This report has been automatically generated by the Uplinx Report Tool. Nothing has been edited (apart from this note). Please note that due to aliasing, some borders might not DISPLAY correctly on the screen. This depends on the resolution of the screen. All lines appear perfectly in print.

Cisco Emergency Responder Configuration Report

Test Customer

As-Built Documentation for project

April 13, 2020

Document Information - Universal

Version Status

Release Number	Date	Reason for Version
1.0	April 13, 2020	Release

Client Information

Prepared for:	Client
Name:	Client
Title:	Client
Address:	Client
Telephone:	Client
Email:	Client@email.com

Presenter Information

Prepared by:	Test
Name:	First Last
Title:	Mr
Address:	ADDRESS
Telephone:	123456787
Email:	john@email.com

Table of Content

1 Report Summary 4
2 System 4
2.1 Cisco ER Groups In Cluster 4
2.2 Cisco ER Group Settings 5
2.3 Telephony Settings 5
2.4 Server Settings 6
2.5 License Manager 6
2.6 Mail Alert Configurations 7
3 ERL 7
3.1 Onsite Alert Settings 8
3.2 Pager and Email Alert Configurations 8
3.3 Conventional ERL 8
4 Phone Tracking 9
4.1 SNMPv2 Settings 10
4.2 SNMPv3 Settings 10
4.3 Schedule 10
4.4 Cisco Unified Communications Manager 11
4.5 LAN Switch Details 11
5 ERL Membership 11
5.1 Switch Ports 11
5.2 IP Subnets 11
5.3 Unlocated Phones 12
5.4 Manually Configured Phones 12
5.5 Synthetic Phones 12
6 User Management 12
6.1 User 13
6.2 Role 13
6.3 User Group 15
7 Reports 15
7.1 Call History 15
7.2 ERL Audit Trail 15
8 Command Line Output 16
8.1 Server 10.5.1.104 16
8.1.1 Show status 16
8.1.2 NTP Status 16
8.1.3 Show hardware 16
8.1.4 Show network eth0 17
8.1.5 Show version active 17
8.1.6 Show version inactive 17
8.1.7 Show timezone config 17
8.1.8 Show stats io 17

1 Report Summary

Cisco Emergency Responder (Cisco ER) helps you manage emergency calls in your telephony network so that you can respond to these calls effectively and so that you can comply with local ordinances concerning the handling of emergency calls. In North America, these local ordinances are called "enhanced 911," or E911. Other countries and locales might have similar ordinances.

Because emergency call ordinances can differ from location to location within a country, region, state, or even metropolitan area, Cisco ER includes the flexibility you need to fit your emergency call configuration to specific local requirements.

To track phones, Cisco ER queries Cisco Unified Communications Manager for a list of phones registered with the cluster. Then, Cisco ER queries the switches on the network (the ones you have identified to Cisco ER) to determine the port to which the phones are connected. Cisco ER does this tracking at regular intervals during the day so that it can identify when a phone moves.

Cisco ER can send emergency calls to the correct PSAP based on port and phone location.

Optionally, you can have an SMTP email server in your network or with a service provider. You can configure Cisco ER to send email to your onsite alert (security) personnel to notify them of emergency calls. If the server is set up as an email-based paging service, the personnel are paged.

Finally, you need a gateway with a PRI or CAMA link to the service provider's network so that Cisco ER can route emergency calls to the local public safety answering point (PSAP).

This configuration report contains the configuration objects for the Cisco Emergency Responder (Cisco ER) cluster.

Report Info	
Report Date	13-Apr-20 8:02:14 PM
Report generated for	Test Customer
Description	As-Built Documentation for project
Server Info	
CER version	10.5.1.20000(3)
CER IP	10.5.1.104
Report Settings	
Report Type	Direct Report
Visual Style	Blu Light.css
Report Content	All objects
Template HTML	CERreportTemplate.htm
Template Word	Squares_RightSidebar_Grey-universal.doc
Report Tool Info	
Report Tool Version	12.0.22 / 17 Feb 2020
Report Tool License	Licensed [Ent all]

2 System

This section describes system settings of Cisco Emergency Responder.

