configured as non-trackable, the View Phones icon will show all phones that are not tracked.

- If a phone falls under both a tracked and non-tracked IP subnets, precedence is given to the more specific IP subnet.
- The phones under the IP subnet marked as non-trackable are not displayed on **Switch Ports** or **Unlocated Phones** page.
- If a phone moves between a trackable and non-trackable IP subnet, you must perform a Major Discovery to reflect the changes.
- Cisco Emergency Responder does not restrict a 911 call flow for the phones that are under a non-trackable IP subnet. If a call is made, the default ERL treatment is provided.

Phone Disappears in Emergency Responder

If Emergency Responder is in the middle of a phone tracking process, and a phone is in the middle of homing to a different Unified CM cluster, no Unified CM cluster has a record of the phone. Thus, Emergency Responder does not know the phone exists, and you cannot look up the phone in the Emergency Responder interface. However, assuming the phone successfully connects to a Unified CM cluster, Emergency Responder tracks the phone during the next incremental phone tracking process, and the phone should then appear in the Emergency Responder interface.

This problem can also occur if phones are reconnecting to a primary Unified CM server from a backup server during the Emergency Responder phone tracking process.

Wrong ERL Used for Shared Line

When two or more phones with a shared line appearance move from switches that are monitored by one Emergency Responder group to switches that are monitored by a different Emergency Responder group, then Emergency Responder may assign an incorrect ERL to these phones during an emergency call. This situation can occur when the phones move to a different campus that has a different Unified CM cluster (although the moved phones are still registered with the original Unified CM cluster), and it can also occur when the phones move within a single large campus that is served by multiple Unified CM clusters.

Because the moved phones are still registered to their original Unified CM cluster, emergency calls from these phones are routed to the original Emergency Responder group. In this case, the Emergency Responder group detects that the calling phone is connected to a switch that is monitored by a different Emergency Responder group, and the call is forwarded to the appropriate Emergency Responder group through an H.323 inter-cluster trunk. Because the inter-cluster trunk does not pass the MAC address of the calling phone, the receiving Emergency Responder group does not know the MAC address of the calling phone and must associate the phone to an ERL based on the calling party number.

In cases with a single phone connected to the switches monitored by the receiving Emergency Responder group, this is not a problem. However, when multiple phones with a shared line appearance connect to switches monitored by the receiving Emergency Responder group, then Emergency Responder must guess which phone has placed the emergency call. If all of the phones with a shared line appearance are in the same ERL, the guess is correct. If the phones span multiple ERLs, then the guess might be incorrect.

Related Topics

Two Main Site Deployments

Wireless Endpoints Using Unexpected ERL

Wireless endpoints (such as CiscoWirelessIP7920Phones and CiscoIPSoftPhones) may be using switch port-based ERL instead of the configured subnet-based ERL.

CiscoEmergency Responder (Emergency Responder) give a higher priority to switch port association for call routing. If Emergency Responder finds a switch port mapping for any endpoint (including wireless endpoints), it uses the switch port mapping to route emergency calls. If the switch port mapping is not found or if the ERL is not configured for the corresponding switch port, Emergency Responder routes emergency calls using subnet-ERL configuration.

See the switch port screen or the ERL debug tool (see Check Emergency Responder Configuration Using ERL Debug Tool , on page 21) to check if the wireless endpoint is associated with a switch port.

It is recommended that you track wireless endpoints using subnet-based ERLs.

Related Topics

Set Up IP Subnet-based ERLs

Troubleshoot Emergency Call Problems

The following sections describe how to troubleshoot emergency calls routing and how to use the information supplied with the calls.

Emergency Calls Not Intercepted by Emergency Responder

If Emergency Responder is not intercepting emergency calls, there is probably a mistake in your Unified CM configuration or its representation in the Emergency Responder configuration.

- The emergency call number (911) is in the Phones partition and uses the E911CSS calling search space. Ensure that this number was identified during Emergency Responder installation (see Installation on a New System) to ensure that users can dial the emergency number. See Create Emergency Call Route Points for information about setting up the Unified CM configuration for this number.
- The standby Emergency Responder server route point (912) is in the E911 partition and uses the E911CSS calling search space. See Create Emergency Call Route Points for information about setting up the Unified CM configuration for this number. Ensure this number is defined as the standby server route point in the Emergency Responder configuration (see Set Up Group Telephony Settings for Server).
- The PSAP callback route point pattern (913XXXXXXXXXX) is in the E911 partition and uses the E911CSS calling search space. See Create Emergency Call Route Points for information about setting up the Unified CM configuration for this number. Ensure this number is defined as the PSAP callback route point pattern in the Emergency Responder configuration, and that the strip prefix (913) is also identified (see Set Up Group Telephony Settings for Server).
- All ELIN route patterns are in the E911 partition. See Create Route Patterns for ERLs for information about setting up the Unified CM configuration for these numbers.
- All phones and CTI ports (both device and line) are in the Phones partition and use the PhoneCSS calling search space. You can use additional partitions, but they must be set up with relationship to the Emergency Responder partitions and calling search spaces in the same manner as these partitions in the examples described in the Create Route Patterns for ERLs.
- All gateways to the service provider's network use the E911CSS calling search space. See Set Up Calling Search Space for Gateway and PSAP Connection for more information.
- The Unified CM Version (JTAPI jar) being configured is proper. To check the Unified CM version, follow these steps:

1. Log in to the Emergency Responder Admin Utility website.
2. Select **Update > CCM Version**
3. In the **Status** section, check the **Current Version of CCM**.

ELIN Not Transmitted to PSAP

If the ELIN is not transmitted to the PSAP, and you are using a PRI connection to route emergency calls to the PSAP, check the configuration of the gateway. The PRI must be configured to send the real calling party number (the ELIN) rather than a static number, such as the main site number. See CAMA and PRI Trunks.

ELIN Default ERL Used for Calls From Other ERLs

If an emergency call is assigned an ELIN defined for the default ERL instead of an ELIN assigned to the ERL from where the call was made:

- Check the Unified CM configuration for the route pattern for the ELIN you expected to be used. See Create Route Patterns for ERLs.
- Check the ERL definition in Emergency Responder to ensure that the ELIN is correctly configured for the ERL. See Set Up Individual ERL and Automatic Location Information (ALI).

If the route pattern for an ERL fails, Emergency Responder uses the route pattern defined for the default ERL.

Emergency Calls Not Routed to Correct PSAP

If an emergency call is not routed to any PSAP, check whether the route patterns used for the ERL from which the call was made and for the default ERL are configured and use the correct partitions and calling search spaces (see Create Route Patterns for ERLs). Ensure that the partitions and calling search spaces for the gateways are correct (see Set Up Calling Search Space for Gateway and PSAP Connection).

Note When a 911 call is made, the call does not route to an alternate PSAP when the primary PSAP call fails. The caller may hear a busy tone, but the Emergency Responder administrator will not receive an email alert that the emergency call could not be routed.

