



Emergency Gateway

System Guide

Software Version 5.6

Notice

Intrado EGW System Guide Software Version 5.6 Documentation
© 2020 by Intrado Safety Services
All Rights Reserved
Printed in U.S.A.

This software product is copyrighted and all rights reserved by Intrado Safety Services. The product is licensed to the original licensee only for use according to the terms and conditions set forth in the System Agreement or applicable document containing the licensing provisions. Copying, selling, or using the product contrary to those licensing terms and conditions is a violation of the law. All parts of this Software documentation are copyrighted and all rights reserved. This documentation may not be copied, photocopied, or reproduced in whole or in part without Intrado's prior written consent except as otherwise provided in writing. Any authorized copying or reproduction in whole or in part, must contain the following statement:

Intrado Emergency Gateway Documentation
© 2020 by Intrado Safety Services
All Rights Reserved
Printed in U.S.A.

If you have any questions regarding the appropriate use of this software product and documentation, please direct your comments to:

Intrado
Life & Safety Business Center
1601 Dry Creek Drive
Longmont, CO 80503
720.494.5800

Trademark Ownership

All trademarks used herein are the property of their respective owners.

Product Updates

It is the policy of Intrado to improve products as new technology, software, hardware, and firmware become available. Intrado, therefore, reserves the right to change specifications without prior notice. All features, functions, and operations described herein may not be available worldwide.

Table of Contents

1	INTRODUCTION	14
1.1	About this Guide.....	14
1.2	Audience	14
1.3	Customer Support.....	14
1.4	Conventions.....	14
1.5	References.....	14
2	PRODUCT OVERVIEW.....	16
2.1	About the Emergency Gateway	16
2.1.1	EGW Features	17
2.2	Emergency Gateway Specifications	18
2.2.1	Software Specifications.....	19
2.2.1.1	Support for Cisco	20
2.2.1.2	Support for Mitel	21
2.2.1.3	Support for Avaya	22
2.2.1.4	Support for Microsoft	23
2.2.2	Hardware Specifications	24
2.2.3	Hardware Requirements for EGW Virtual Appliance.....	26
2.3	Licensing.....	26
2.3.1	EGW Server Licenses.....	26
2.3.2	Activation.....	26
2.3.2.1	Automatic Activation	26
2.3.2.2	Manual Activation.....	27
2.3.3	Changing/Upgrading an EGW Server License	27
2.3.4	Feature Licenses	27
2.3.4.1	Endpoint Licensing	27
2.3.5	Viewing the Status of a License	27
3	SYSTEM PLANNING.....	29
3.1	How the EGW Fits Into the Network.....	29
3.1.1	Network Interfaces	30
3.2	Topology Scenarios	31
3.2.1	SIP/NAT-Enabled Firewall	31
3.2.2	EGW Connecting via VPN Tunnel to ERS.....	32
3.2.3	SIP/NAT-Enabled Session Border Controller (SBC)	32
3.2.4	EGW in SBC mode	33
3.2.5	Demilitarized Zone (DMZ).....	33
3.2.6	EGW in Transparent NAT Traversal Mode	34
3.3	Deploying the Emergency Gateway	34

3.3.1	EGW Deployment Scenarios	34
3.3.2	Cisco Extension Mobility Cross Cluster Deployments.....	37
3.3.3	Centralized LIS Deployment.....	38
3.4	Call Routing	39
3.4.1	Planning for Call Routing via the ERS	39
3.4.2	Planning for Call Routing via the Local Exchange Carrier	40
3.4.3	Planning for Emergency Conferencing and Routing Calls to Security Desks	41
3.4.4	Test Mode.....	42
3.5	SIP and the EGW	43
3.5.1	Redundancy and Failover.....	43
3.5.1.1	Redirection.....	43
3.5.1.2	SIP Routing Server Redundancy.....	44
3.5.1.3	Service Unavailable.....	44
3.5.2	Supported SIP Standards	45
3.5.3	Supported SIP Request Methods	45
3.5.4	Call Failure Scenarios for Failed Calls.....	45
3.5.4.1	Scenario 1: EGW immediately sends service unavailable response based on peer status.....	45
3.5.4.2	Scenario 2: EGW tries ERS but call routing is unsuccessful.....	46
3.5.4.3	Scenario 3: EGW immediately sends service unavailable response based on peer status. (local trunking) 46	
3.5.4.4	Scenario 4: EGW tries destination but call routing is unsuccessful.	47
3.5.4.5	Scenario 5: EGW tries destination but call routing is unsuccessful. (not monitored)	47
3.5.5	Restrictions	48
3.6	Notification Capabilities.....	48
3.6.1	Planning for Sending SNMP Traps	48
3.6.2	Mail Server Settings	49
3.6.3	Crisis Alerts	49
3.6.4	Desk Alert.....	49
3.6.5	URL Variables and URL Template Editor	49
3.7	Preparing Your Users for the EGW.....	50
3.8	Planning for Unified Communications	50
4	CONFIGURING BASIC SETTINGS.....	52
4.1	Configuration Overview	52
4.2	First Run Configuration/Activation	55
4.2.1	Configure Network Settings.....	55
4.2.2	Configure 911 Administrator Password.....	56
4.2.3	Replication Setup.....	57
4.2.4	First Run EGW Activation.....	57
4.2.4.1	Manual Activation.....	57
4.3	Web-Based Dashboard.....	58
4.3.1	Browser Requirements	58
4.3.2	Logging On	58
4.3.2.1	Passwords	59
4.3.3	User Management	59

4.3.3.1	Access Levels.....	59
4.3.4	LDAP System, Directory and Authentication Settings.....	60
4.3.4.1	LDAP Directory settings	60
4.3.4.2	LDAP Field Equivalence.....	62
4.3.5	Modifying Default Access Levels for Limited and Provisioning	62
4.3.6	LDAP Server Certificates	63
4.4	Server Certificates.....	63
4.4.1	Generate the Certificate Request	63
4.4.2	Submit the Certificate Request to the CA.....	65
4.4.3	Install the Server Certificate	65
5	CONFIGURING CALL ROUTING.....	67
5.1	Configuring Basic Telephony and Networking Settings.....	67
5.1.1	ERS Account Settings	67
5.1.2	Callback Settings	69
5.1.2.1	RegEx Exclusion List	70
5.1.2.2	Digit Manipulation	70
5.1.3	Understanding How Callbacks work with the ERS.....	71
5.1.4	NAT Traversal.....	72
5.1.4.1	Configuring Transparent NAT Traversal.....	72
5.2	EGW Dial Plan.....	73
5.2.1	What Happens when a Dial Plan number is dialed?.....	73
5.2.2	Configuring the Dial Plan	74
5.2.3	Misdial Protection.....	75
5.2.4	Override ERL Security Desk Number.....	75
5.3	Test Mode	76
5.3.1	Configuration	76
5.3.1.1	Adding a Test IP-PBX Server.....	77
5.3.1.2	Adding Test Endpoint.....	77
5.3.1.3	Adding Test Dial Plan	77
5.3.2	CDRs	78
5.4	Configuring Emergency Conferencing and Security Desk Routing	78
5.4.1	Understanding Security Desk Call Routing and Emergency Call Conferencing.....	78
5.4.1.1	Configuration Checklists and Scenarios	80
5.4.1.2	Security Desk Call Leg Feature Codes	81
5.4.2	Security Desk Routing and Emergency Call Conferencing Configuration Requirements.....	81
5.4.2.1	ERL Configuration	82
5.4.2.2	Dial Plan Settings	83
5.4.2.3	Dashboard Settings.....	85
5.4.3	Limitations of Emergency Call Conferencing	87
6	CONFIGURING LOCAL TRUNKING (LEC CALL ROUTING)	88
6.1	Overview	88
6.2	Understanding What Happens When a Local Trunking Call is Made	88
6.2.1	Supported Deployments.....	88

6.2.1.1	PSTN Gateways in Multiple Locations	88
6.2.1.2	Support for Multiple Emergency numbers in Local Trunking	89
6.2.1.3	Single Gateway or SBC	89
6.3	Provisioning ERLs for Local Trunking.....	90
6.4	Configuring EGW Local Trunking Settings	90
6.5	Working with NENA 2 Files.....	90
6.6	ELIN Management	91
6.6.1	Uploading ELINs to the EGW's ELIN Pool	91
6.6.2	Understanding Multiple ERLs per ELIN	92
6.6.3	Configuring Multiple ERLs per ELIN	94
7	CONFIGURING IP-PBX SETTINGS.....	95
7.1	Configuring Cisco UCM Settings.....	95
7.1.1	Understanding How the EGW works with Cisco Unified Communications Manager (CUCM) Deployments.....	95
7.1.1.1	Call Routing Overview.....	95
7.1.2	Device Inventory.....	96
7.1.2.1	AXL Filtering	97
7.1.2.2	Understanding the Endpoints Count on System Status.....	97
7.1.2.3	Automatic Phone Inventory.....	97
7.1.3	Configuring the EGW for the CUCM	98
7.1.3.1	CUCM server settings.....	103
7.1.3.2	Configuring Extension Mobility Cross Cluster	104
7.2	Configuring Avaya Communications Manager (CM) Settings	105
7.2.1	Understanding How the EGW works with Avaya CM Deployments.....	105
7.2.1.1	Call Routing Overview.....	105
7.2.1.2	Provisioning	105
7.2.1.3	Extension Numbering in the Avaya Dial Plan.....	107
7.2.1.4	Understanding the Endpoints Count on System Status.....	107
7.2.2	Configuring EGW for the Avaya Communications Manager.....	107
7.3	Configuring Avaya Session Manager.....	110
7.3.1	Understanding How the EGW works with Avaya Session Manager Deployments	110
7.3.1.1	Call Routing Overview.....	110
7.3.1.2	Provisioning	111
7.3.1.3	Extension Numbering in the Avaya Dial Plan.....	113
7.3.1.4	Understanding the Endpoints Count on System Status.....	113
7.3.2	Configuring EGW for the Session Manager	113
7.4	Configuring Microsoft Skype for Business Server Deployments.....	117
7.4.1	Understanding How the EGW Works with Microsoft Skype for Business Server Deployments.....	117
7.4.2	Device Inventory.....	119
7.4.2.1	Devices Added to EGW Device Inventory	119
7.4.2.2	HELD PBX Preferences	120
7.4.2.3	HELD Request.....	120
7.4.2.4	Understanding the Endpoints Count on System Status.....	121
7.4.2.5	Callbacks	122