This section contains the following chapters:

- Cisco ER Groups in Cluster
- Cisco ER Group Settings
- Telephony Settings
- Server Settings
- License
- Mail Alert Configurations

2.1 Cisco ER Groups In Cluster

Cisco Emergency Responder (Cisco ER) groups form a Cisco ER cluster.

A Cisco ER server group consists of up to two Cisco ER servers, a primary and a standby, or backup, server. This redundancy helps ensure that Cisco ER remains available in case one server becomes disabled. Consider placing the two servers in a group in separate physical locations not separated by a WAN link so that problems that might affect one server do not affect the other, such as a fire, flood, or network disruption.

Deploy Cisco Emergency Responder (Cisco ER) in your network as a pair of redundant servers. One server is designated as the Publisher server and the other as the Subscriber server. Each Cisco ER Publisher server and Subscriber server make up a Cisco ER Server Group. Configuration data for the server groups is stored in a database on the Publisher. This data is replicated to the Subscriber.

A Cisco ER cluster is a set of Cisco ER server groups that share data to provide correct emergency call handling capabilities. Cisco ER cluster information is stored in a central location in the cluster called the cluster database. A Cisco ER server group is considered part of a cluster when the group points to the same cluster database as the other server groups in that cluster.

A Cisco ER server group consists of up to two Cisco ER servers, a primary and a standby, or backup, server. This redundancy helps ensure that Cisco ER remains available in case one server becomes disabled. Consider placing the two servers in a group in separate physical locations not separated by a WAN link so that problems that might affect one server do not affect the other, such as a fire, flood, or network disruption.

The following Cisco ER Server Groups are present in the cluster:

CER Servers and Server Group			
Server	**Type**	**Server Group**	**Schemaversion**
cer104	Publisher	CERServerGroup	10.5.1.20000(3)

2.2 Cisco ER Group Settings

A Cisco ER server group consists of up to two Cisco ER servers, a primary and a standby, or backup, server. This redundancy helps ensure that Cisco ER remains available in case one server becomes disabled.

The following settings are configured for the a Cisco Emergency Responder (Cisco ER) server groups:

Cisco ER Group Settings	
Cisco ER Group Name	CERServerGroup
Peer TCP Port	17001
Heart beat Count	3
Heart beat Interval (in sec)	30
Active Call Time out (in min)	180
SMTP Mail Server	
Source Mail ID	
System Administrator Mail ID	
Calling Party Modification	disable
SysLog	disable
Syslog Server	
Notes	
Dynamic Tracking of Switch IP Address	N
Security end user web interface language	English(US)
Limit Concurrent Sessions	N
Max. number of concurrent sessions	< None >

2.3 Telephony Settings

The Telephony Settings page defines telephone numbers and telephony ports used by the Cisco ER group.

Telephony Settings	
Route Point for Primary Cisco ER Server	911
Route Point for Standby Cisco ER Server	912
PSAP Callback Route Point Pattern	913XXXXXXXXX
ELIN Digit Strip Pattern	913
UDP Port Begin	32000

Inter Cisco ER Group Route Pattern	
IP Type of service (00-FF)	0xb8
Onsite Alert Prompt Repeat Count	2
Use IP Address from call signaling	N
Intrado Route Pattern Settings	

2.4 Server Settings

Cisco ER servers are inserted in the Cisco ER group when the Cisco ER services are started

Different levels of privilege exist for each application. For the Cisco Unified Communications Manager Administration application, two levels of privilege exist: read privilege and update privilege.

Server	
Server	**Info**
Publisher	**Server Settings**
	Server Name: Publisher
	Host Name: cer104
	Debug Package List
	CER_DATABASE: N
	CCER_REMOTEUPDATE: N
	CER_PHONETRACKINGENGINE: N
	CER_ONSITEALERT: N
	CER_CALLENGINE: N
	CER_SYSADMIN: N
	CER_TELEPHONY: N
	CER_AGGREGATOR: N
	CER_GROUP: N
	CER_CLUSTER: N
	Trace Package List
	CER_DATABASE: N
	CCER_REMOTEUPDATE: N
	CER_PHONETRACKINGENGINE: N
	CER_ONSITEALERT: N
	CER_CALLENGINE: N
	CER_SYSADMIN: N
	CER_TELEPHONY: N
	CER_AGGREGATOR: N
	CER_GROUP: N
	CER_CLUSTER: N

2.5 License Manager

Cisco ER requires server and user licenses.