If an emergency call successfully leaves your network but does not get routed to the correct PSAP, look at these possible points of failure:

- Is Emergency Responder configured to assign the correct ELIN to the ERL assigned to the phone? Emergency calls are routed based on the ELIN, so if you assign the wrong ELIN, the call is not routed correctly. See ERL Creation.
- No Calling Party Transformation masks are set at the Gateway or Trunk, which may transform the ELIN set by Emergency Responder.
- If the ELIN is correct, is the ELIN route pattern configured to use the correct gateway? If you select the wrong gateway, the call might be routed to a part of the service provider's network that cannot connect to the desired PSAP. Consult with your service provider to determine gateway requirements.

See these topics:

- ELIN Numbers Emergency Calls and PSAP Callbacks
- Deployment in Main Site with Two or More PSAPs

- Does the service provider's ALI database contain the correct information for the ELIN? Emergency call routing outside your network is based on the information in the service provider's database, not on the information in your local network. See Export ERL Information.
- Does the emergency caller's phone register with a Unified CM cluster supported by a different Emergency Responder group than the Emergency Responder group that supports the originating switch port? Then you might have a mis-configured Emergency Responder cluster. See these topics:
  - Installation on a new system
  - Create route patterns for Inter-Cisco Emergency Responder Group communications
  - Set up group telephony settings for server

Note If the call reaches the PSAP, but the PSAP cannot talk to the caller, ensure that the Unified CM for the remote Emergency Responder group has the Unified CM for the local Emergency Responder group defined as a gateway.

Emergency Calls Get Busy Signal and Not Routed

If callers hear a busy signal when calling the emergency call number, or if emergency calls sometimes do not get routed, there is probably a problem with the configuration of your standby Emergency Responder server:

- If you have only configured a primary Emergency Responder server, install and configure a standby Emergency Responder server. If CPU utilization on the primary server reaches 100 percent, Emergency Responder cannot handle emergency calls. In this case, the standby server handles the calls.
- Check the route point configuration for the standby server. Ensure the emergency call route point's call forward settings are configured to forward calls to this number. See Create Emergency Call Route Points for information about the Unified CM configuration, and the Set Up Group Telephony Settings for Server for the Emergency Responder configuration.

PSAP Call Back Errors

You might encounter a PSAP call back error if a PSAP operator tries to call back an emergency caller using the ELIN provided by caller ID. The following sections describe two such errors: if a PSAP cannot reach the original emergency call extension and if onsite security personnel get a call back from a PSAP.

PSAP Cannot Reach Original Emergency Call Extension

Problem PSAP could not reach the original emergency call extension.

Solution Emergency Responder caches a mapping between the caller's true extension and the ELIN you define for an ERL. If more calls get made than the number of ELINs you define for an ERL, Emergency Responder

must reuse these numbers and thus overwrites the original caller's extension. You can view the call history to determine the extension of the original caller. See Emergency Call Process.

If this is not the problem, check the configuration of the PSAP callback route point in Unified CM and Emergency Responder (see Create Emergency Call Route Points and Set Up Group Telephony Settings for Server), and ELIN translation patterns in Unified CM (see Create Translation Patterns for ELINs).

Onsite Alert Security Personnel Get Callbacks From PSAP

Problem Onsite alert (security) personnel get callbacks from the PSAP.

Solution Please check if Default ELIN Digit Translation is set in the Group Telephony Settings for Server. For more information, see Set Up Group Telephony Settings for Server.

Onsite Alert Personnel Not Getting Telephone Alerts

If the onsite alert personnel are not getting telephone alerts when an emergency call is made in an ERL they are covering, ensure that all phones and CTI ports (both device and line) are in the Phones partition and use the PhoneCSS calling search space. You can use additional partitions, but they must be set up with relationship to the Emergency Responder partitions and calling search spaces.

Also, ensure that the Emergency Responder configuration for the Unified CM clusters is correct. The Emergency Responder configuration should show the correct beginning address for the telephony ports that you defined as CTI ports in Unified CM. The number of telephony ports should be the correct number, and the number must be greater than 0 for any calls to occur. Emergency Responder uses this CTI port to place the telephone calls to onsite alert personnel.

If the Event Viewer in the Emergency Responder Serviceability web interface displays the error message “No port to place call,” then there were not enough CTI ports defined to initiate all the calls to onsite alert personnel. Therefore, you must define additional ports. To access the Event Viewer, log in to the Emergency Responder Serviceability web interface and select **Tools > Event Viewer**.

Onsite Alert Phone Does Not Ring When Emergency Call Placed

You might encounter this problem if the onsite alert phone does not ring when an emergency call is placed.

Problem The onsite alert phone does not ring when an emergency call is placed.

> **Possible Cause** The onsite alert phone does not ring if the Do Not Disturb (DND) feature is enabled on the phone and if Emergency Responder is configured with Unified CM6.x.

Solution Do not enable DND on an onsite alert phone.

You might encounter this problem if the onsite alert does not work during an emergency call, when the Cisco Emergency Responder publisher database is not operational.

Problem The onsite alert does not work for an emergency call if the Cisco Emergency Responder publisher database is not operational.

> **Possible Cause** The onsite alert will not work as the Cisco Emergency Responder publisher is still active even when the database is not operational and the Cisco Unified Communications Manager CTI ports get registered with the Cisco Emergency Responder publisher.

Solution Restart the Cisco Emergency Responder publisher.

Prompts for Phone Alerts Not Getting Played

You might encounter this problem if prompts for phone alerts are not getting played.

Problem Prompts do not get played at the onsite alert phone when the call is initiated from the CTI ports.

Possible Cause This problem can occur when a single CTI port is configured with multiple lines. Prompts may not get played from one or more of these lines when the onsite alert notifications call is initiated through them.

Solution To avoid this problem, configure only one line per CTI port in the Unified CM that is configured for Emergency Responder.

Onsite Alert Personnel Not Getting Email or Paging Notifications

If the onsite alert personnel are not getting email or email-based pages, even though you configure email addresses for them, check the Emergency Responder configurations SMTP settings. Ensure that the SMTP server address and source mail ID are correct, and that there is an account for the mail ID in the SMTP server.

Incorrect Location Information Sent to Onsite Alert Personnel

If your onsite alert (security) personnel are receiving incorrect location information for an emergency call, consider these potential problems:

- Is the ALI data for the ERL correct? See ERL Creation.
- Is the phone location data for the switch port correct? See Switch Port Configuration.
- Is the correct ERL assigned to the switch port to which the phone is connected? If not, there could be two problems:
  - Someone switched wires on the switch, so your previously correct configuration is no longer correct. Wires cannot be moved from port to port without potentially invalidating the ERL assignment. See Data Integrity and Reliability.
  - The wiring closet is secure, but the ERL assignment is incorrect. See Switch Port Configuration.
- Did the call come from the Default ERL (assuming you do not use the Default ERL for any permanent ERL)? This could indicate these problems:
  - The phone is connected to an unsupported port and is not defined as a manual phone. See Manually Define Phones.
  - The phone is not supported and it is not defined as a manual phone. See Manually Define Phones.
  - The phone is supported but Emergency Responder could not locate it. You might have to manually assign the phone to an ERL if you cannot resolve the problem. See Unlocated Phones , on page 2.
- Did the call come from a manually-defined phone extension? If so, it is likely the incorrect ERL is assigned, perhaps because the phone moved. See Manually Define Phones.