7.4.3	Configuring EGW for Microsoft Lync	122
7.5	Configuring ShoreTel Settings.....	125
7.5.1	Understanding How the EGW Works with ShoreTel	125
7.5.1.1	Provisioning	126
7.5.1.2	Understanding the Endpoints Count on System Status.....	127
7.5.2	Configuring the EGW for the ShoreTel	128
7.6	Configuring Generic IP-PBX Settings	131
7.6.1	Automatic Phone Inventory.....	135
7.7	Configuring Aastra Clearspan	135
7.7.1	Understanding how the EGW works with Aastra Clearspan	135
7.7.1.1	Call Routing Overview.....	135
7.7.1.2	Provisioning	136
7.7.1.3	Understanding the Endpoints Count on System Status.....	138
7.7.2	Configuring the EGW for the Aastra Clearspan	138
7.8	Configuring Lync for MSE	141
7.8.1	Call Routing Overview.....	141
7.8.2	Dashboard Configuration.....	142
8	CONFIGURING ALERTING, NOTIFICATION.....	143
8.1	Configuring Mail Server Settings	143
8.2	Configuring SNMP Traps Settings	144
8.2.1	Configuring the SNMP Trap Receiver Settings.....	144
8.2.2	Authentication	145
8.2.2.1	SNMP Version 3	145
8.2.2.2	Sending a Test Trap Notification.....	145
8.2.3	Configuring the Scheduled Task.....	146
8.3	Alarms.....	146
8.3.1	Alarm Reporting.....	146
8.3.1.1	Alarm Reporting Mechanism	146
8.3.2	Alarms Frequency Settings	147
8.3.2.1	Understanding Alarm Notification Frequency Settings	147
8.4	Configuring Crisis Alerts	149
8.4.1	Crisis Alert Email Settings	149
8.5	Configuring Unprovisioned Call Alerts	150
8.5.1	Unprovisioned Alert Email Settings	150
8.6	Configuring Off-Campus Call Alerts.....	151
8.6.1	Off-campus alert email settings.....	151
8.7	Customize Address.....	152
8.7.1	Multiline Address Template.....	152
8.7.1.1	Multiline Address Template Example:.....	153
8.7.2	Single Line address template	153
8.7.2.1	Single Line Address Template Example	154

8.8 Configuring Desk Alert	154
9 ADVANCED SETTINGS	155
9.1 Global Settings Screen	155
9.1.1 Changing the Time Zone	159
9.1.2 Configuring Timer Settings	159
9.1.3 Batch Settings	160
9.1.4 Redundancy Settings	160
9.1.4.1 Modifying Task Redundancy Status.....	161
9.1.4.2 Setting Task Dependencies	161
9.1.5 SOAP Server	161
10 TASK SCHEDULER.....	163
10.1 Configuring the Task Scheduler Time of Day Settings.....	165
10.1.1.1 Run Now	166
10.1.2 Scheduled Reporting.....	166
11 EMERGENCY RESPONSE LOCATIONS (ERLs)	167
11.1 Understanding Emergency Response Locations (ERLs)	167
11.1.1 Establishing Enterprise ERLs	167
11.1.2 EGW ERL Settings.....	167
11.1.3 Assigning ERLs to the Network	168
11.1.4 Assigning ERLs to IP subnets.....	168
11.1.5 ERL Maintenance	168
11.2 Provisioning ERLs	168
11.2.1 Deletion Restrictions.....	169
11.2.2 Dashboard Interface	169
11.2.2.1 ERL Page.....	169
11.2.2.2 Add ERL Page	170
11.2.2.3 URL Template Editor	175
11.2.3 Batch File Processing	178
11.2.3.1 ERL Batch File Processing Mechanism	178
11.2.4 FTP	179
11.2.5 SOAP interface	179
11.3 ERL Batch File Format.....	179
11.3.1 US/Canada ERL Batch File Format	180
11.3.2 Dynamic ELIN Management	184
11.3.2.1 Dynamic ELIN Management Example.....	185
11.3.3 Worldwide Mode Batch File Format.....	185
11.3.4 ERL Batch Logs	188
11.3.4.1 Log File	188
11.3.4.2 Error Log File	188
11.3.5 ERL Batch Results	189
11.4 Exporting/Backing Up ERLs.....	193

12 ENDPOINTS	194
12.1 Understanding Endpoints.....	194
12.1.1 Phone Discovery	194
12.1.2 Phone Tracking	194
12.1.3 Unprovisioned Phones (Call Center Mode)	195
12.2 Provisioning Endpoints.....	195
12.2.1 Dashboard.....	195
12.2.1.1 Endpoints Page	195
12.2.2 Batch Files.....	197
12.2.2.1 Endpoint Batch File Processing Mechanism	197
12.2.3 FTP	198
12.2.4 SOAP	198
12.2.5 Endpoint Batch File Format	198
12.2.6 Endpoint Batch Logs	201
12.2.6.1 Log File	201
12.2.6.2 Log Error File	201
12.3 Exporting/Backing Up Endpoints	204
12.4 Call History (CDRs)	204
13 LAYER 2 DISCOVERY.....	206
13.1 Switch Requirements for EGW	206
13.2 Understanding How Layer 2 Discovery Works.....	207
13.2.1 EGW Scans	207
13.2.2 3rd Party Scanning	207
13.2.3 The Layer 2 Discovery Scan Manager	207
13.2.4 Automatic Phone Inventory.....	208
13.2.5 How Does the EGW assign ERLs to Endpoints Using Layer 2 Discovery	208
13.2.5.1 Unprovisioned/Call Center	208
13.3 Interconnected/Cascaded Switches.....	208
13.3.1 Understanding How the EGW Supports Interconnected Switches.....	208
13.3.1.1 Port Types	209
13.3.2 Provisioning the EGW with Interconnected Switches	209
13.3.3 Voice VLAN Options	211
13.4 Configuring Layer 2 Discovery	211
13.4.1 Global.....	212
13.4.1.1 Configuring Automatic Phone Inventory	213
13.4.2 Switch Identification	214
13.4.2.1 SNMP Version 3	215
13.4.2.2 Assigning ERLs to Specific Ports on a Switch.....	215
13.4.3 Provisioning Switches in a Batch.....	216
13.4.3.1 Dashboard.....	216
13.4.3.2 FTP	216
13.4.4 Batch File Format.....	217
13.4.4.1 CSV batch file format	217
13.4.4.2 Structural Restrictions	219

13.4.5 Batch Logs.....	220
13.4.5.1 Batch Log Error Codes.....	220
13.4.6 Text batch file format	221
13.5 Scans	224
13.5.1 Scan Jobs.....	224
13.5.2 Creating a Job Manually.....	225
13.5.3 About Layer 2 Discovery Logging.....	225
13.5.4 Creating a Layer 2 Discovery Scheduled Task	226
13.6 3rd Party Scanning	226
13.6.1 Loading 3 rd Party Scanning Data	226
13.6.1.1 Dashboard.....	226
13.6.1.2 FTP	227
13.6.1.3 SOAP	227
13.6.2 3rd Party Scan Batch File Format.....	227
13.6.2.1 Batch Logs for External Scan.....	228
13.6.3 Discovered Ports	229
13.6.3.1 MAC Results.....	229
13.7 Export Layer 2 Switch Details	230
13.8 Troubleshooting Layer 2 Discovery.....	230
13.8.1 Undiscovered Switch Ports	230
13.8.2 Undiscovered Phones	230
13.8.3 Endpoint gets associated to wrong location.....	231
14 LAYER 3 DISCOVERY.....	232
14.1 Understanding Layer 3 Discovery	232
14.2 Provisioning Subnets.....	232
14.2.1 Provisioning Subnets Individually	232
14.2.2 Provisioning Subnets in a Batch.....	232
14.2.2.1 Subnet Batch File Processing Mechanism.....	233
14.2.2.2 Batch File Format.....	233
14.2.3 Layer 3 Batch Logs	234
14.2.3.1 Log File	234
14.2.3.2 Error Log File	235
14.2.3.3 Response Codes	235
14.3 Export Layer 3 Discovery Details.....	236
15 WLAN DISCOVERY	237
15.1 WLAN Scanning and WLAN Discovery Mechanism	237
15.1.1 WLAN Discovery Task	238
15.1.2 Understanding WLAN Discovery and Layer 2 Discovery Interactions.....	238
15.2 Setting Up the Network for WLAN Discovery.....	239
15.2.1 Controlling Access Point Scanning	239
15.2.2 Support for Cisco Mobility Services Engine (MSE).....	239

15.2.3	Support for Aruba AirWave	243
15.2.3.1	Network Configuration	243
15.2.4	Support for Aruba ALE	245
15.3	Provisioning WLAN Discovery.....	248
15.3.1	WLAN Discovery Global Configuration	248
15.3.2	Provisioning Controllers and Access Points Individually.....	249
15.3.2.1	Add Access Point.....	250
15.3.3	Provisioning Controllers and Access Points in a Batch	251
15.3.3.1	Batch File Processing Mechanism.....	251
15.3.4	Batch File Format.....	251
15.3.4.1	Text format for Batch File	252
15.3.4.2	CSV format for Batch File.....	254
15.3.5	WLAN Discovery Batch Logs	257
15.3.5.1	Log File	257
15.3.5.2	Error Log File	258
15.3.6	Adding Location Servers	262
15.3.7	Wireless Infrastructure Maintenance Using the Dashboard	262
15.4	Export WLAN Discovery Details	263
15.5	Troubleshooting WLAN Discovery	263
15.5.1	Accuracy of ERL Assignment to the Access Switches.....	263
15.5.2	WLAN Discovery and Layer 2 Discovery Interactions	263
16	NENA 2 PROVISIONING.....	264
16.1	Overview of NENA 2 Files.....	264
16.2	Understanding the EGW's NENA 2 Feature	264
16.2.1	NENA 2 ELIN Filtering.....	264
16.2.2	Cycle Counter.....	265
16.2.3	NENA 2 Reports	265
16.3	EGW Configuration for NENA 2 Feature.....	265
16.3.1	Configuring NENA 2 Fields	265
16.3.1.1	NENA 2 ELIN Filtering.....	267
17	PROVISIONING OFF-CAMPUS USERS	268
17.1	Overview of Support for Off-campus Users	268
17.2	RLM Settings.....	268
17.2.1	RLM Proxy Uplink Settings.....	269
17.2.2	RLM Disclaimer	270
17.3	Understanding On-site and Off-site Provisioning	270
17.4	Configuring the Network for Off-Campus Users	271
17.4.1	Configuring the SOAP API	271
17.4.2	Configuring the Remote Location Manager (RLM) for IP Hardphones.....	271
17.4.2.1	Cisco.....	271