You must purchase a separate **server license** for each Cisco ER server in a server group. Cisco generates the server license based on the MAC Address on the server. You must use the MAC Address of the ethernet card on the publisher server to generate a server license for the Publisher. Order two server licenses for each server in a Cisco ER group: one server license for the primary (Publisher) server and a separate server license for the secondary (Subscriber) server. You cannot share a server license between the Publisher server and the Subscriber server.

You must purchase a separate **user license** for each Cisco ER group. User licenses can be shared between Publisher and Subscriber servers within each Cisco ER group. This includes both implicit 100-user licenses that are provided by the primary and secondary server license. You cannot share Cisco ER user licenses between different Cisco ER groups in a Cisco ER cluster, or between different Cisco ER clusters.

The following licenses are present:

< Not Available >

2.6 Mail Alert Configurations

The Email Alert Settings page is used to specify the parameters under which Cisco ER will send email alerts. The checkbox to the right of each parameter is used to enable (check) or disable (uncheck) email alerts for that parameter. Check the Include event viewer contents in mail checkbox if you want to include the details from the event viewer in the email message.

Different levels of privilege exist for each application. For the Cisco Unified Communications Manager Administration application, two levels of privilege exist: read privilege and update privilege.

Email Alert Settings

Settings

Discovery Parameters

Event	Get Mail	Include event viewer contents in mail
Discovery Engine Registration Failed	Y	Y
Discovery Engine goes out of connection	Y	Y
For unreachable devices during discovery	Y	Y

Emergency Call Routing Parameters

Event	Get Mail	Include event viewer contents in mail
Call information	Y	Y
Call routing session ended due to problems	Y	Y
Re-Routing of call	Y	Y
Routing failure	Y	Y
Route Point status (In service/Out of service)	Y	Y

Cluster Parameters

Event	Get Mail	Include event viewer contents in mail
Cluster DB Failure	Y	Y
Intra Cluster Failure	Y	Y

Misc Parameters

Event	Get Mail	Include event viewer contents in mail
Subscriber becomes active	Y	Y
Publisher comes back online	Y	Y
Not able to get the JTAPI Provider	Y	Y
Available user licenses get exhausted during phone tracking	Y	Y
Switch Port location change reporting	N	Y
Suppress IP Communicator/ Unified Personal Communicator location change reporting	N	Y
Alert System Administrator about Audit Log processing failures	N	N
DRF Alert	N	N

3 ERL

This section describes system settings of Emergency Responder Locations (ERLs).

The Emergency Responder Locations (ERL) is an area from which an emergency call is placed. The ERL is not necessarily the location of the emergency. If an emergency caller is reporting a general emergency, the actual emergency might be in a different area. In Cisco ER, you assign switch ports and phones to ERLs, and ERL definitions include Automatic location information (ALI) data.

Automatic location information (ALI) ties an ELIN to a location and is used to route emergency calls from that ELIN to the correct local PSAP, and is presented to the PSAP to help the PSAP locate the emergency caller. In Cisco ER, you fill in ALI data for each ERL and submit the ALI data to your service provider for inclusion in the ALI database.

Emergency location identification number (ELIN) is a phone number that routes the emergency call to the local PSAP, and which the PSAP can use to call back the emergency caller. The PSAP might need to call the number if the emergency call is cut off, or if the PSAP needs additional information after normally ending the emergency call.

The Public safety answering point (PSAP) is the organization that receives emergency calls (for example, the 911 operator) and is staffed by people trained in handling emergency calls. The PSAP talks to the emergency caller and notifies the appropriate public service organizations (such as police, fire, or ambulance) of the emergency and its location.

This section contains the following sub chapters:

- Onsite Alert Settings
- Pager Alert Configurations
- Conventional ERL

3.1 Onsite Alert Settings

Onsite Alert Settings contain information about your onsite alert personnel. When you configure ERLs, you assign these personnel to them. Cisco ER will alert the assigned personnel when an emergency call is made within the zone.