Emergency Call History Problems

There are two issues you might encounter when viewing the emergency call history information:

- Emergency call information does not appear in call history.
- Call history does not show call ELIN and route pattern.

For additional information, see View Emergency Call History.

Emergency Call Information Does Not Appear in Call History

Problem Emergency call information does not show up in call history right away.

Solution Emergency Responder writes call history information to the database every 15 seconds. You can view history information after 15 seconds.

Call History Does Not Show Call ELIN and Route Pattern

Problem The call history does not show the ELIN and route pattern used for a call.

Solution If the call could not be routed to the PSAP, you will not see an ELIN or route pattern. Check to determine why the call could not be routed. See Emergency Calls Not Routed to Correct PSAP , on page 8.

Troubleshoot Licensing

Cisco Smart Software Licensing is a new way of thinking about licensing. It adds flexibility to your licensing and simplifies it across the enterprise. It also delivers visibility into your license ownership and consumption.

Cisco Smart Software Licensing helps you to procure, deploy, and manage licenses easily where devices self-register and report license consumption, removing the need for product activation keys (PAK). It pools license entitlements in a single account and allow you to move licenses freely through the network, wherever you need them. It is enabled across Cisco products and managed by a direct cloud-based or mediated deployment model.

This service registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Cisco Smart Software Manager replaces Prime License Manager in Cisco Emergency Responder Release 12.0 and later versions.

Related Topics

E911 and Cisco Emergency Responder Terminology
Cisco Smart Software Licensing

License Manager Status Messages

The following table shows a list of all status messages as they appear on the **License Manager** page.

Table 2: Status Messages on the Landing Page

Device	State	Status or Warning Message	Description
Emergency Responder	Evaluation mode	Cisco Emergency Responder (CER) is currently unregistered with Smart Software Manager and running in Evaluation mode with 90 days remaining. Register with Smart Software Manager or Smart Software Manager satellite to avoid stopping of Cisco Phone Tracking Engine.	This message is displayed on Emergency Responder during the Evaluation Period.
Emergency Responder	Evaluation period expired	The system has passed the Evaluation Period. The Cisco Phone Tracking Engine has been stopped. Register with Smart Software Manager or Smart Software Manager satellite to restart the Cisco Phone Tracking Engine.	This message is displayed on Emergency Responder when the Evaluation Period expires.

Troubleshoot Email Alerts

The following sections describe how you troubleshoot problems related to the email alerts generated by Emergency Responder.

JTAPI Incompatibility Warning

As an administrator, you will be alerted if the Unified CM version configured on Emergency Responder differs from the version to which Emergency Responder route points are registered, so that you can take corrective action and assure that emergency calls are processed correctly. An email alert will be sent to the configured email address using SMTP mail server.

Ensure that email alerts for Emergency Call Routing Parameters are enabled under Email Alert Settings on the Emergency Responder administration pages.

The error is also displayed on the Event Viewer page. See the Related Links below.

Alert would be as follows:

```
Unified CM at <IP address> is version CUCM x which differs from CUCM version
setting CUCM y on Cisco Emergency Responder.
```

This warning could occur in the following cases:

- Unified CM version is no longer supported; for example, Unified CM 2.0 integrated with Cisco Emergency Responder 8.7 or 9.0
- Unified CM version is not yet supported; for example, Unified CM 9.5 integrated with Cisco Emergency Responder 8.7 or 9.0
- Unified CM version is supported, but Unified CM version setting on Emergency Responder is incorrect; for example, Unified CM 9.0 integrated with Cisco Emergency Responder 8.7 or 9.0, but Emergency Responder Unified CM version setting is Unified CM 7.1

Multiple Unified CM versions in the same Emergency Responder will always cause one of the above situations.

Related Topics

Event Viewer

JTAPI Route Point Registration Failure Alarm

As an administrator, you will be alerted if Emergency Responder cannot register its JTAPI route points so that you can take corrective action and assure that emergency calls are processed correctly.

The following events can cause the route point to register or unregister:

- Cisco Emergency Responder or SNMP service restart.
- Cisco Emergency Responder failover or fallback.
- JTAPI version upgrade or downgrade.
- Incompatible JTAPI version.
- Emergency Responder or Unified CM upgrade.
- Application user's credential is incorrectly mentioned in Emergency Responder.
- Application user password expired.
- CTI telephony port begin number is wrongly mentioned in Emergency Responder (impacts only CTI ports).
- CTI telephony port count is wrongly mentioned in Emergency Responder (impacts only CTI ports).
- SNMP configuration is incorrect in either Emergency Responder or Unified CM.
- Route point DN numbers mismatch in Cisco Emergency Responder or Unified CM.

If Unified CM is SNMP unreachable or application user credentials to Unified CM are incorrect, then Emergency Responder will send an email alert to the configured email ID. Ensure that the email alert settings under the discovery parameters are enabled under Email Alert Settings on the Emergency Responder administration pages.

The email alert would be as follows:

<CERserver hostname> Cisco ER Phone Tracking could not get information [using SNMP] from 1 Cisco CallManager(s) Check EventViewer on CERServer for details.

This is a serious condition and may indicate that Emergency Responder will not receive and process emergency calls.

Emergency Call Alert

Whenever a user makes a 911(Emergency) call, Emergency Responder generates an email alert. Emergency Responder sends the email alert to all the onsite alert (security) personnel whose email IDs are configured for the ERL from which the call was made.

Security personnel are expected to respond to that user. For detailed call information, see the following URL:

`http://<<CERServer HostName>>/ceruserreports`

When a 911 call is made and the backup Emergency Responder server handles the call, an alert similar to the following is sent:

```
Subject: Emergency Call Alert -- Extn # 332101 (Generated by Backup CiscoER)
Message: EMERGENCY CALL DETAILS (Generated by Emergency Responder)
Caller Extension : 332101
Display Name     : Caller's Name
Zone/ERL         : Z1
Location         : ddd
System Call Time : March 13, 2018 11:07:54 AM IST
Local Call Time  : March 12, 2018 22:37:54 PM PDT (Note: In this example, Local Call Time
is for the America/Los_Angeles time zone.)
```

Transition Alert

When the standby Emergency Responder server takes control and becomes the active server, a Transition Alert is sent to the Emergency Responder administrator. This situation occurs under any of the following circumstances:

- If the primary Emergency Responder server is stopped.
- If the Emergency Responder service is stopped on that server.
- If the connectivity between primary and standby Emergency Responder servers is broken.

The administrator should diagnose the cause and fix the problem as soon as possible.

When the Emergency Responder backup server takes control, an alert similar to the following is sent:

```
Subject: Transition Alert: Cisco ER Backup is activeMessage:
Backup Cisco ER <<CER HostName>> has taken control as Active Cisco ER.
Transition Time  :June 2, 2003 3:57:12 PM IST
```

When the master Emergency Responder server takes control, an alert similar to the following is sent:

```
Subject: Transition Alert: Cisco ER Master is activeMessage:
Master Cisco ER <<Emergency Responder Server HostName>> has taken control
as Active Cisco ER. Transition Time  :June 2, 2003 3:57:12 PM IST
```

Tracking Failure

At the end of a switch port and phone tracking process, if there are any devices that could not be tracked, Emergency Responder sends a Tracking Failure email to the Emergency Responder administrator.