17.4.2.2	Avaya	272
17.5	Mobile and Remote Access	272
18	SYSTEM STATUS	273
18.1	Overview	273
18.2	System Status Overview.....	273
18.2.1	General Information	273
18.2.2	Routepoint Status	274
18.2.2.1	Reset CTI	274
18.2.3	Last 12 Months Endpoints Peak Reported.....	275
18.2.4	Database Synchronization	275
18.2.5	Search Layer 3.....	275
18.2.6	View Switches	275
18.2.7	View WLAN Controllers and Access Points.....	275
18.3	Logs	276
18.3.1	Configuration Logs	276
18.3.2	Alarms Logs.....	276
18.3.3	EGW Debug Logs.....	277
18.3.3.1	About EGW Application Logs	277
18.3.3.2	Additional Logs	278
18.3.3.3	Generate Debug Logs.....	278
18.4	Reports.....	279
18.4.1	ERL Reports	279
18.4.2	Endpoint Reports	280
18.4.3	Subnets	282
18.4.4	Switches and Ports.....	282
18.4.5	NENA 2 Reports	283
18.4.6	WLAN and Access Point Reports.....	283
18.4.7	User Reports	283
18.5	Call Detail Records	283
18.5.1	Call Destination	285
18.5.1.1	CDRs and the EGW Dial Plan.....	285
18.5.2	CDR Export to FTP	285
18.5.2.1	Export CDR File Types	285
18.5.2.2	Accessing Records by FTP	287
18.6	Alarms	287
18.6.1	Clearing Alarms	288
18.6.1.1	Clearing Individual Alarms	288
18.6.1.2	Clearing Multiple Alarms	288
19	MAINTENANCE	289
19.1	Server Maintenance.....	289
19.2	Network Settings	290

19.2.1	Replication Setup	292
19.2.2	Deactivate EGW	292
19.2.3	Grace Mode	292
19.2.4	Inactive Mode	292
19.3	Upgrade EGW	293
19.3.1	Requirements	293
19.3.1.1	Backup	293
19.3.2	Upgrade Procedure.....	294
19.3.2.1	Results of the Upgrade	294
19.3.3	Post Upgrade Procedure.....	295
19.3.3.1	Log File	295
19.4	Help.....	296
20	EGW ALARMS	297
20.1	EGW Application Alarms by Module.....	297
20.1.1	AXL.....	297
20.1.1.1	Special Considerations.....	299
20.1.2	Configuration	300
20.1.3	CTI	301
20.1.4	Dashboard.....	302
20.1.5	Discovery	302
20.1.6	Monitoring.....	305
20.1.7	Routing.....	315
20.1.8	Scheduler	318
20.1.9	System Status.....	319
21	GLOSSARY	324
22	APPENDIX A.....	327
22.1	Legacy batch file format for ERLs.....	327
22.1.1	Dynamic ELIN Management	329
22.1.2	ERL Batch Logs	330
23	APPENDIX B.....	332
23.1	All Supported Countries for WWE EGW	332
23.2	Country Specific Validation Requirements.....	337
23.2.1	Regular Expressions for Country-Specific Validations	343
24	APPENDIX C: EGW PROPRIETARY MIB REFERENCE.....	346

1 Introduction

1.1 About this Guide

This guide provides information to help 911 administrators plan, configure, and maintain an Emergency Gateway (EGW) deployment. It describes E911 concepts, common network topologies, and deployment scenarios.

1.2 Audience

This guide is for the 911 administrator who will work with network and telephony administrators to install, configure, and maintain the E911 system.

Network and telephony personnel should read the document “Emergency Gateway Appliance Standard Operating Procedures.”

1.3 Customer Support

Intrado hardware support policies provide comprehensive telephone, email, and web-based support for the EGW hardware appliance. For more information, see the document “West Safety Services Support Policy”. This document provides details on using all of the support resources—from calling the Network Operations Center (NOC) to accessing the Technical Resource Center (TRC) website. The document also includes EGW hardware support policies and lists the procedural steps to be followed when obtaining support.

1.4 Conventions

In procedures, interface terminology appears in bold type. For example,

- If the displayed action is **View Peer**, the administrator must log in to the peer gateway to view the log file.

Command paths are indicated using the symbol >. For example,

- An IP-PBX may be added to the system by selecting **Configuration > IP-PBX > Add a New IP-PBX**.

Important: Indicates important information which is integral to the proper configuration of your EGW or phone system. Failure to follow these notes or warning instructions may result in the improper or incomplete configuration of the 911 system.

Note: Indicates important information which will help you to configure your EGW or phone system.

1.5 References

The documents listed below provide additional information that may be of use. Product related technical documentation is available from your account manager. Items followed by an asterisk (*) are available from the respective vendor’s website.

- *EGW Networking Interface Description*
- *Administrator Guide for Avaya Communication Manager**
- *Cisco Call Manager Administration Guides*
- *ShoreTel Application Note for Emergency Gateway*
- *EGW Appliance Standard Operating Procedures*
- *West Safety Services Support Policy*
- *Configuring the Avaya Communication Manager for the EGW Appliance*
- *Microsoft Skype for Business EGW Configuration Guide*
- *Addendum to Using DRAC with Windows Active Directory*
- *Avaya Communication Manager Application Notes: Emergency Calling**

- *SOAP Server Interface Description Document*
- *EGW Configuration Worksheet*
- *Desk Alert Administrator User Guide*
- *NENA Standard Data Formats for ALI Data Exchange and GIS Mapping.*
- *E911 Softphone Locator (ESL) Installation and Configuration Guide*

2 Product Overview

2.1 About the Emergency Gateway

The Emergency Gateway (EGW) automates and simplifies 911 administration with features such as automatic phone discovery. The EGW also supports remote users (work-at-home employees and teleworkers) and advanced IP-PBX features such as shared line appearance and extension mobility.

The EGW is designed to support centralized IP-PBX deployments and may be integrated into a variety of network topologies and deployment scenarios. It is capable of routing emergency calls to Intrado's Emergency Routing Service (ERS) or a local exchange carrier's 911 network. The ERS is a national E911 call termination service which delivers 911 calls on priority trunks to over 6,000 Public Safety Answering Points (PSAP) across the US and Canada.

The EGW is capable of providing service internationally, when operating in Worldwide mode. Features of primary interest in Worldwide mode include on-site call delivery and notification, Desk Alert software, and call routing to local emergency responders (e.g. PSAP), depending on local service availability.

The diagrams below illustrate high level deployments in US/Canada mode and Worldwide mode.