The following Onsite Alert Settings are configured:

< No records found >

3.2 Pager and Email Alert Configurations

Use the Pager Alert Configurations page to limit the size of system-wide pager messages by selecting the fields that are sent to the pager and by editing the labels for those fields.

You can limit the size of the pager message that is sent by selecting the following fields and editing the labels are associated with those fields: Extension, ERL, Location, Time, Server.

Pager and Email Alert Settings		
Enabled	**Title**	**As it appears on the pager or email**
Pager Alert Settings		
Y	EXTENSION	Extension
Y	ERL	Zone/ERL
Y	LOCATION	Location
N	SYSTEM TIME	Time of Call
Y	SERVER	Server
N	LOCAL TIME	Local Call Time
Email Alert Settings		
N	CALLER EXTENSION	Caller Extension
N	DISPLAY NAME	Display Name
N	ZONE	Zone/ERL
N	LOCATION	Location
N	SYSTEM CALL TIME	System Call Time
N	LOCAL CALL TIME	LOCAL_CALL_TIME
N	SERVER DETAILS	
N	ADDITIONAL NOTES	
N	DISCARD DN DIGITS	

3.3 Conventional ERL

Use the Conventional ERL Data page to define the emergency response locations (ERLs) for your company. An ERL might be a whole building (if it is small), the floor of a building, or an area on a floor. Each community can have different laws concerning the size of an ERL, so consult your local ordinances and with your service provider before deciding on your ERLs. The ERLs you create will be used by emergency response teams to locate the emergency, so the ERL should be small enough that these teams can locate the caller within a reasonable time.

You must configure the Default ERL before configuring any other ERLs. The default ERL is the system-defined ERL that will be used to route calls if no other ERL configuration is found.

Conventional ERL	
ERL Name	**ERL Information**

Conventional ERL	
ERL Name	**ERL Information**
Default	

ERL Settings	
Description	
ELIN	
ELIN	
Onsite Alert	
Onsite Alert	
ERL Address	
House Number	
House Number Suffix	
Street Name	
Prefix Directional	
Street Suffix	
Post Directional	
Community Name	
State	
Main NPA	
Main Telephone No	
Class Of Service	
Type of Service	
Exchange	
Customer Name	
Order Number	
Extract Date	
County ID	
Company ID	
Zip Code	
Zip Code Extension	
Customer Code	
Comments	
Longitude	
Latitude	
Elevation	
TAR Code	
Location	
Reserved	

4 Phone Tracking

Cisco Emergency Responder (Cisco ER) uses Cisco Discovery Protocol (CDP) to locate phones, so you should enable CDP on all of your switches. If you do not enable CDP, Cisco ER must use the Content Addressable Memory (CAM) table on the switch to track phones. Using the CAM table is less efficient than using CDP.

If some of the phones on your network do not use CDP, Cisco ER tracks them using the CAM table.

To track phones successfully, Cisco Emergency Responder (Cisco ER) must periodically contact switches to obtain port and device information.

Cisco ER updates network information using two processes:

- **Phone Tracking:** A periodic comparison of the phones registered with Cisco Unified Communications Manager to the location information obtained from the switches. If a phone moves, Cisco ER updates the phone's ERL. Phones that cannot be located are classified as unlocated phones. If you do not configure a switch port phone update schedule, the default schedule will run at midnight.

- **Switch Port and Phone Update:**The phone tracking process plus a more extensive check of the network switches, which can identify new or changed switch modules (additional or removed ports). Any newly-discovered ports are assigned to the Default ERL. Ensure that your ERL administrator updates the ERL assignment for new ports.

The Public safety answering point (PSAP) is the organization that receives emergency calls (for example, the 911 operator) and is staffed by people trained in handling emergency calls. The PSAP talks to the emergency caller and notifies the appropriate public service organizations (such as police, fire, or ambulance) of the emergency and its location.