The administrator should look at the event log on the Emergency Responder server to find the list of devices that were not tracked. The administrator should check the following and make any required corrections:

1. Make sure that the correct SNMP Community String is configured in Emergency Responder.
2. Check that the device is connected.
3. Check that the host name for the Emergency Responder server is resolvable, that is, it can be found.
4. Check that the SNMP service is enabled on that particular device (Switch / Unified CM).

Here is an example of a tracking failure alert:

```
Subject: CER Phone Tracking failed to track some devicesMessage:
CER Phone Tracking could not get information [using SNMP] from 2
CiscoUnified CM(s) and 1 Switch(es)Check Event Viewer
on CER Server for details.
```

Failed to Get Provider Alert

Emergency Responder sends a Failed to Get Provider alert to the Emergency Responder administrator if Emergency Responder is not able to register to one of the configured Unified CM clusters. Emergency Responder continues trying the registration until it succeeds. Emergency Responder sends the Failed to Get Provider email after a few retries.

The message provides information about how to clear the problem, as shown in the following example:

```
Subject: Failed to get JTAPI Provider for Cisco Unified CM <<CCM IP/Host Name>>
(Generated by Backup Cisco ER)Message:
Please check the following:
1) Check if the Cisco Unified CM is connected to the CER server.
2) Check if the configured Call Manager is running a version
supported by the CER server.
3) Check if the given login credentials are correct:
CTI Manager Host Name:<<CCM IP/HostName>>
```

Failed to Establish Communication with Emergency Responder Phone Tracking Engine

Emergency Responder sends this email alert to the Emergency Responder administrator if the Emergency Responder server fails to establish communication with the Phone Tracking Engine for a period of time. This failure to communicate can occur if the Emergency Responder Phone Tracking Engine service is down. The administrator should perform the following steps:

1. If the Emergency Responder Phone Tracking Engine service is down, start the service.
2. Make sure that the Host Name of the Emergency Responder server does not contain any underscore (_) characters.

Here is an example of a tracking failure alert:

```
Subject: CER Server failed to establish communication
with CER Phone Tracking Engine.Message:
CER Server could not communicate with CER Phone Tracking Engine.
```

Lost Communication with Emergency Responder Phone Tracking Engine

Emergency Responder sends this email alert to the Emergency Responder administrator if the Emergency Responder server loses communication with the Emergency Responder Phone Tracking Engine. This situation is likely to occur if the Emergency Responder Phone Tracking Engine service goes down when the Emergency Responder server is running.

The administrator should restart the Emergency Responder Phone Tracking Engine service.

The following shows an example of a tracking failure alert:

```
Subject: CER Server lost communication with CER Phone Tracking EngineMessage:
CER Server could not communicate with CER Phone Tracking Engine.
```

Failed to Send Unlocated Phone Details to Remote Emergency Responder Server Group

If Emergency Responder fails to send unlocated entries to a server group because it is already in the process of sending entries to that server group, this alert is sent.

This alert occurs very rarely. It can occur when a Emergency Responder server is found in more than one Emergency Responder server group. To resolve this problem, check to see which server group is an old configuration and remove that server group.

```
Subject: CER Server failed to send Unlocated Phones details
to Remote CER Server Group.Message:
CER Server failed to send Unlocated Phones to Remote CER Server Group.
Please ensure that the CER servers are not found under more than one CER Server
Group.
CER Servers in Remote Server Group:<< CERServer HostNames >>
```

Emergency Call Could Not Be Routed

If the emergency call routing to some route patterns configured in the ERL fails, Emergency Responder sends an email to the system administrator.

Subject: Emergency call could not be routed using some route patterns (CERServer:<server hostname>)

Message Body: Emergency call from :<Caller Extn> could not be routed using some Route Patterns. Check Event Log.

The Event Log displays the following message:

```
Emergency call from <extn> could not be routed using the following route patterns
<RoutePattern1>
<RoutePattern2>
*****************
Call Routed to <RoutePattern-X>

Please check the availability of the above routes. Also, check for the following
 error conditions:
```

```
1. If FAC and/or CMC are configured on the route patterns used for Cisco ER,
please disable them.
2. If the "Calling Party Number Modification" flag on the CER user page in
the Cisco Unified CM is not enabled, please enable it.
```

Solution

- If you are running Unified CM 4.2 or4.3, make sure that the Calling Party Number check box on the Emergency Responder User page is checked.
- If you are running Unified CM 5.x or Unified CM 6.x, make sure that the routes are available.
- Add the Emergency Responder Application User to the “Standard CTI Allow Calling Number Modification” user group.

Calling Party Modification Failed

If the calling party modification was not successful, Emergency Responder sends the following email to the system administrator:

Subject: Emergency Calling Party Modification Failed (Emergency ResponderServer: <server>)

Message Body: Emergency call from :<Caller Extn> cannot be routed with calling party modification. Check Event Log.

The Event Log displays the following message:

```
Emergency Call from <Caller Extn> has been routed to default ERL because the
calling party modification failed. Please make sure that the check box "Enable
Calling
Party Number Modification: is checked on the Cisco Unified CM user page for the
CER user. PSAP callbacks MAY NOT work correctly. The CER service will need to
be restarted once the flag is checked on the Cisco Unified CM User page.
```

Solution

Check the box for the “Enable Calling Party Number Modification” in the Emergency Responder user page in Unified CM 4.2 or4.3 Administration. After you enable this flag, restart the Emergency Responder service for the changes to take effect.

Troubleshoot Web Alerts

You might encounter Web Alert Refreshes Every 30 Seconds , on page 18 when receiving web alerts.

Web Alert Refreshes Every 30 Seconds

Problem Web alert continues to refresh every 30 seconds. You can see this problem by checking the status in the browser. The status displays the seconds remaining before refresh if it is in this mode.

Solution Check if there are other web alert screens open on the same client machine. Only one browser from a client machine can operate in the real-time mode. Remove any extra browsers.

Troubleshoot Emergency Responder System and Administration Problems

The following sections describe how you can troubleshoot problems related to the Emergency Responder system and its administration, such as server and web server problems.

Cannot Validate Publisher

If the installation cannot validate the Publisher (Step 5 of the Install Emergency Responder Subscriber), check the following:

1. Verify that the Publisher hostname is correct and that the Publisher is reachable by hostname.
2. Verify that the Publisher and Subscriber servers are running the same version of Emergency Responder.
3. Verify that the database password that you entered is correct. This password was specified on the Database Access Security Configuration page during installation.
4. Make sure that the Subscriber has been configured correctly on the Publisher.

Troubleshoot Login Problems

The following section shows some issues you might encounter while logging into Emergency Responder.

Cannot Access Emergency Responder Administration Website

Problem You cannot log in to the Emergency Responder Administration website.

Solution Log in to CLI and run the **utils service list** command. Check if the status "Cisco IDS" is STARTED. If not, start the service using the **utils service start service name** command.