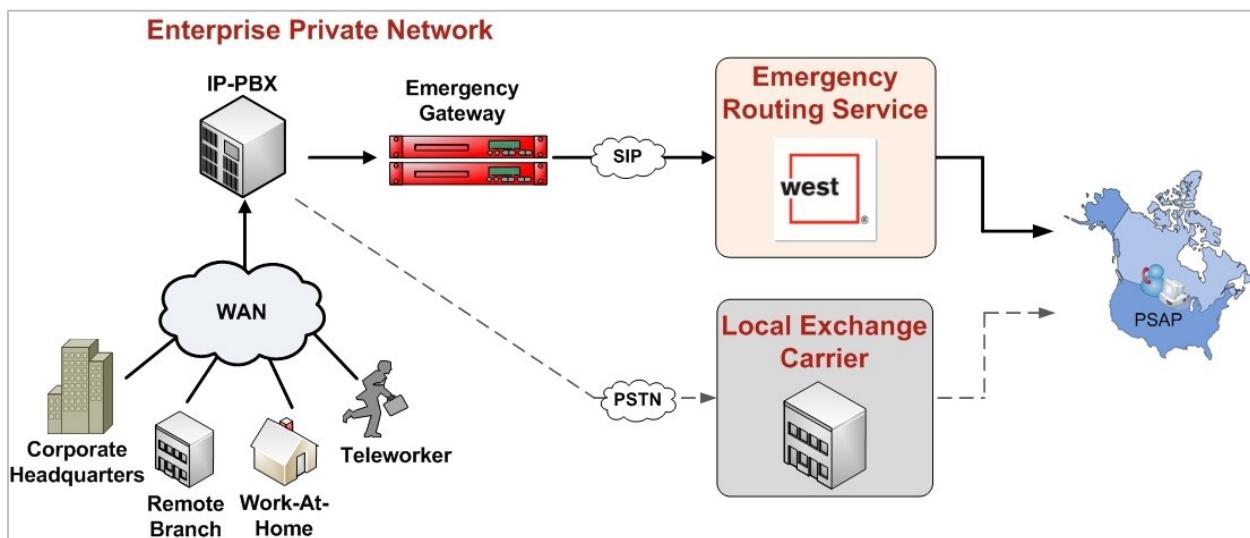


Figure 1: High Level Call Flow- US and Canada

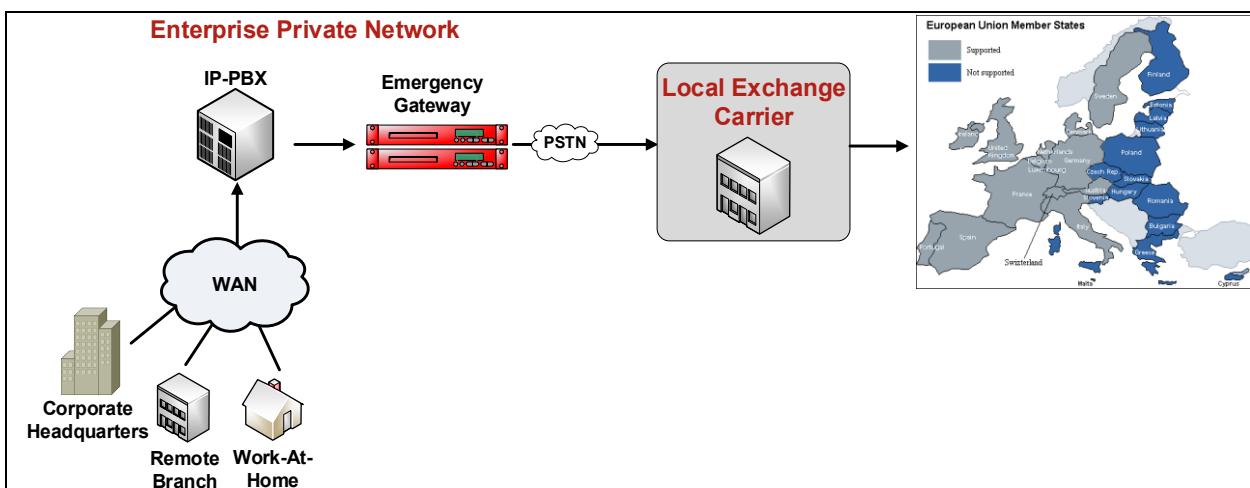


Figure 2: High Level Call Flow WorldWide Mode

2.1.1 EGW Features

Automatic Phone Tracking for Wired and Wireless IP phones/softphones

The EGW automatically tracks and assigns locations to IP phones and softphones as they move on the corporate network, using either layer 2/3 discovery, or wireless discovery. Layer 2 Discovery uses SNMP to scan network switches in order to identify the locations of IP phones. Layer 2 Discovery provides a high level of location granularity, and is the preferred discovery method for enterprises that would like to provision ERLs down to the switch/switch port level. Layer 3 Discovery, on the other hand, works by associating IP subnets to ERLs. If an enterprise has geographically assigned subnets, Layer 3 discovery is an accurate way of providing location discovery to the floor level. The EGW's WLAN Discovery feature tracks wireless IP phones and softphones, and can provide seamless discovery of phones in wireless or wired modes of operation (when used in conjunction with layer 2/3 Discovery). WLAN Discovery tracks wireless phones using the BSSID of the nearest wireless access point.

Call Routing

The EGW performs processing during an emergency call to obtain the correct location of the caller. Unique call routing policies can be configured on a per-ERL basis; based on the ERL associated with the phone, the EGW delivers the call to the appropriate destination. The following unique call routing policies can be configured:

- Emergency routing (ERS or local trunks to the PSAP)
- On-site security desk (emergency or non-emergency call)
- Test mode recording
- Security desk routing

The EGW may be configured to route calls to on-site security desks. The EGW supports two types of security desk call routing:

- Direct call delivery
- Call monitoring with optional one-way mute

In direct call delivery, the call is sent directly to the security desk or private answering point, bypassing the PSAP entirely. When call monitoring is enabled, a three-way call is routed between the security desk and the PSAP. An optional one-way mute can be configured to restrict security desk personnel from participating in the call.

Configuration of security desk routing is flexible, and the EGW supports the use of a specific number, or non-emergency number to route calls to security desks.

Multiple Dial Plan

The Emergency Gateway can support multiple route plans for both emergency and non-emergency numbers. For example, for the same enterprise location, 911 and 9911 calls can be routed to the appropriate PSAP, while 888 and 9888 calls can be routed to the appropriate security desk located in the caller's building or campus. It is also possible to support enterprise configurations that include non-emergency numbers (help desks etc.).

Identifies Caller Location at the PSAP

If an emergency call is routed to the local exchange carrier (LEC), the EGW provides the correct Emergency Location Identification Number (ELIN) for the caller, which the LEC depends on to identify the caller's location at the PSAP. If ERS call routing is used, ELINs are not required. The EGW provides station level identification for all phones, including those that do not have assigned DIDs (10-digit telephone numbers). For endpoints without DIDs, "Extension-Bind" technology dynamically assigns a callback number during a 911 call. This feature greatly reduces the amount of callback numbers that must be procured, and eliminates time-consuming ELIN management tasks altogether.

Supports Employee Mobility

The EGW provides accurate location-based call delivery to the PSAP for on-campus, off-campus and wireless IP phones and softphones. Off-campus users can self-provision locations using the Remote Location Manager (RLM). This off-site provisioning tool allows users to provision valid locations in the emergency network, and includes real-time error correction and suggested alternatives. Once on-site, location tracking is completely transparent to

users: The E911 Softphone Locator (ESL) provides automatic tracking of Windows-based IP softphone and works in the background to continuously update the EGW with the required provisioning data. On-site IP hard phones are automatically discovered and tracked by the EGW using layer 2 or layer 3 discovery. Wireless phones are supported using WLAN Discovery, allowing phones to seamlessly move between wireless and wired modes of operation: If a phone is in wireless mode, it can be picked up by the next WLAN scan, or ESL push. If it is in wired mode, it can be discovered using layer 2/3 discovery.

Administrative Dashboard

The EGW can be administered using a web interface Dashboard. The Dashboard is used to upload and process batch files, in order to provision the EGW with endpoints, ERLs, layer 2 switches, subnets, and other parameters.* In addition to provisioning, the EGW provides in-depth system status information, logs, reports, call detail records, and call recordings via the administrative Dashboard.

*These parameters may also be provisioned using the EGW's ftp server.

Call Alerting and Notification

The EGW provides extensive call alerting and notification capabilities. The EGW can notify personnel using the following methods:

- Crisis alerts
- Unprovisioned call alerts
- Off-campus call alerts
- Desk Alert notifications

The EGW is capable of sending crisis alerts via email, SMS, or pager. This feature enables notifications to be sent to patrolling personnel or off-campus staff, and helps organizations to better coordinate response efforts. The alerts can also be sent as SNMP traps to management stations, such as a network management system (NMS).

The Desk Alert application is installed on security desk workstations, and allows pop-up notifications and audible alarms to be sent to on-site personnel when 911 is dialed.

For both crisis alert emails and Desk Alerts, a URL link to a campus map or corporate database may be included with the notification.

Worldwide Mode (WW mode):

The EGW is also capable of operation in Worldwide mode. For a complete list of countries, the EGW supports, please go to *All Supported Countries for WWE EGW*.

When the EGW is deployed in Worldwide mode, the following features are supported:

- Onsite call delivery and notification (security desk/private answering point routing and notification)
- Local trunking to the local emergency services provider
- Desk Alert (security desk notification and alerting software)

Hardware or Virtual Appliance

The EGW is available as either a hardware appliance deployed in redundant pairs, or as a redundant virtual appliance, deployed on customer-provided hardware. In either case, the appliances can be deployed in geographically diverse data centers for greater redundancy.

The EGW virtual appliance is a pre-integrated, unified offering that contains both the underlying OS and EGW application stack. The virtual appliance is now available for VMWare ESX platforms.

2.2 Emergency Gateway Specifications

2.2.1 Software Specifications

Table 1: EGW Software Specifications

Operating System	<ul style="list-style-type: none"> • Security-Hardened Enterprise Linux
Supported IP-PBX Systems	<ul style="list-style-type: none"> • Cisco Unified Communications Manager • Avaya Communications Manager • Avaya Aura Session Manager • Microsoft Skype for Business Server, • Microsoft Phone System Direct Routing • Mitel MiVoice Connect ONSITE, Clearspan • Voalte Platform • Generic SIP PBX systems
Mobile and Remote Access	<ul style="list-style-type: none"> • Cisco Expressway
Telephony	<ul style="list-style-type: none"> • Signaling Protocols: SIP/UDP, H.323/UDP • Payload: RTP/UDP, G.711 • Capacity: 20 concurrent calls
Layer 2 Discovery	<ul style="list-style-type: none"> • Protocols: SNMP v1, SNMP v2c, SNMP v3 • Capacity: Up to 5000 switches • Supported Switches: <ul style="list-style-type: none"> ◦ Cisco Catalyst ◦ HP Procurve ◦ Dell PowerEdge and PowerConnect ◦ Juniper EX ◦ Extreme Networks Summit, BlackDiamond, and Alpine ◦ Brocade FastIron ◦ Phybridge Uniphyer and PoLRE ◦ All other switches that support Bridge MIB (RFC 1493), Q-Bridge MIB and IF-MIB • Real-time scanning progress report available on EGW Dashboard • Automatic endpoint inventory • Supports third-party scanning tools with batch file interface
Layer 3 Discovery	<ul style="list-style-type: none"> • Supported Protocols: IPv4
Wireless LAN Discovery	<ul style="list-style-type: none"> • Protocols: SNMP v2c, SNMP v3 • Supported Infrastructure: <ul style="list-style-type: none"> ◦ Cisco ◦ Aruba
Capacity	<ul style="list-style-type: none"> • Maximum ERLS: 500,000 • See vendor specifications for maximum endpoints • Maximum number of IP-PBX servers: 64
Alerting Capabilities	<ul style="list-style-type: none"> • Crisis Alert Email – includes time, location, and callback number of caller • Security Desk Direct Call Delivery • Three-way call monitoring with PSAP (includes mute/unmute capabilities) • Pop-up screen (requires Desk Alert software)

Redundancy	<ul style="list-style-type: none"> • Deployed in redundant pairs • Active/Active Mode • Load Balancing Mode
Reporting	<ul style="list-style-type: none"> • Call Detail Records – includes location data information, exportable as CSV or flat text file • Call Recording (.wav file format) • Emergency Response Location Reports • Endpoint Status Reports • Test Call status • NENA 2 report generation with ELIN filtering options
Call Recording Capacity	The size available to the CDR recordings is 10% of the entire hard drive capacity. On a hard drive with a 300 GB capacity, the CDR recordings would take 30 GB, meaning approximately 31,000 call minutes = 512 hours.
Provisioning	<ul style="list-style-type: none"> • Real-time Address Validation Tool (requires ERS) • ERL/Endpoint/Layer 2 and 3/Wireless using Batch, API and Dashboard • Analog/Digital phones • Remote Location Manager (RLM) module for off-site users (requires ERS)
Off-site User Tracking	<ul style="list-style-type: none"> • Updates the off-site user location in real-time • Requires Remote Location Manager • Requires Emergency Routing Service (ERS) • See vendor specifications below for supported endpoints
Operation and Maintenance	<ul style="list-style-type: none"> • Email alerts and alarms • Syslog support • Active monitoring • SNMP v2c/v3 traps • Test mode (standalone and ERS end-to-end) • Web-based management interface • Pre-configured user access levels • Support for LDAP for Microsoft Active Directory
Additional Features	<ul style="list-style-type: none"> • Mis-dial protection • Integration with PS-ALI systems • Support for multiple dial plans • Transparent NAT traversal • Configurable digit manipulation for incoming DIDs • Callback support for users without a DID