This section contains the following chapters:

- SNMP Settings
- Schedule
- Cisco Unified Communications Manager (CUCM)
- LAN Switch Details

4.1 SNMPv2 Settings

Emergency Responder supports SNMP V1/V2C and V3. You can use the Serviceability web interface to configure SNMP V1/V2C (Community String and Notification Destination) and SNMP V3 (User and Notification Destination).

Each SNMP version has security models and security levels. Users are assigned to groups that are defined by a security model and specified security levels. Each group also has a defined security access level to a set of MIB objects for reading and writing, which are known as views. The switch has a default view (all MIB objects) and defaults groups defined for SNMP V1 and V2C security models. SNMP V3 provides additional security features that cover message integrity, authentication, and encryption. In addition, SNMP V3 controls user access to specific areas of the MIB tree

< No records found >

4.2 SNMPv3 Settings

Emergency Responder supports SNMP V1/V2C and V3. You can use the Serviceability web interface to configure SNMP V1/V2C (Community String and Notification Destination) and SNMP V3 (User and Notification Destination).

Each SNMP version has security models and security levels. Users are assigned to groups that are defined by a security model and specified security levels. Each group also has a defined security access level to a set of MIB objects for reading and writing, which are known as views. The switch has a default view (all MIB objects) and defaults groups defined for SNMP V1 and V2C security models. SNMP V3 provides additional security features that cover message integrity, authentication, and encryption. In addition, SNMP V3 controls user access to specific areas of the MIB tree

< No records found >

4.3 Schedule

To track phones successfully, Cisco Emergency Responder (Cisco ER) must periodically contact switches to obtain port and device information. Cisco ER updates network information using two processes:

Phone Tracking: A periodic comparison of the phones registered with Cisco Unified Communications Manager to the location information obtained from the switches. If a phone moves, Cisco ER updates the phone's ERL. Phones that cannot be located are classified as unlocated phones

Note: If you do not configure a switch port phone update schedule, the default schedule will run at midnight.

Switch-Port and Phone Update: The phone tracking process plus a more extensive check of the network switches, which can identify new or changed switch modules (additional or removed ports). Any newly-discovered ports are assigned to the Default ERL. Ensure that your ERL administrator updates the ERL assignment for new ports.

Switch-Port and Phone Update Schedule								
Sun	**Mon**	**Tue**	**Wed**	**Thu**	**Fri**	**Sat**	**Hour**	**Minute**
Y	Y	Y	Y	Y	Y	Y	00	00

4.4 Cisco Unified Communications Manager

Use the Cisco Unified Communications Manager Clusters page to identify the Cisco Unified Communications Manager clusters whose emergency calls this Cisco Emergency Responder (Cisco ER) group will handle. Only assign a Cisco Unified Communications Manager cluster to a single Cisco ER group. Cisco ER gets the list of phones registered with these Cisco Unified Communications Manager servers and tracks the movements of these phones.

< No records found >

4.5 LAN Switch Details

You must tell Cisco Emergency Responder (Cisco ER) which switches to manage. Cisco ER tracks port changes, including changes to the devices connected to those ports, and can recognize which ports have phones connected to them. Identify all switches that might have phones attached to them, essentially all edge switches.

The following LAN switches are defined:

< No records found >

5 ERL Membership

In Cisco ER, you assign switch ports and phones to ERLs, and ERL definitions include Automatic location information (ALI) data. The Emergency response location (ERL) defines an area from which an emergency call is placed. The ERL is not necessarily the location of the emergency. If an emergency caller is reporting a general emergency, the actual emergency might be in a different area

To track phones, Cisco ER queries Cisco Unified Communications Manager for a list of phones registered with the cluster. Then, Cisco ER queries the switches on the network (the ones you have identified to Cisco ER) to determine the port to which the phones are connected. Cisco ER does this tracking at regular intervals during the day so that it can identify when a phone moves.

This section contains the following chapters:

- Switch Ports
- IP subnets
- Unlocated phones
- Manually configured phones
- Synthetic phones

5.1 Switch Ports

Use the Switch Port Details page to assign switch ports to Emergency Responder Locations (ERLs). This assignment allows Cisco Emergency Responder (Cisco ER) to assign the correct ERL to phones that connect to the network through the configured ports.