HTTP Error 500

If the Emergency Responder Administration website displays a HTTP Error 500 after the installation or upgrade, try the following:

- Restart Cisco Emergency Responder and Cisco Tomcat service.
- Run a select query to cerremote table and check if the RMI objects have been created for both Publisher and Subscriber Nodes.
- If you have replication issues between Publisher and Subscriber:
  - Check the .rhosts file of the Publisher and confirm that it was entered with the correct values. If the correct values have not been entered, restart the Cisco Emergency Responder service.
  - Run the **utils dbreplication repair** and **utils dbreplication reset** commands to reset the Database replication.
- If these steps do not fix this issue, set the server to permissive mode using the **utils os secure permissive** command and reboot it.

Cisco Unified Operations Manager

Use Cisco Unified Operations Manager to continuously monitor the health of the Emergency Responder system.

For information about setting up Emergency Responder to use Cisco Unified Operations Manager, see Set Up Test ERLs.

For information about installing and using Cisco Unified Operations Manager, go to this location:

http://www.cisco.com/en/US/partner/products/ps6535/index.html.

Troubleshoot Emergency Responder Switch and Port Configuration Problems

The following sections describe several common issues that you might encounter while configuring switches or switch ports in Emergency Responder.

Phones Do Not Get Discovered

Problem Emergency Responder is configured with Unified CM information, but no phones get discovered.

Solution Ensure that the Unified CM servers are reachable on the network. Then ensure that the SNMP read community strings are configured correctly for the switches and Unified CM servers (see Set Up SNMPv2.) Manually run the switch port and phone update process (see Manually Run the Switch-Port and Phone Update Process.) Use the CLI-based **utils snmp** command to determine if the Unified CM is SNMP reachable.

Emergency Responder Does Not Show Ports on Switch

Problem Emergency Responder does not show the ports on a switch configured in Emergency Responder.

Solution If you add a supported switch to Emergency Responder and run phone tracking on the switch after adding it, you can view the list of Ethernet ports on the switch. If Emergency Responder does not list the ports, check the SNMP settings in Emergency Responder for the switch (see Set Up SNMPv2.) Also, verify that the switch is reachable over the network. Retry the selective phone tracking process on the switch (click **Locate Switch Ports** when viewing the switch details; see LAN Switch Details.)

If the problem persists, ensure that the switch is supported (see Network Hardware and Software Requirements.) Also, check the Event Viewer for error messages.

Some Phones Do Not Appear in Switch Port List

Problem Some phones do not appear in the switch port list.

Solution Check if the phone is found under configured IP subnets or in synthetic phones. If it is not found in either of those places, then they are placed as unlocated phones. See Unlocated Phones , on page 2 for a list of reasons that a phone could not be located.

Cannot Delete Switch From Emergency Responder Configuration

Problem Cannot delete a switch from the Emergency Responder configuration.

Solution You cannot delete a switch when a phone tracking process is in progress. Retry the deletion after the process has ended. If this is not the problem, the Emergency Responder server might not be running. Check the control center and restart the server (see Manage Emergency Responder Server , on page 26.)

Import or Export of Switch Port Details Fails

Problem Import or export of the switch port details fails.

Solution If a switch port import or export attempt fails, it might be due to these reasons: the first switch port and phone update process has not yet ended (wait for it to finish); the Emergency Responder server is not running (use the control center to restart it, see Manage Emergency Responder Server , on page 26); the Emergency Responder server is not completely initialized (wait for it to initialize).

Import of Some Switch Port Configurations Fail

Problem The import of some switch port configurations fail.

Solution To import switch port configurations, Emergency Responder must already be configured with the switch and Emergency Responder must first discover the ports on the switch using the switch port and phone update process. If you try to import a configuration for ports not yet discovered in Emergency Responder, the importation of those settings fails. See Manually Run the Switch-Port and Phone Update Process for information about the process. Run it on the switches whose port configurations you could not import, then retry the import.

Phones Moved To and From Various Emergency Responder Groups Incorrectly Display in Switch Port Details

Problem Phones moved from other Emergency Responder groups to this Emergency Responder group, and then moved back, are still showing up in the switch port details for the Emergency Responder group.

Solution These types of phones are not removed from the switch port details until the next full switch port and phone update process is run. If this is an issue for you, you can run the process on the switch (or on all switches) manually. See Manually Run the Switch-Port and Phone Update Process.

Check Emergency Responder Configuration Using ERL Debug Tool

The ERL Debug Tool takes a phone extension as the search criteria and displays the ERLs currently being used for routing emergency calls for the phones.

Use this diagnostic tool to verify the Emergency Responder configuration during the ERL creation and the ERL assignment phase, and to troubleshoot calls directed to incorrect ERLs.

For example, you configured the phone in ERL_1 as a manually configured phone; however, a mis-configured IP subnet matches this phone's IP address, and associates it with ERL_2. Now that you have found the configuration problem using the Debug Tool, you can correct it.

Procedure

Step 1 Select **Tools > ERL Debug Tool**.

Emergency Responder displays the ERL Debug Tool page.

Step 2 In the Find Phones field, to list specific phones, select the search criteria and click **Find**.

Emergency Responder displays the ERL currently being used for routing emergency calls for the phone.

Step 3 If the configurations are not correct, make the required changes.

Note Emergency Responder displays a maximum of 1,000 records.

Publisher and Subscriber Server Replacement

The following sections describe how to replace a faulty Publisher server and how to replace a faulty Subscriber server.

Replace Faulty Subscriber

To replace a faulty Subscriber, go to Emergency Responder administration and delete the faulty Subscriber. Install a new Emergency Responder Subscriber for the Publisher (see Installation on a New System).

Note If the same host name is not going to be used by the replacement Subscriber server, you must delete the faulty Subscriber using the Emergency Responder administration screen on the Publisher server.

Replace Faulty Publisher

You can restore the Publisher only if you have backed up the Publisher using the Disaster Recovery System available as part of the Emergency Responder.

Procedure

Step 1 Install the same version of the Emergency Responder Publisher on a server with the same host name as the one you used previously.

Step 2 Choose the same configuration options (such as the Unified CM version, and so on) during the installation.

Step 3 Restore the old configuration data using the Disaster Recovery System.

Emergency Responder Admin Utility

You can use the Emergency Responder Admin Utility tool to perform the following tasks:

- To update Emergency Responder cluster database host details
- To upgrade the CCM version

Use Emergency Responder Admin Utility Tool

Procedure

Step 1 Log in to the Emergency Responder Admin Utility web interface.

Step 2 Using the menu bar, choose a task to perform:

a) To change the Publisher that the Subscriber server points to, select **Update > Publisher**.
b) To update the Unified CM version, select **Update > CCM Version**.
c) To update the cluster settings on both the Publisher and Subscriber servers, select **Cluster > DBHost**.

Note This action updates the Emergency Responder cluster DB details for this server group only. Other servers in this Emergency Responder cluster will NOT be updated automatically.

Step 3 To save the changes that you have made, restart both the Publisher and the Subscriber servers.

Set Up Subscriber Database

To configure the Publisher-Subscriber setup again if you have an issue with the Subscriber (apart from DB replication), follow these steps:

Procedure

Step 1 Log in to the Emergency Responder Admin Utility web interface on the Subscriber server.

Step 2 Select **Update > Publisher**.

Step 3 Specify the same Publisher Host Name, IP address (already being pointed to) and database access security password.

Step 4 Click **Go**.