2.2.1.1 Support for Cisco

Table 2: Support for Cisco

Supported Cisco versions	<ul style="list-style-type: none"> • Cisco Unified Communications Manager 11.x, 12.x • Cisco Expressway for Mobile Remote Access X8 or newer
---------------------------------	--

Layer 2 Discovery	Supported Cisco Phones: <ul style="list-style-type: none"> • All Unified IP phones (except 3911) • All Unified IP Conference Stations • IP Communicator • Jabber 11.x, 12.x for (Windows and macOS) • Webex Teams
Layer 3 Discovery	Supported Cisco Phones: <ul style="list-style-type: none"> • All Unified IP phones (except 3911) • All Unified Wireless IP Phones • All Unified IP Conference Stations • IP Communicator • Jabber 11.x, 12.x (Windows and macOS) • Webex Teams
Wireless LAN Discovery	Supported Cisco Phones: <ul style="list-style-type: none"> • Wireless IP Phone 792x series • IP Communicator • Jabber 11.x, 12.x (Windows and macOS) • Webex Teams
Maximum Endpoints	<ul style="list-style-type: none"> • 120,000
Remote Location Manager (RLM)	Supported Cisco Phones: <ul style="list-style-type: none"> • Unified IP phones 7940 and above • IP Communicator • Jabber 11.x, 12.x (Windows and macOS) • Webex Teams

2.2.1.2 Support for Mitel

Table 3: Support for Mitel

Supported Mitel versions	<ul style="list-style-type: none"> • MiVoice Connect ONSITE • Clearspan
Layer 2 Discovery	Supported MiVoice Connect Phones: <ul style="list-style-type: none"> • All IP hard phones • Connect Softphone Client (Windows)
Layer 3 Discovery	Supported MiVoice Connect Phones: <ul style="list-style-type: none"> • All IP hard phones • Connect Softphone Client (Windows)
Wireless LAN discovery	Supported MiVoice Connect Phones: <ul style="list-style-type: none"> • Connect Softphone Client with ESL (Windows)
Maximum Endpoints	<ul style="list-style-type: none"> • 120,000
Additional Information	<ul style="list-style-type: none"> • ShoreTel Edge Gateway is not supported
Remote Location Manager	Supported MiVoice Connect Phones:

	<ul style="list-style-type: none"> • Connect Softphone Client (Windows)MiTel MiVoice Connect
--	---

2.2.1.3 Support for Avaya

Table 4: Support for Avaya

Supported Avaya versions	<ul style="list-style-type: none"> • Avaya Communication Manager 7.x, 8.x • Avaya Aura Session Manager 7.x, 8.x
Layer 2 Discovery	<p>Supported Avaya Phones:</p> <p>H.323:</p> <ul style="list-style-type: none"> • 1608, 1616 firmware r1.0 and above • 4610SW, 4620 firmware r1.8 and above • 620SW, 4621SW, 4622SW firmware r2.2, 2.5 and above • 4625SW firmware r2.5 and above • 9608, 9611G, 9621G, 9641G firmware r6.0 and above • 9610 firmware r1.2 and above • 9620, 9630, 9639G, 9640, 9640G, • 9650 firmware r1.0 and above • 9620L, 9620C, 9650C, 9650L firmware 3.0 and above • 9670G firmware 2.0 and above <p>SIP:</p> <ul style="list-style-type: none"> • 9620, 9630, 9630G, 9640, 9640G firmware r2.2, 2.5 and above • 9620L, 9620C, 9650, 9650C firmware r2.5 and above • 9608, 9611G, 9621G, 9641G firmware r6.0 and above • IP Softphone R5.x and above (Windows) • One-X Communicator R5.21 and above (Windows) • One-X Agent R2.0 and above (Windows) • Equinox 3.x for Windows

Layer 3 Discovery	<p>Supported Avaya Phones:</p> <p>H.323:</p> <ul style="list-style-type: none"> • 1608, 1616 firmware r1.0 and above • 4610SW, 4620 firmware r1.8 and above • 4620SW, 4621SW, 4622SW firmware r2.2, 2.5 and above • 4625SW firmware r2.5 and above • 9608, 9611G, 9621G, 9641G firmware r6.0 and above • 9610 firmware r1.2 and above • 9620, 9630, 9639G, 9640, 9640G, 9650 firmware r1.0 and above • 620L, 9620C, 9650C, 9650L firmware 3.0 and above 9670G firmware 2.0 and above <p>SIP:</p> <ul style="list-style-type: none"> • 9620, 9630, 9630G, 9640, 9640G • firmware r2.2, 2.5 and above • 9620L, 9620C, 9650, 9650C firmware r2.5 and above • 9608, 9611G, 9621G, 9641G firmware r6.0 and above • IP Softphone R5.x and above (Windows) • One-X Communicator R5.21 and above (Windows) • One-X Agent R2.0 and above (Windows) • Equinox 3.x for Windows
Wireless LAN Discovery	<p>Supported Avaya Phones:</p> <ul style="list-style-type: none"> • IP Wireless Phones 3631, 3641, 3645 • IP Softphone R5.x and above (Windows) • One-X Communicator R5.21 and above (Windows) • One-X Agent R2.0 and above (Windows) • Equinox 3.x for Windows
Maximum Endpoints	<ul style="list-style-type: none"> • 40,000 • 80,000 with load balancer
Remote Location Manager (RLM)	<p>Supported Avaya Phones:</p> <ul style="list-style-type: none"> ○ 4610SW, 4620/4620SW, 4621SW, 4622SW, 4625SW ○ 9620/9620C/9620L, 9630/9630G, 9640/9640G, 9650/9650C, 9670G ○ IP Softphone R5.x and above (Windows) ○ One-X Communicator R5.21 and above (Windows) ○ One-X Agent R2.0 and above (Windows) ○ Equinox 3.x for Windows

2.2.1.4 Support for Microsoft

Table 5: Support for Microsoft

Supported Microsoft versions	<ul style="list-style-type: none"> ○ Skype for Business Server 2015, 2019 ○ Teams Direct Routing
-------------------------------------	--

Layer 2 Tracking	<ul style="list-style-type: none"> • Teams Direct Routing <ul style="list-style-type: none"> ◦ All Microsoft certified Teams clients • Supported Skype for Business Server <ul style="list-style-type: none"> ◦ Windows and macOS Skype Client ◦ Windows and macOS Teams client • Certified Microsoft Skype for Business devices <ul style="list-style-type: none"> ◦ Aastra 6721ip, 6725ip ◦ Polycom CX500, CX600, CX700 ◦ Polycom VVX500 ◦ Snom 300 UC edition, 821 UC edition, 370 UC edition
Layer 3 Tracking	<ul style="list-style-type: none"> • Teams Direct Routing <ul style="list-style-type: none"> ◦ All Microsoft certified Teams clients • Supported Skype for Business Server <ul style="list-style-type: none"> ◦ Windows and macOS Skype Client ◦ Windows and macOS Teams client • Certified Microsoft Skype for Business devices <ul style="list-style-type: none"> ◦ Aastra 6721ip, 6725ip ◦ Polycom CX500, CX600, CX700 ◦ Polycom VVX500 ◦ Snom 300 UC edition, 821 UC edition, 370 UC edition
Wireless LAN Tracking	<ul style="list-style-type: none"> • Teams Direct Routing <ul style="list-style-type: none"> ◦ All Microsoft certified Teams clients • Supported Skype for Business Phones: <ul style="list-style-type: none"> ◦ Windows and macOS Skype Client • Qualified or Optimized for Microsoft Lync devices: <ul style="list-style-type: none"> ◦ Polycom SpectraLink 8440, 8450, 8452
Maximum Endpoints	<ul style="list-style-type: none"> • 60,000 • 120,000 with load balancer

2.2.2 Hardware Specifications

Table 6: Hardware Specifications

Primary Processors	<ul style="list-style-type: none"> • 2 Intel(R) Xeon(R) CPU E5-2609 v3 @ 1.90GHz
Number of Cores per Processor	<ul style="list-style-type: none"> • 6
Memory	<ul style="list-style-type: none"> • 8GB DDR3 DIMM 2133 MT/s **
Hard Drive	<ul style="list-style-type: none"> • 300 GB, SAS, 3.5-inch, 10K RPM Hard Drive, configured in RAID 1 ***
Network Adapter	<ul style="list-style-type: none"> • 4 x 1GbE LOM
Management Network Adapter	<ul style="list-style-type: none"> • EGW Remote Management Embedded Ethernet NIC

Redundancy	<ul style="list-style-type: none"> • Deployed as an active-active pair • Can be deployed at separate data centers
Chassis Configuration	<ul style="list-style-type: none"> • Rack Chassis with Sliding Rails, Universal
Chassis	<ul style="list-style-type: none"> • 1U Rack-mountable chassis • 24.69" (62.7cm) D x 17.09" (43.4cm) W x 1.39" (4.3cm) H without bezel attached • Rack Weight 35.8 lbs (16.3 Kg) • Gray Chassis • Red front bezel • 4-post rack support with universal rails
Ports	<ul style="list-style-type: none"> • USB 2.0 ports quantity 3 • USB 3.0 ports quantity 1 • Serial ports quantity 1 • Ethernet LAN (RJ-45) ports 4
Environmental	<ul style="list-style-type: none"> • Operating Temperature: 10° C to 35° C (50° F to 95° F) • Storage Temperature: -40° C to 65° C (-40° F to 149° F) • Operating Relative Humidity (non-condensing twmax=29°C): 10% to 80% non-condensing • Maximum humidity gradient: 10% per hour, operational and non-operational conditions • Storage Relative Humidity: 5% to 95% non-condensing (twmax=38°C) • Operating Vibration: 0.26G at 5Hz to 350Hz for 2 minutes • Storage Vibration: 1.54Grms Random Vibration at 10Hz to 250Hz for 15 minutes • Operating Shock: 1 shock pulse of 41G for up to 2ms • Storage Shock: 6 shock pulses of 71G for up to 2ms • Operating Altitude: -15m to 3,048m (-50 ft to 10,000 ft) • Storage Altitude: -15m to 10,668m (-50 ft to 35,000 ft)
Power	<ul style="list-style-type: none"> • Primary power supply: 550 Watt hot-plug • Secondary power supply: 550 Watt hot-plug • Auto-switching universal 110/220 Volts
Regulatory	<ul style="list-style-type: none"> • FCC Class A • ICES Class A • CE Class A
Product Number	<ul style="list-style-type: none"> • HW911-EGWVPC - EGW hardware plus 2,500 user license • SW911-EGWALF - 2,500 additional user license • HW911-EGWRAC - Optional Management Network Adapter
Package Contents	<ul style="list-style-type: none"> • S Two (2) EGW appliances • Two (2) rack mount hardware kits • Two (2) Intrado red front bezels • Two (2) power cords
Licensing	<ul style="list-style-type: none"> • Perpetual License to run on EGW hardware • 2,500 base user license plus additional user licenses to an unlimited number of users

Maintenance and Support	<ul style="list-style-type: none"> Includes one (1) year maintenance and support
Documentation	<ul style="list-style-type: none"> EGW System Guide (Planning and Configuration) EGW Appliance Standard Operating Procedures EGW Networking Interface Description West Safety Services Support Policy

**Please note that a minimum of 8 GB of RAM is a mandatory requirement for the EGW to function properly.

***Please note that a minimum of 300 GB of hard drive space is a mandatory requirement for the EGW 5.X to be upgraded (from EGW 4.X) or installed.