After the network administrator adds switches to the Cisco Emergency Responder (Cisco ER) configuration, and runs the switch-port and phone update process, you can assign the switch ports to emergency response locations (ERLs). When you assign a port to an ERL, make sure that you assign the ERL based on the location of the device attached to the port, not the location of the port itself.

< No records found >

5.2 IP Subnets

IP Subnet configurations are used to automatically assign phones to Emergency Responder Locations (ERLs). You need to manually define an IP Subnet if any of these conditions apply:

Cisco Emergency Responder (Cisco ER) cannot automatically track the type of phone, for example, if the phone is wireless.

Use the CiscoWorks IP Telephony Environment Monitor (ITEM) 2.0 to monitor the health of your Cisco ER system. You create subnets, configure test ERLs and associate them to the subnet, and configure synthetic phones to belong to the test ERLs.

The following IP Subnets are configured:

< No records found >

5.3 Unlocated Phones

Use the Unlocated Phones page to identify phones that are registered with Cisco Unified Communications Manager, but which Cisco Emergency Responder (Cisco ER) cannot locate. This can happen for several reasons:

- The phone is attached to a switch that is not defined in Cisco ER.
- The phone is connected to an unsupported device, such as a router port, a hub connected to a router, or an unsupported switch.
- The switch to which the phone is connected is currently unreachable; for example, it does not respond to SNMP queries.
- The phone is not found under any configured IP subnet and the phone is not configured as a synthetic phone.
- The phone that was manually assigned.
- The phone that was previously identified as an unlocated phone and assigned an ERL.

Because Cisco ER cannot assign an unlocated phone to the appropriate ERL, try to identify and resolve all problems that are preventing Cisco ER from locating these phones on your network. If you cannot resolve the problems by defining switches in Cisco ER, or by moving phones to supported switch ports, you might have to manually assign a phone to an ERL.

The following unlocated phones have been found by CER:

< No records found >

5.4 Manually Configured Phones

The following manual phones and associated ERL are defined. You need to manually define a phone if any of these conditions apply:

- Cisco Emergency Responder (Cisco ER) cannot automatically track the type of phone, for example, if the phone is analog. See the "Network Hardware and Software Requirements" topic for information on phone support.
- The phone is hosted on an unsupported port, such as a router port, a hub connected to a router, or a port on an unsupported switch.

For manually defined phones, Cisco ER cannot automatically locate and update ERL information. You should regularly review manual phone configurations to ensure they are correct.

The following manual phones are defined:

< No records found >

5.5 Synthetic Phones

You must configure synthetic phones in the subnet for testing ERL configurations. You can use the CiscoWorks IP Telephony Environment Monitor 2.0 (ITEM) in conjunction with Cisco ER's test ERLs.

For synthetic phones, Cisco ER cannot automatically locate and update ERL information. You should regularly review synthetic phone configurations to ensure they are correct.

The following synthetic phones are defined:

< No records found >

6 User Management

The following chapters contain the configuration of users, roles and user groups. Cisco ER uses a role based user management mechanism.

You can add additional users. Once the additional users are added, you assign them to user groups. The new user then inherits the roles that were defined for that user group.

- User
- Roles

- User Group Configuration

6.1 User

On installation, the system creates one default user, CERAdministrator. The CERAdministrator has access to all system administration screens except the Platform Administration and Disaster Recovery System screens. By default, the CERAdministrator user is assigned to the CER System Administrator, CER Serviceability, CER Admin Utility, and CER User user groups and has access to the resources defined for the CER System Admin, CER Serviceability, CER Admin Utility, and CER User roles.

Note: The default CERAdministrator user cannot be deleted.

You can add additional users. Once the additional users are added, you assign them to user groups. The new user then inherits the roles that were defined for that user group

The following users are defined:

User				
Name	**Authentication Mode**	**Standard User**	**Groups**	**Roles**
admin	Local	Y	CER Admin Utility CER Serviceability CER System Administrator CER User	CER Admin Utility CER Serviceability CER System Admin CER User

6.2 Role

Roles define privileges which allow functionality within the application. Roles are assigned to user groups which are assigned to users.