This step might a take a while to set up.

Database and Enterprise Replication Troubleshooting

Use the following CLI commands for troubleshooting the Informix Dynamic Server (IDS) database:

- **utils service list**—Checks whether the IDS service is running or not.
- **show tech dbstateinfo**—Provides the DB state information, which is helpful in debugging database issues.
- **show tech dbinuse**—Displays the currently used database.
- **show tech dbintegrity**—Shows database integrity information.
- **show tech database**—Creates a .csv file with contents of all the tables in the database.

Use the following CLI commands for troubleshooting Enterprise Replication:

- **utils dbreplication status**—Displays the status of the database replication.
- **utils dbreplication reset**—Resets and restarts the database replication between the Publisher and Subscriber.
- **utils dbreplication repair**—Compares the data on replication servers (Publisher and Subscriber) and creates a report listing data inconsistencies and repairs the data inconsistencies. This command also tries to repair replication by rebuilding the corrupted .rhosts file if it is corrupted for some reason.

For troubleshooting database problems using logs, download logs from the Emergency Responder Serviceability website or through the CLI.

The following logs provide information for debugging database-related issues:

- Install and Upgrade logs—/var/log/install/
- Install DB logs—/var/log/active/er/trace/dbl/sdi/
- CERDbMon logs—/var/log/active/er/trace/dbl/sdi/cerdbmon/
- CLI logs—/var/log/active/platform/log/

Replication Fails to Start After Subscriber and DNS Installation

Problem Replication fails to start after the Subscriber is installed with DNS and the CLI command **utils dbreplication status** indicates that replication is not working.

Possible Cause The .rhosts have the host name for the Subscriber instead of FQDN (Fully Qualified Domain Name) of the Subscriber.

Solution Use the CLI command **utils dbreplication repair** to repair the replication issue. This command tries to repair replication by rebuilding the corrupted .rhosts file.

Troubleshoot Emergency Responder System Problems

The following sections discuss some issues you might encounter with general operation of the Emergency Responder system and the configuration screens that involve the Emergency Responder server, group, and cluster.

Emergency Responder Intra-Cluster Call Routing Fails or Phones Not Discovered Correctly

Problem Emergency Responder intra-cluster call routing fails or Emergency Responder does not discover phones correctly.

Solution Ensure that all the Emergency Responder servers in an Emergency Responder cluster can be found by their host name, and ensure that all are reachable on the network by all the other Emergency Responder servers.

Solution Ensure that all the Emergency Responder servers can reach the Emergency Responder cluster DB host and that the cluster DB password is the same across all servers in the cluster.

Emergency Responder Exits After Starting

Problem Emergency Responder exits after starting.

Possible Cause

You have configured Emergency Responder to use a TCP port that is already in use.

Solution Check the Windows Event Viewer for the message "CER could not open socket at port peer-tcp-port, Exiting." If you see this message, change the Emergency Responder group configuration to use a different TCP port.

Emergency Responder Groups in Cluster Screen Does Not Load and Displays a Cannot Connect to Cluster DB Host Error

Problem The Emergency Responder Groups in Cluster screen does not load, and exhibits the error “Cannot connect to cluster DB host.”

Solution Ensure that the cluster DB host can be found by host name.

Ensure that the specified cluster DB host password is the same across all Emergency Responder server groups in the cluster.

For more information, see Set Up Emergency Responder Cluster and Cluster DB Host.

Related Topics

Identify Emergency Responder Groups and Servers in Cluster , on page 26
Manage Emergency Responder Server , on page 26
Event Messages , on page 32
Performance Management , on page 32
Data Backup and Recovery

Troubleshoot Cisco Unified Communications Manager Configuration Problems

These are some issues that you might encounter when the Emergency Responder communicates with Unified CM. Additional problems with symptoms that involve emergency call failures are discussed in the Troubleshoot Emergency Call Problems , on page 7.

Emergency Responder Does Not Register with Route Points and CTI Ports

Problem Emergency Responder does not register with the route points and CTI ports configured for its use.

Solution Ensure that the route points and CTI ports are associated with the Unified CM CiscoEmergency Responder user (see Create Emergency Responder Cisco Unified Communications Manager User.) Ensure that the CTI Manager on the Unified CM server (or the DC Directory on a Windows-based Unified CM server) is running properly.

Cannot Delete Unified CM From Emergency Responder Configuration

Problem When trying to delete a Unified CM from the CiscoEmergency Responder configuration, Emergency Responder displays the message “Phone tracking in progress.”

Solution You cannot delete a Unified CM server from the Emergency Responder configuration while a phone tracking process is in progress. Retry the deletion after the process has ended.

Updating Cisco EmergencyResponder After You Add Devices

You must create a Unified CM user for Emergency Responder use and CTI ports and route points that must be assigned to the user before Emergency Responder tries to create a provider with the Emergency Responder cluster. Emergency Responder only registers the CTI ports and route points that are associated with the user when the provider is created. Any devices that you add to the user after starting Emergency Responder is not registered by Emergency Responder.

If you add devices to the Emergency Responder user in Unified CM, you can force Emergency Responder to recreate the provider using any of these techniques:

- Restart the Emergency Responder server.
- Delete the Unified CM server from the Emergency Responder configuration and reenter it.
- Change the backup CTI Manager setting for the Unified CM server in the Emergency Responder configuration and click **Update** to force Emergency Responder to log off the provider and to recreate it.
- Change the name of the user in Unified CM, or create a new user, and associate all devices with it. Then update the Emergency Responder configuration to use the new user.

Phone Moves Between Clusters

For additional information, see Track Phone Movement Across a Cluster.

Identify Emergency Responder Groups and Servers in Cluster

If you are connected to the administrator interface on a Emergency Responder server, you can view the details of the server and the Emergency Responder group's standby server by selecting **System > CiscoER Group Settings**.

You can also identify the Emergency Responder groups and their Emergency Responder servers that are in the same Emergency Responder cluster. To view the other Emergency Responder groups in the cluster, select **System > CiscoER Groups in Cluster**. From the Emergency Responder Groups in Cluster page, select the group that you want to view; and Emergency Responder displays the Emergency Responder servers that are in the group. To view the details for these servers, you must log into the Emergency Responder Administration interface running on one of the servers, select **System > CiscoER Groups in Cluster**, then select the group that you want to view from the list of groups.

If you must uninstall a Emergency Responder group, first delete the group from the Emergency Responder cluster using this page. You must log in as a system administrator to delete the group. Deleting the group from the cluster only removes the entries for the group from the Emergency Responder Cluster DB; it does not remove Emergency Responder from the group's servers.

Related Topics

Server Groups in Cluster

Manage Emergency Responder Server

When you install Emergency Responder, the Emergency Responder server is set up to automatically start whenever the computer is powered up or rebooted. However, you can stop and then restart an Emergency

Responder server through the Emergency Responder Serviceability web interface without powering down or rebooting the computer.

Procedure

Step 1 Log in to the Emergency Responder Serviceability web interface and select **Tools > Control Center**. The Control Center Services page displays, showing all Emergency Responder services and the current status of each one.

Step 2 Click the radio button to the left of the service name, then click **Start**, **Stop**, or **Restart** to perform the desired action on the service. Click **Refresh** to refresh the screen with updated information.