2.2.3 Hardware Requirements for EGW Virtual Appliance

For information on EGW Virtual Appliance, see the document “EGW VMware ESX Host Installation Guide.”

2.3 Licensing

The EGW uses a connection to Intrado for activating and re-activating product licenses. You can also manually activate or re-activate a server license if you do not allow your EGW servers access outside the corporate network.

This section describes the following:

- EGW Server Licenses
- Activation
- Changing/ Upgrading an EGW Server license
- Feature Licenses
- Viewing the status of your EGW license

2.3.1 EGW Server Licenses

The EGW uses licenses* to control the features that apply to the EGW. The following EGW licenses are available:

*EGW licenses are granted per hardware/virtual appliance (standalone or redundant pair).

- ERS only:** 911 call routing to the ERS only. No local trunking supported
- Local trunking only:** 911 call routing to the local emergency services provider only. No ERS connectivity.
- ERS and local trunking:** Call routing to both the ERS and local emergency services provider
- Trial:** One of the above licenses with applicable time restriction.

Note: In Worldwide mode, the EGW currently only supports local trunking (no ERS).

2.3.2 Activation

The EGW server license can be activated automatically using a connection to Intrado, or you can use a manual activation process.

2.3.2.1 Automatic Activation

The first run activation will prompt you for your networking settings and EGW software license key. When you click on Activate, the EGW will attempt to communicate with Intrado’s licensing server. Provided that there are no problems with your license, your license will be validated and the Dashboard login screen will be displayed.

For more information about first run configuration/activation, see section 4.2 “First Run Configuration/Activation.”

For more information about logging into the Dashboard see section 4.3 “Web-Based Dashboard.”

2.3.2.2 Manual Activation

If you do not allow your EGW servers to connect outside of the corporate network you can manually activate the EGW.

To manually upgrade the EGW

1. Click on **Manual Activation**.
2. Copy the key displayed in the **Manual Activation Authentication** screen.
3. Provide this key to your Intrado support technician.
4. Obtain the Activation code from Intrado.
5. Paste the activation code into the appropriate field on the **Manual Authentication** screen.
6. Click **OK**.

2.3.3 Changing/Upgrading an EGW Server License

If you would like to change the EGW license type, you will need to deactivate your EGW and perform a re-activation. You will also need to inform your Intrado account representative that you would like to change/upgrade your license. The upgraded license will be applied to the Intrado licensing server.

To re-activate (change/upgrade) an EGW sever license

1. Login to the administrative Dashboard
2. Click on **System Status>Maintenance>Network Settings>Deactivate EGW**
3. Click on **Deactivate EGW**. Your EGW will be de-activated and you will be prompted to re-activate
4. Click on **Reactivate** to re-activate via the ERS, or click on **Manual Activation** to re-activate manually
5. If the ERS licensing server is correctly provisioned, your new EGW license will be activated.

2.3.4 Feature Licenses

If you would like to add additional features to your existing EGW license, such as Desk Alert or support for additional endpoints, you can use the Feature activation screen on the Dashboard.

To enable a feature, you need to copy the feature activation code into the Feature Activation screen and click on **Activate**. Provided that there is nothing wrong with your feature license, the new feature will be activated.

To apply a feature license

1. Login to the administrative Dashboard
2. Click on **System Status>Maintenance>Feature Activation**
3. Paste the activation code provided by Intrado
4. Click on **Activate**

2.3.4.1 Endpoint Licensing

Endpoint licenses dictate the maximum amount of users that are allowed for the EGW service.

On the System Status screen Maximum Endpoints Allowed counters are used to track the endpoints/user licensing. However, these counters do not represent that amount of endpoints that are billed for each month. You are only billed for the monthly count of provisioned endpoints.

For more information about system status, 18.2 “System Status.”

2.3.5 Viewing the Status of a License

You can view the status of your EGW license from the Dashboard. The status information displays the version number of the EGW software, the license key number, and the **Valid until** date. If you have purchased a perpetual license, the **Valid until** date will display **Always**.

To view the status of a license

1. Log into the administrative Dashboard
2. Click on **Help>About**. The EGW License key information is displayed under **About the Emergency Gateway**

For more information concerning logging into the administrative Dashboard, see section 4.3 “Web-Based Dashboard.”

3 System Planning

This section is intended to help you shape your strategy of integrating the EGW with your current deployment. It contains descriptions of supported deployments and network topologies, to provide a thorough understanding of how the EGW may be integrated with your network. It also includes detailed planning requirements for call routing via the Emergency Routing Service (ERS) or the local exchange carrier.

3.1 How the EGW Fits Into the Network

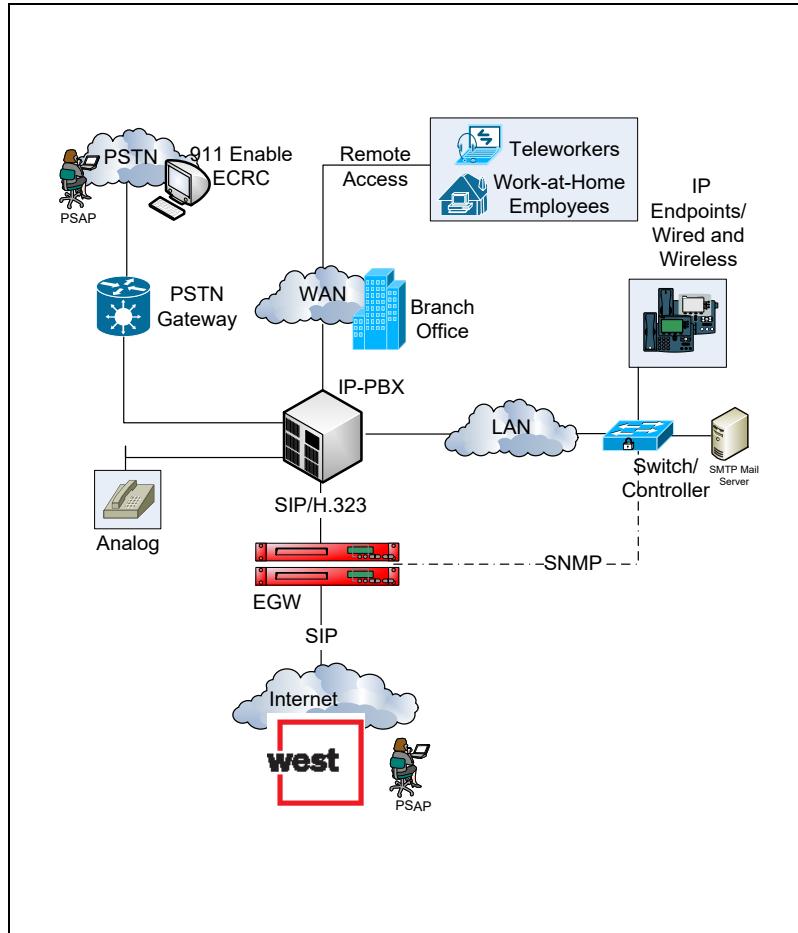


Figure 3: How does EGW Fits into the Network

The EGW handles emergency calling for the entire deployment, including branch offices, teleworkers, and work-at-home employees. Configuration of the corporate dial plan is required to send emergency traffic to the EGW. An emergency number (typically 911) can be used to send calls to the appropriate PSAP, based on the caller's location. The emergency number may also be configured to route calls to an on-site private answering point (e.g. on-site security desk). In addition to the emergency number, additional non-emergency numbers may be entered into the EGW's dial plan. These numbers can be used to route calls to on-site security desks or to test mode recordings. The test mode dial plan number is used to test the proper functioning of the EGW system.

The EGW performs call processing and retrieves the correct call route by analyzing the dialed digits (DNIS) and referencing the endpoint data to a provisioned emergency response location (ERL). The call is delivered to the appropriate destination (PSAP, security desk, local trunks, etc.) and any applicable call policies are applied (call monitor, one-way mute, Desk Alert, etc.).

The EGW can be used to deliver 911 calls to Emergency Routing Service (ERS), which provides E911 call routing to over 6,000 PSAPs across the US and Canada.* The EGW may also route calls to the local emergency network provider (e.g. the LEC that provides the local trunks).

*ERS call termination not applicable in worldwide mode.

The EGW supports automatic discovery and tracking for a variety of wired or wireless IP phones and softphones. Also, some IP softphones are supported by the E911 Softphone Locator (ESL), a service that periodically pushes phone provisioning data to the EGW. The ESL enables these softphones to be automatically tracked using layer 2, 3, or WLAN discovery. The EGW can also be provisioned with analog and digital phones using a variety of methods (e.g. batch file processing, soap interface). Third party SNMP scanning tools can also be used to populate the EGW with scanning data. The EGW can co-relate this data with the endpoints inventory and layer 2 switch information, in order to track phones connected to switches that you would not like the EGW to scan.

To implement layer 2 discovery, network switches and ports must be programmed into the EGW and associated to ERLs. The EGW then uses SNMP to associate registered phones to specific network switches and ports. When 911 is dialed, the ERL associated to the phone's current switch port is used to set up call routing to the correct destination.