Four default roles are created during installation and are listed here. They are:

- CER System Admin
- CER ERL Admin
- CER Network Admin
- CER User

You can only modify information for roles that you create. After you create additional roles, they will also be listed along with the default roles.

The following roles are defined:

Role	
Name	**Details**
CER System Admin	**Details** Description: All System Configurations Standard Role: Y **Resource Permissions** Resource Permissions: ALI Formatting Tool Add Subscriber Application User CER Groups in Cluster Call History Call Manager Details Device Snmp Settings ERL ERL Audit Trail ERL Debug Tool ERL Migration File Management Utility Functional role IP Subnet Intrado ERL Intrado VUI Settings LAN Switches License Management Mail Alert Configurations

Role	
Name	**Details**
	Manually Configured Phones Off-Premises ERL OnsiteContact PS ALI Convert PS ALI Export Pager Alert Configurations Purge Run Tracking Server Server Group Switch Port Synthetic Phone Telephony Tracking Schedule Unlocated Phones User Group
CER ERL Admin	**Details**
	Description: ERL Configurations
	Standard Role: Y
	Resource Permissions
	Resource Permissions: ERL IP Subnet Manually Configured Phones OnsiteContact Switch Port Synthetic Phone Unlocated Phones
CER Network Admin	**Details**
	Description: Network Configurations
	Standard Role: Y
	Resource Permissions
	Resource Permissions: Call Manager Details Device Snmp Settings LAN Switches Run Tracking Tracking Schedule
CER Serviceability	**Details**
	Description: Serviceability Pages
	Standard Role: Y
	Resource Permissions
	Resource Permissions: All Logs CPU & Memory Usage Control Centre Disk Usage Event Viewer MIB2 system group configuration Processes SNMP V1/V2c configuration SNMP v3 configuration
CER Admin Utility	**Details**
	Description: Admin utility Pages
	Standard Role: Y
	Resource Permissions
	Resource Permissions: Change CCM Version Cluster DB Host setting
CER User	**Details**
	Description: Security User Pages
	Standard Role: Y
	Resource Permissions
	Resource Permissions: Phone Search

Role	
Name	**Details**
	User Call History Web Alert

6.3 User Group

Cisco ER 2.0 uses a role-based user management mechanism. When you create a user group, you assign roles and add users to the group. Multiple roles can be assigned to a single group. The users in the group will have access to all the resources defined by the roles assigned to the group.

Six default user groups are created during installation and are listed here. They are:

- CER System Administrator (Assigned System Administration roles)
- CER Network Administrator (Assigned Network Administration role)
- CER ERL Administrator (Assigned ERL Administration role)
- CER Serviceability (Assigned Serviceability role)
- CER Admin Utility (Assigned Admin Utility role)
- CER User (Assigned User role)

The following user groups are defined:

User Group		
Name	**Description**	**Standard Group**
CER System Administrator	ER Administrator for all system configurations	Y
CER ERL Administrator	ER Administrator for ERL configurations	Y
CER Network Administrator	ER Administrator for network configurations	Y
CER Serviceability	ER Serviceability user for serviceability pages	Y
CER Admin Utility	ER Admin utility user for admin utility pages	Y
CER User	ER security user who attends to emergency calls	Y

7 Reports

The following chapters contain additional reports.

- Call History
- ERL Audit Trail

7.1 Call History

The Call History page lists the history of emergency calls made from your network. Cisco Emergency Responder (Cisco ER) maintains the most recent 10,000 call history records. There is no restriction on when these calls were placed.

System administrator, ERL administrator, network administrator, or user authority have access to this page.

< No records found >

7.2 ERL Audit Trail

The audit trail lists for an ERL when, and by whom an ERL was created or changed.

System administrator, ERL administrator, or network administrator authority can view the audit trail.

ERL Audit Trail		
ERL Name	**Details**	
Default	**Details**	
	ERL Type	Conventional ERL
	Modified By	SYSTEM
	Modified Time	April 9, 2020 5:00:57 AM PDT
	Modification Details	Added new ERL

8 Command Line Output

This section contains status and configuration objects obtained via the command line.

8.1 Server 10.5.1.104

This section contains status and configuration objects obtained via the command line.