Note The buttons only appear if the action is possible; for example, **Start** only appears if the service is currently stopped.

Note The Cisco Tomcat and Cisco IDS services cannot be started or stopped from the Control Center. These services can only be started or stopped using the **utils service** command.

The following table explains the meaning of the icons that you see on the Control Center Services page.

Table 3: Cisco Emergency Responder Control Center Icons

Icon	Meaning
	The Emergency Responder server or the Emergency Responder Phone Tracking Engine is started and functioning normally.
	The Emergency Responder server Emergency Responder Phone Tracking Engine was stopped by the administrator.

Related Topics

Control Center

Troubleshoot 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.

Emergency Responder 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 can provide you with a list of errors, or you can 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 need to manually edit the records in error.

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

Fix ALI Data Records

To correct data errors that you might receive when uploading ALI records to your service provider, follow these steps.

Before you begin

Obtain NENA Doc 02-010, refer the appropriate Exhibit for NENA version for the Recommended Formats and Protocols for Data Exchange, from NENA or your service provider. Service Provider may have additional requirements.

Procedure

Step 1 Check the error reports to determine the problems you encountered.

Step 2 In the Emergency Responder web interface, change the fields that were in error for the ERL or 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 3 Export the ALI data again (see the online help).

Step 4 If any of the records in error were new, you must change the database function for the records. Because Emergency Responder has already exported these records, Emergency Responder labels them as updates instead of new insertions. However, because these records failed on upload, the service provider's database views 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:

- NENA 2.0 and 2.1 File Formats , on page 28
- NENA 3.0 File Formats , on page 29

Step 5 Submit the edited file to your service provider.

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 (Exhibit 5.5 for Version 2.0 and Exhibit 5.9 for Version 2.1), 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.

The following table describes the fields you are most likely to edit. You should use the Emergency Responder web interface to change the other fields.

Table 4: 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. Emergency Responder only generates a deletion record once, in the export file created after you deleted the ALI from the Emergency Responder configuration. If you must regenerate the record, cut and paste it from the previous export file (and adjust the record count), or recreate the ALI in Emergency Responder, 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 or 2.) 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 or 2.) The number is right-aligned with leading spaces.

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 included with a non-blank value, the value of the element is changed to the new value.

- Tags are separated by a verticalbar(|).
- End of record is indicated by a predefined character.

Use NENA Doc 02-010 (Exhibit 5.13 for Version 3.1), 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.

The following table describes the fields that you are most likely to edit. You should use the Emergency Responder web interface to change the other fields.

Table 5: 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). Emergency Responder only generates a deletion record once, in the export file created after you deleted the ALI from the Emergency Responder configuration. If you must regenerate the record, cut the version number and paste it from the previous export file (and adjust the record count); or recreate the ALI in Emergency Responder, 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 or CYC2.) 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 that you are submitting to the service provider (for example REC1 or REC2.)

Call History Logs

Emergency Responder maintains extensive call history logs, which include entries for each emergency call handled. You can view call history information from the administration and user interfaces.

Emergency Responder maintains in its database a history of the emergency calls that have been placed. When the primary Emergency Responder server (Publisher) is not active, emergency calls are handled by the backup Emergency Responder server (Subscriber). Through replication, the call history records on both these servers are synchronized when they are active. For this reason, the call history can be viewed on either of the Emergency Responder servers.

To download these records, click the **Download** button at the top of the table displaying the call history. These records are downloadable in Excel (.xls) format.

Trace and Debug Information

When you contact Cisco Technical Support for help with a problem that you are having with Emergency Responder, Cisco might request that you collect trace and debug information.

Because collecting trace and debug information affects Emergency Responder performance, you should only turn on tracing and debugging at Cisco's request. The generated information is for Cisco's use in resolving product problems.

Enable Emergency Responder Trace and Debug Information

Procedure

Step 1 From the Emergency Responder web interface, select **Cisco ER Group > Server Settings For CERServerGroup**.

Step 2 From the left column, select the server from which you must collect debug or trace information.

Step 3 Scroll down to the debug package and trace package sections and select the packages that Cisco Technical Support has requested.

The lists in each section are identical; make sure that you select the package in the list that Cisco requested. Packages selected in the Debug list generate trace information plus extra debug data. If Cisco requests that you select all packages, click **Select All** for the appropriate list.

The available packages include:

- CER_DATABASE—The database subsystem, covers the log information generated by the database access code.
- CER_REMOTEUPDATE—The remote update subsystem, which manages updates between servers.
- CER_PHONETRACKINGENGINE—The phone tracking subsystem, which runs the phone tracking and switch port and phone update processes.
- ER_ONSITEALERT—The onsite alert subsystem for notifying onsite alert personnel.
- CER_CALLENGINE—The call engine subsystem, which routes and processes calls.
- CER_PROVIDER—The local service provider.
- CER_AUDIT—The Audit trials provide change history for ERL configurations.
- CER_SYSADMIN—The system administration web interface subsystem.
- CER_TELEPHONY—The telephony subsystem, used for interactions with Unified CM.
- CER_AGGREGATOR—The aggregator module covers all Emergency Responder server communication and data handling with the phone tracking engine. The module includes the search and lookup of tracked data for the subsystems such as cluster, Administration, CiscoIPSoftPhone, and call routing.
- CER_GROUP—The Emergency Responder server group subsystem used for communicating between servers within a group.
- CER_CLUSTER—The server cluster subsystem used for communicating between Emergency Responder groups in a cluster.
- CER_ACCESSPOINT—The access point details all the devices configured in Unified CM.

- CER_CREDENTIALPOLICY—The credential policy defined for all the local and remote user accounts.

Step 4 Click **Update** to save and activate your changes.

Emergency Responder begins generating the requested trace and debug information.

Note The traces for Emergency Responder can be collected from either Emergency Responder Serviceability web interface or by using the CLI.

Step 5 When you have finished generating debug and trace information, click **Clear All** for each section in which you have made a selection to turn off debug and trace. Click **Update** to complete the change.

Related Topics

Server Settings for Emergency ResponderServerGroup
Cisco Emergency Responder Serviceability Web Interface

Syslog Enablement

To collect trace and debug information, you must enable syslog for Emergency Responder.

To enable syslog for Emergency Responder, see Collect Information From Syslog , on page 33.

Event Messages

You can view Emergency Responder event messages to help diagnose problems with the software by using the Emergency Responder Serviceability web interface.

For information about viewing Emergency Responder events, see Use Event Viewer.

For details about the Find and List Events page, see Event Viewer.

Performance Management

See the latest version of the Release Notes for Cisco Emergency Responder for supported platforms and their Emergency Responder scalability.

Emergency Responder performance can be affected if Emergency Responder is managing switches across a WAN link. Emergency Responder must send SNMP requests to the managed switches, and WAN delays can lead to SNMP timeouts and increase the time needed to track phone and switch changes. You might need to tune the SNMP parameters. See Set Up SNMPv2 for more information.

Network Management Systems Integration

You can manage the status of the Emergency Responder server remotely using any SNMP-based network management system.

The following sections provide information to assist you in integrating Emergency Responder with network management systems.