To implement layer 3 discovery, the EGW is provisioned with a list of network subnets associated to ERLs. When 911 is dialed, the ERL associated to the phone's IP address is used to set up call routing to the correct destination.

To support WLAN Discovery, wireless controllers are loaded into the EGW's configuration. Wireless access points can either be automatically scanned or manually added to the configuration. Manual configuration is the preferred method for enterprises whose wireless endpoints support the E911 Softphone Locator (ESL)*. In these deployments, the ESL pushes the required provisioning data to the EGW, and there is no need to scan the access points. If the deployment includes some phones that do not support the ESL, access point scanning is enabled.

The corporate mail server may be used to send emergency alert emails to personnel when 911 is dialed. If email-based paging is set up, personnel may also be paged. The alarms and alert events can also be sent to management stations using SNMP traps.

To route emergency calls to a LEC emergency network, additional gateways and 911 trunks may be required. Call routing to the ERS eliminates these requirements.

The EGW includes a NENA 2 file generation feature, which allows location data to be exported in the appropriate NENA-valid format for upload to a LEC's PS-ALI or an on-site Private ALI. For enterprises with a Private ALI or a PS-ALI serving a single PSAP jurisdiction (single NPA-NXX), ELINs may be handled dynamically by the EGW. Using dynamic ELIN management, the EGW automatically adds and removes ELINs from ERLs as emergency locations are added, deleted or changed. This eliminates the administratively burdensome task of managing ELIN assignment to account for ERL changes.

Note: NENA 2 and dynamic ELIN features are not available in worldwide mode.

A single EGW pair can support every IP-PBX server in the deployment.

3.1.1 Network Interfaces

The EGW is equipped with internal (primary), external, and remote access controller interfaces (RAC), which can be configured based on the enterprise's deployment.

The three EGW interfaces are depicted in the diagram below:



Figure 4: EGW Hardware Appliance – Rear View

- The internal (primary) interface is labeled **1**.
- The external interface is labeled **2**.

By default, the port labeled **1** is both the “Internal” network port and the RAC port. The RAC port can be changed in the IDRAC configuration.

Each EGW server should be connected to an independent Ethernet switch, if possible, to enforce a higher degree of redundancy.

The Remote Access Controller

The EGW remote access controller (RAC) is a systems-management hardware and software solution designed to provide remote management capabilities, crashed-system recovery, and power-control functions for EGW systems. The EGW management interface may be configured to send email alerts for warnings or errors related to voltages, temperatures, intrusion, and fan speeds. It also logs event data to help diagnose the probable cause of a system crash. The management interface is pre-installed on every EGW appliance.

To learn how to configure the RAC to work with Active Directory, see the document “Addendum to Using DRAC with Windows Active Directory.”

3.2 Topology Scenarios

The following diagrams represent the preferred methods for customers to connect to the ERS.

The connectivity scenarios are presented in order of preference, with SIP Enabled Firewall as the most preferred method.

Note: For each deployment scenario a VPN connection to the ERS is optional.

3.2.1 SIP/NAT-Enabled Firewall

The SIP/NAT-enabled firewall topology has the following characteristics:

- The EGW’s Internal interface is assigned a private IP.
- The firewall performs IP/port filtering and SIP network address translation (NAT)*.

* NAT must be enabled for all SIP traffic and RTP streams between the EGW and the ERS. All packets must be re-written to use a public IP.

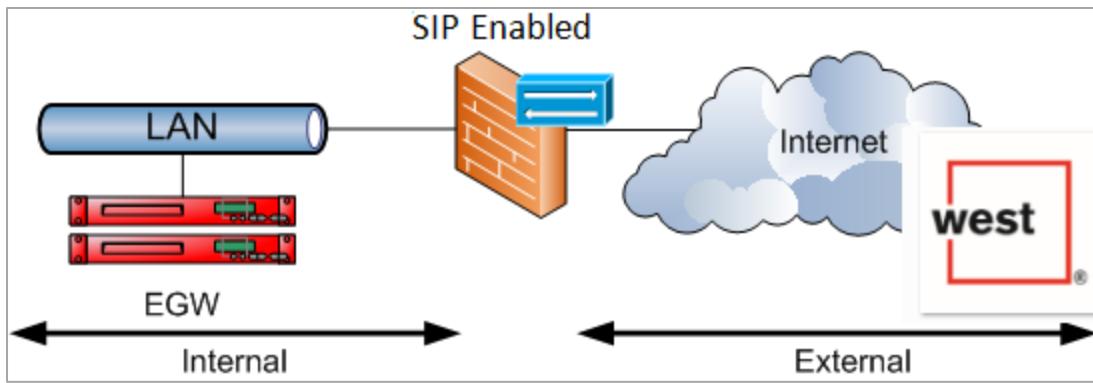


Figure 5: SIP Enabled Firewall

3.2.2 EGW Connecting via VPN Tunnel to ERS

- The EGWs are assigned private IP addresses on the internal LAN
- VPN Concentrators maintain an IPSEC VPN Tunnel between the customer network and the ERS networks
- Routes to the ERS are added to the network to pass traffic between the EGW and the ERS
- The VPN tunnel is configured with IP/Port filtering
- Note: Each EGW will require connectivity to both ERS Los Angeles and ERS New York.

This can also be established over dedicated NNI (T1) links instead of the VPN connections. If this is required, ERS New York datacenter is located at 60 Hudson New York, NY and ERS Los Angeles is located at One Wilshire in Los Angeles California.

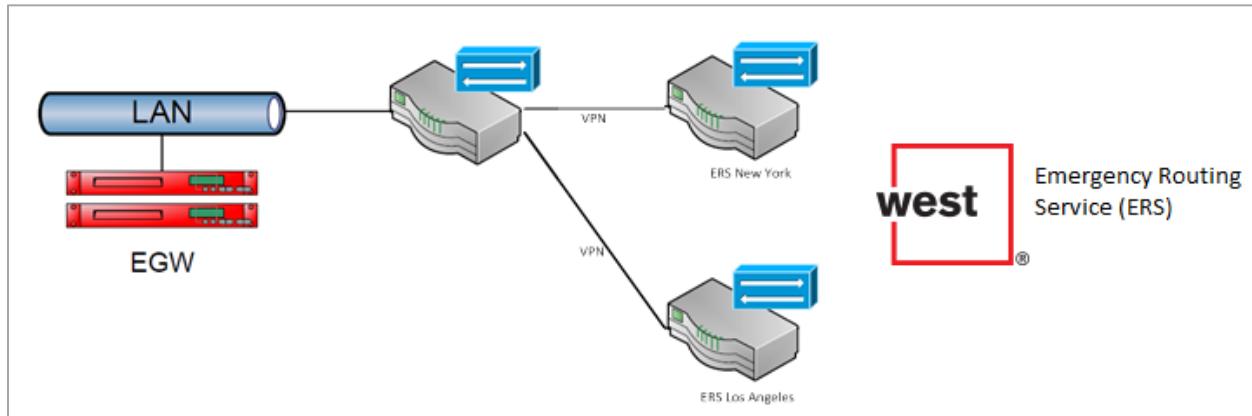


Figure 6: VPN Connection

3.2.3 SIP/NAT-Enabled Session Border Controller (SBC)

The SBC topology has the following characteristics:

- The EGW's Internal interface is assigned a private IP.
- The SBC performs IP/port filtering and NAT.

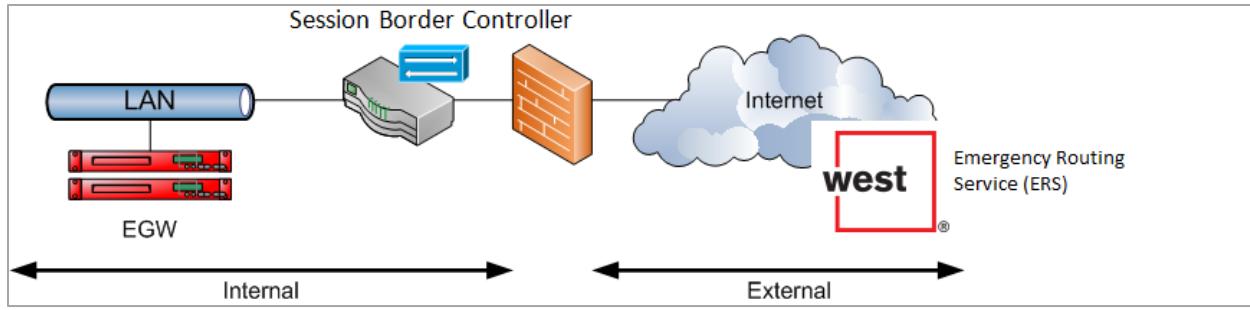


Figure 7: SIP/NAT Enabled SBC

3.2.4 EGW in SBC mode

The EGW in SBC mode has the following characteristics:

- The EGW's internal interface is assigned a private IP.
- The External interface is assigned a public IP.
- The firewall performs IP/port filtering.