- show status
- utils ntp status
- show hardware
- show network eth0
- show version active
- show version inactive
- show timezone config
- show stats io

8.1.1 Show status

show status

```
Host Name : cer104
Date : Mon Apr 13, 2020 11:02:19
Time Zone : Pacific Daylight Time (America/Los_Angeles)
Locale : en_US.UTF-8
Product Ver : 10.5.1.20000-3
Unified OS Version : 6.0.0.0-2
License MAC : 71cffb44872e

Uptime:
11:02:21 up 4 days, 5:50, 2 users, load average: 0.35, 0.10, 0.03

CPU Idle: 58.59% System: 05.05% User: 36.36%
IOWAIT: 00.00% IRQ: 00.00% Soft: 00.00%

Memory Total: 3926064K
Free: 2015432K
Used: 1910632K
Cached: 531044K
Shared: 0K
Buffers: 301536K

Total Free Used
Disk/active 13711708K 2596908K 10975496K (81%)
Disk/inactive 13711708K 12850088K 165096K (2%)
Disk/logging 47708064K 44246172K 1038444K (3%)
```

8.1.2 NTP Status

utils ntp status

```
ntpd (pid 7270) is running...

remote refid st t when poll reach delay offset jitter
==============================================================================
*10.5.1.100 95.81.173.8 3 u 885 1024 377 1.333 -0.082 0.410


synchronised to NTP server (10.5.1.100) at stratum 4
time correct to within 177 ms
polling server every 1024 s

Current time in UTC is : Mon Apr 13 18:02:21 UTC 2020
Current time in America/Los_Angeles is : Mon Apr 13 11:02:21 PDT 2020
```

8.1.3 Show hardware

show hardware

```
HW Platform : VMware Virtual Machine
Processors : 1
Type : Intel(R) Core(TM) i7-4930K CPU @ 3.40GHz
```

show hardware

CPU Speed : 3400
Memory : 4096 MBytes
Object ID : 1.3.6.1.4.1.9.1.1348
OS Version : UCOS 6.0.0.0-2.i386
Serial Number : VMware-56 4d 25 3c 24 bc eb f5-64 dd 63 42 0e 74 72 3a

RAID Version :
No RAID controller information is available

BIOS Information :
PhoenixTechnologiesLTD 6.00 04/05/2016

RAID Details :
No RAID information is available

Physical device information

Number of Disks : 1
Hard Disk #1
Size (in GB) : 75

Partition Details :

Disk /dev/sda: 9790 cylinders, 255 heads, 63 sectors/track
Units = sectors of 512 bytes, counting from 0

Device Boot Start End #sectors Id System
/dev/sda1 * 2048 27863039 27860992 83 Linux
/dev/sda2 27863040 55724031 27860992 83 Linux
/dev/sda3 55724032 56248319 524288 83 Linux
/dev/sda4 56248320 157286399 101038080 5 Extended
/dev/sda5 56250368 60346367 4096000 82 Linux swap / Solaris
/dev/sda6 60348416 157286399 96937984 83 Linux

8.1.4 Show network eth0

show network eth0

Ethernet 0
DHCP : disabled Status : up
IP Address : 10.5.1.104 IP Mask : 255.255.255.000
Link Detected: yes Mode : Auto disabled, Full, 10000 Mbits/s
Duplicate IP : no

DNS
Not configured.
Gateway : 10.5.1.1 on Ethernet 0

8.1.5 Show version active

show version active

Active Master Version: 10.5.1.20000-3
Active Version Installed Software Options:
No Installed Software Options Found.

8.1.6 Show version inactive

show version inactive

Inactive Master Version: 0.0.0.0000-0000

8.1.7 Show timezone config

show timezone config

Current timezone: Pacific Daylight Time (America/Los_Angeles)
Timezone version: 2015a

8.1.8 Show stats io

show stats io

avg-cpu: %user %nice %system %iowait %steal %idle

show stats io
0.57 0.01 0.53 0.12 0.00 98.77 Device: tps Blk_read/s Blk_wrtn/s Blk_read Blk_wrtn sda 11.51 2.18 91.83 796506 33600652