Cisco Discovery Protocol Support

CiscoEmergency Responder uses the Cisco Discovery Protocol (CDP) to periodically send out CDP messages on the active interface to a designated multicast address. These messages contain information such as device identification, interface name, system capabilities, SNMP agent address, and time-to-live. Any Cisco device with CDP support can locate a CiscoEmergency Responder server by listening to these periodic messages.

Using information provided through CDP, the SNMP-based network management server can detect the CiscoEmergency Responder server and build topology maps displaying the CiscoEmergency Responder server.

In addition to sending out CDP messages, the CiscoEmergency Responder server uses CDP to locate phones that support CDP. You must ensure CDP is enabled on your switches so that CiscoEmergency Responder can obtain this information through SNMP queries to the switches.

Emergency Responder Components

CiscoEmergency Responder supports the SYSAPPL-MIB that allows you to use any SNMP-based browser to remotely access information about the following Emergency Responder components:

- CiscoEmergency Responder Server
    - CERServer.exe
- Cisco PhoneTrackingEngine
    - CERPhoneTracking.exe
- MSQL Server-related Services

The SYSAPPL-MIB uses SNMP. Emergency Responder supports the following SYSAPPL-MIB tables:

- SysApplInstallPkgTable—Provides installed application information such as Manufacturer, Product Name, Version installed, Date installed, and Location, which is a partial URL for accessing the associated Application Administration web page (when applicable).
- SysApplRunTable—Describes the application starting time and run-time status.
- SysApplInstallElmtTable—Describes the individual application elements, or associated executables, which comprise the applications defined in the SysApplInstallPkgTable.
- SysApplElmtRunTable—Describes the processes, or executables, that are currently running on the host system.

Collect Information From Syslog

You can configure Emergency Responder to use Syslog output from Emergency Responder for use with other network management systems.

Procedure

Step 1 Select **System > CiscoER Group Settings**.

Emergency Responder opens the Emergency Responder Group Settings page.

Step 2 Select enable in **Enable Syslog**.

Step 3 Enter the fully qualified DNS name of the server in the **Syslog Server** field, for example, server.domain.com.

Step 4 Click **Update Settings** to save your changes.

Emergency Responder immediately begins writing messages to syslog.

Related Topics

Group Settings

Data Backup and Recovery

Emergency Responder uses the Disaster Recovery System to backup and restore system data.

For information about using the Disaster Recovery System, see Configure Cisco Emergency Responder Disaster Recovery System

During a backup and restore procedure, you might encounter one of the following errors:

- Unable to send network request to master agent. This may be due to Master or Local Agent being down.
- Local Agent is not responding. This may be due to Master or Local Agent being down.

Check your Publisher and Subscriber services and confirm that your DRS Local and Master services are active and running.

Check your IPSEC certificates via the Cisco Emergency Responder OS Administration UI. Make sure these IPSEC-Trust certificates are not expired or corrupted. If they are expired or corrupted, regenerate these IPSEC certificates on all nodes and restart the Master and local agents.

Troubleshooting Data Migration Assistant

The Data Migration Assistant (DMA) operates in two phases. In the first phase, Database, the following folders are backed up to a tar file:

- export
- import
- etc
- nena_msag_records

In the second phase, the contents of the backed-up Emergency Responder database are verified against the Emergency Responder database schema.

DMA Backup and Validation Failed

Problem DMA backup and validation failed.

Solution Go through the following check list:

- Check if MSDE is running. If the database is not running, the backup fails.
- Verify that the node being backed up is a Publisher node, not a Subscriber node. DMA backup cannot be performed on a Subscriber node.
- Verify that CSA is not running. If CSA is running, stop it before starting the backup.

DMA Backup Is Successful but Validation Failed

Problem DMA backup is successful but the validation failed.

Solution Go through the following check list:

- Verify that CSA is not running. If CSA is running, stop it before starting the backup. CSA interferes with DMA operation.
- Collect the data validation logs for further analysis. In this case, some changes may need to be made to the data in the database before a migration to Emergency Responder can succeed.

Solution The DMA Logs are in the following locations:

- exportdb.log and migratecCERCSV.log are in C:\CiscoWebs\DMA\Bin
- installdbw1.log, installdbw1.log.err, installdbccm.log, installdbccm.log.err, and dbl_INSTALLDBxxxxxx.txt are located under C:\Program Files\Cisco\Trace\DBL
- Log Files are located under C:\Program Files\Cisco\Trace\DMA

Solution The validation log files are as follows:

- **Solution** exportdb.log
- **Solution** installdbw1.log
- **Solution** installdbw1.log.err
- **Solution** dbl_INSTALLEDBxxxxxx.txt

Troubleshoot Linux Upgrades

You might encounter certain problems when upgrading to future versions of Emergency Responder from your current version of Emergency Responder. This section explains what could cause these problems and the provides recommended actions.

No Valid Upgrade Options Found Error Appears on the First Page of Install/Upgrade Menu

Problem On the first page of the Install / Upgrade menu, after you enter the details for an upgrade patch, the error message “No valid upgrade options found” appears.

Solution Verify that you are not trying to upgrade the Subscriber before upgrading the Publisher. When upgrading an Emergency Responder server group, you must always upgrade the Publisher first.

Solution Verify that the local or remote path that you have specified actually contains a valid, signed ISO image, having the extension .sgn.iso.

Incorrect User Name/Password Error Appears on the First Page of the Install/Upgrade Menu

Problem On the first page of the Install / Upgrade menu, after you enter the details for an upgrade patch at a remote location, the error message “Incorrect user name/password” appears.

Solution Verify that the username and password entered for the remote SFTP or FTP location are correct.

Checksum Values Do Not Match After Downloading ISO Image on Emergency Responder Server

Problem After downloading the ISO image onto the Emergency Responder server, the checksum values do not match.

Solution Download a fresh ISO image from Cisco.com and try the upgrade again.

Upgrade Cancelled and Warning Message Appears Prompting You to Reboot System

Problem The upgrade was cancelled, but a warning message appears prompting you to reboot the system.

Solution During the upgrade, certain services on the Emergency Responder server could have been stopped, depending on when the upgrade was cancelled. In this case, it is highly recommended that you reboot the server.

Troubleshoot SAML Single Sign-On

Problem—The User Interface page does not come up when SAML Single Sign-On is Enabled or Disabled.

Solution—Check the status of the Cisco Tomcat service and restart the service manually on both publisher and the subscriber nodes if the status is not active.

Troubleshoot IOS Switch Upgrades

Assigned ERLs Turns to Null After IOS Switch Upgrade in Emergency Responder Server

Problem—After upgrading the IOS software on the switch in the Emergency Responder, it changes the port index value of the switch. And, the Emergency Responder treats the existing port as a new port and turns the assigned ERL to Blank (no ERL).

Solution—If the snmp-server ifindex persist configuration is present on the switch before the upgrade, then port information stays correct. By executing the "snmp-serverifindex persist" command on the switch, port information remains same after the upgrade.

Note Execute the **show run| inc snmp ifmib** command to check whether the snmp-server ifindex persist configuration is present in the Switch. If the ifIndex persist configuration exists, the output is displayed as:

```
Snmp ifmib ifindex persist
```