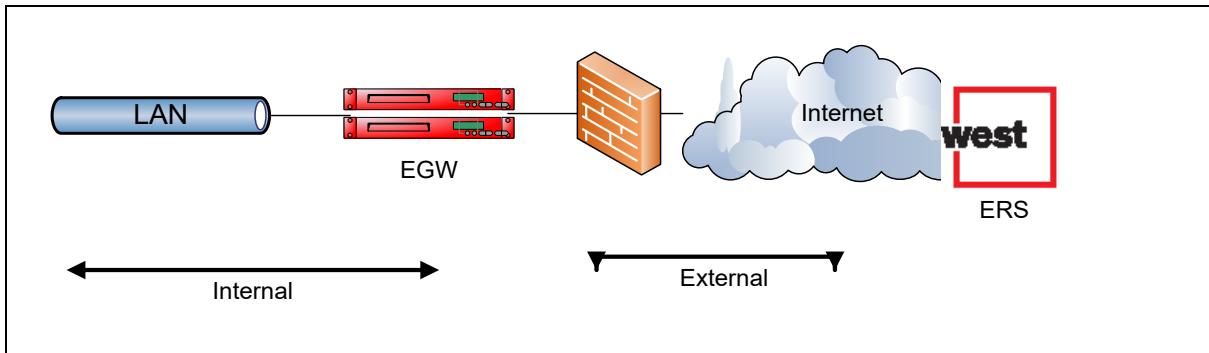
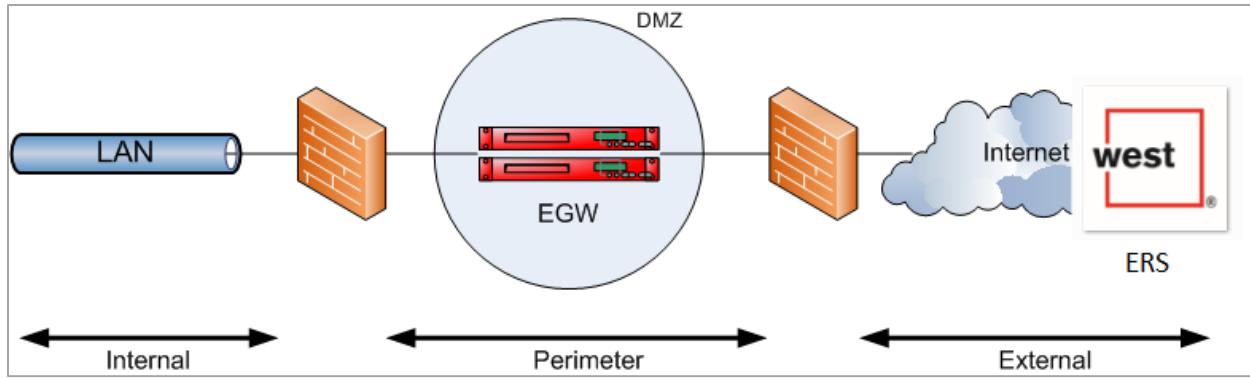


Figure 8: EGW in SBC Mode

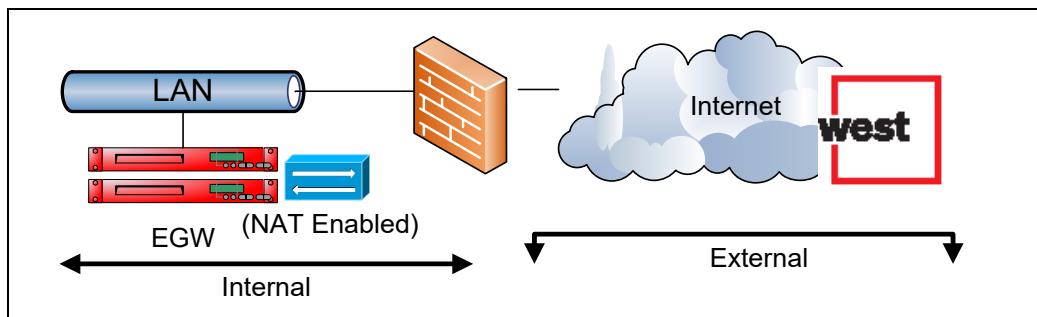
3.2.5 Demilitarized Zone (DMZ)

The DMZ topology has the following characteristics:

- The EGW's Internal interface is configured with a private IP.
- The EGW's External interface is configured with a public IP.
- The external firewall performs IP/ port filtering.



3.2.6 EGW in Transparent NAT Traversal Mode



- The EGW's internal interface is assigned a private IP.
- The public IP of the firewall is configured on the EGW*
- The EGW performs NAT-ing and SIP application layer inspection
- The corporate firewall allows SIP to transparently pass through, and perform IP/port filtering

3.3 Deploying the Emergency Gateway

This section describes deployment models for various types of networks. You may use these examples to determine the best way to deploy the EGW in your own network.

3.3.1 EGW Deployment Scenarios

1. Centralized IP-PBX deployment :
 - One pair of EGWs accommodates both legacy and IP systems.
 - The EGW can support remote branch offices and work-at-home employees that connect over the WAN.
 - 911 calls are routed to the ERS or local exchange carrier.

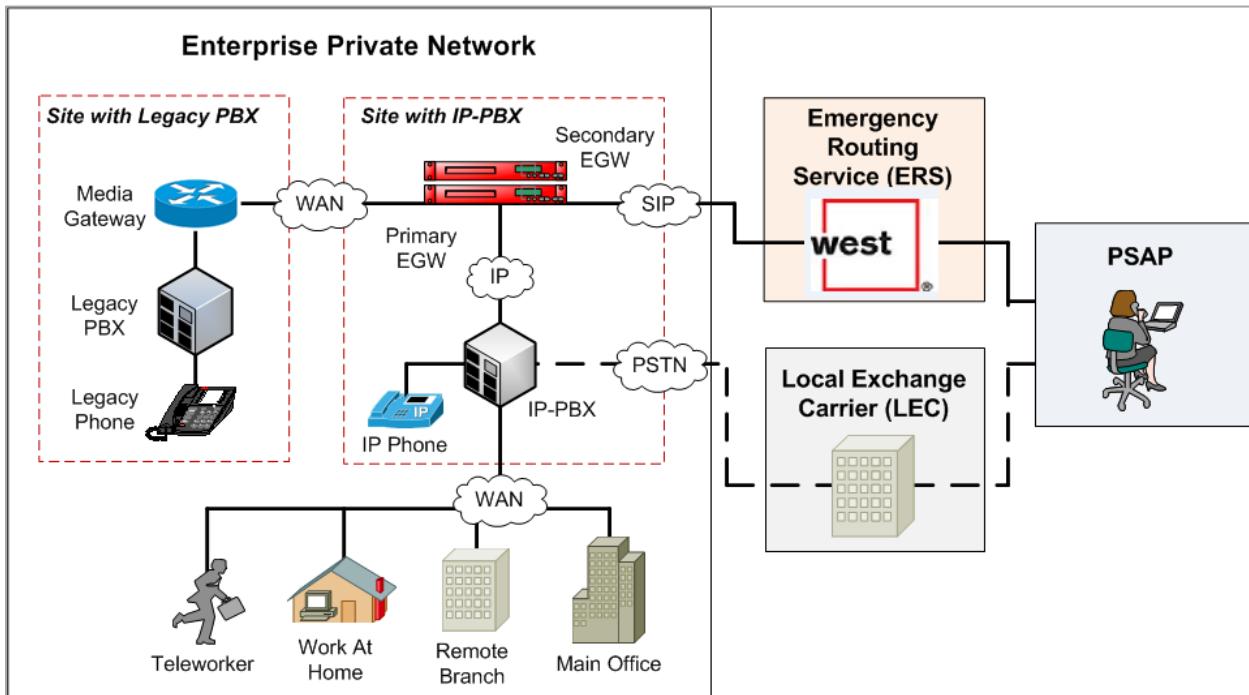


Figure 11: Centralized IP-PBX Deployment – Multiple Sites

2. Multiple IP-PBX servers behind a session border controller (SBC)

- Multiple IP-PBX servers may share the same signaling IP address.
- The EGW uniquely identifies each IP-PBX using a DNS Prefix.

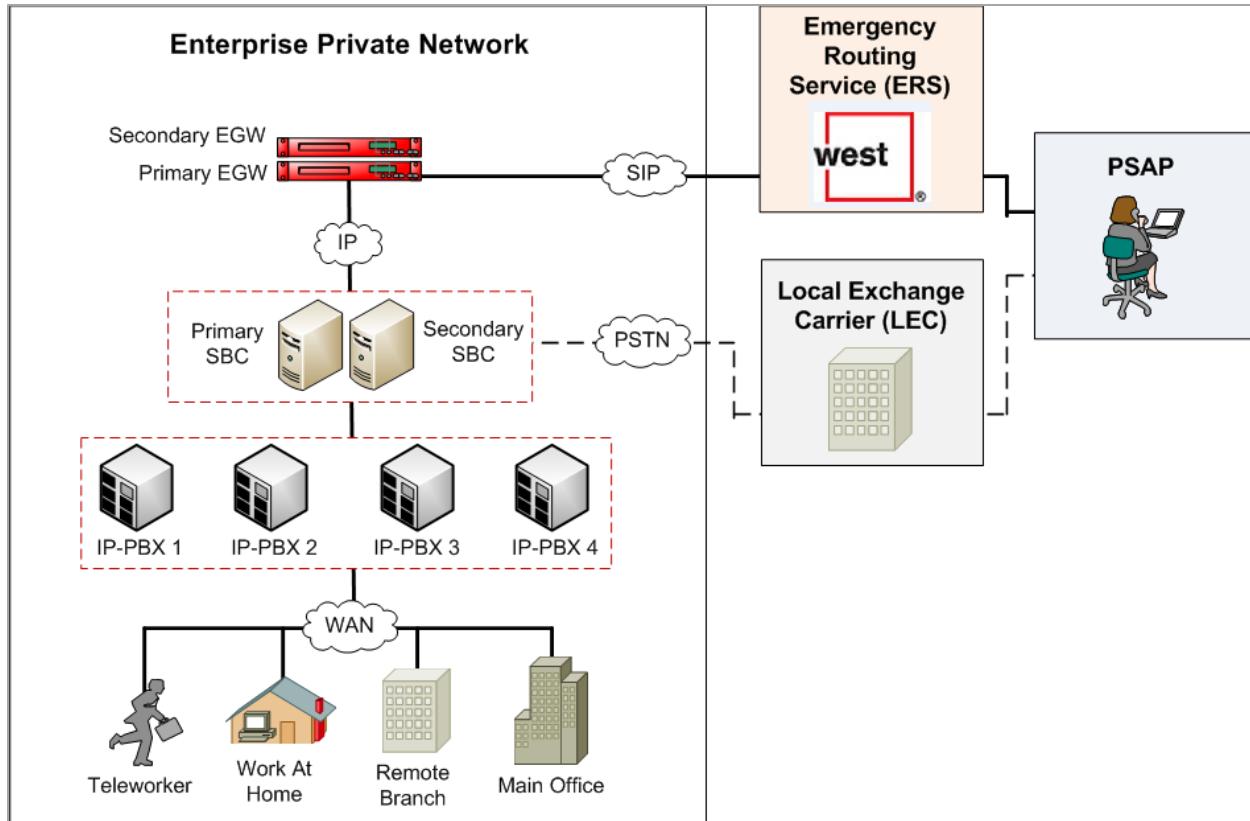


Figure 12: Multiple IP-PBX Servers Behind SBC

3. Distributed data sites
 - EGWs are distributed between different data sites for survivability.*
 - Service fails-over to secondary EGW in the event of a disruption.

*recommended round trip delay is 100ms or less.

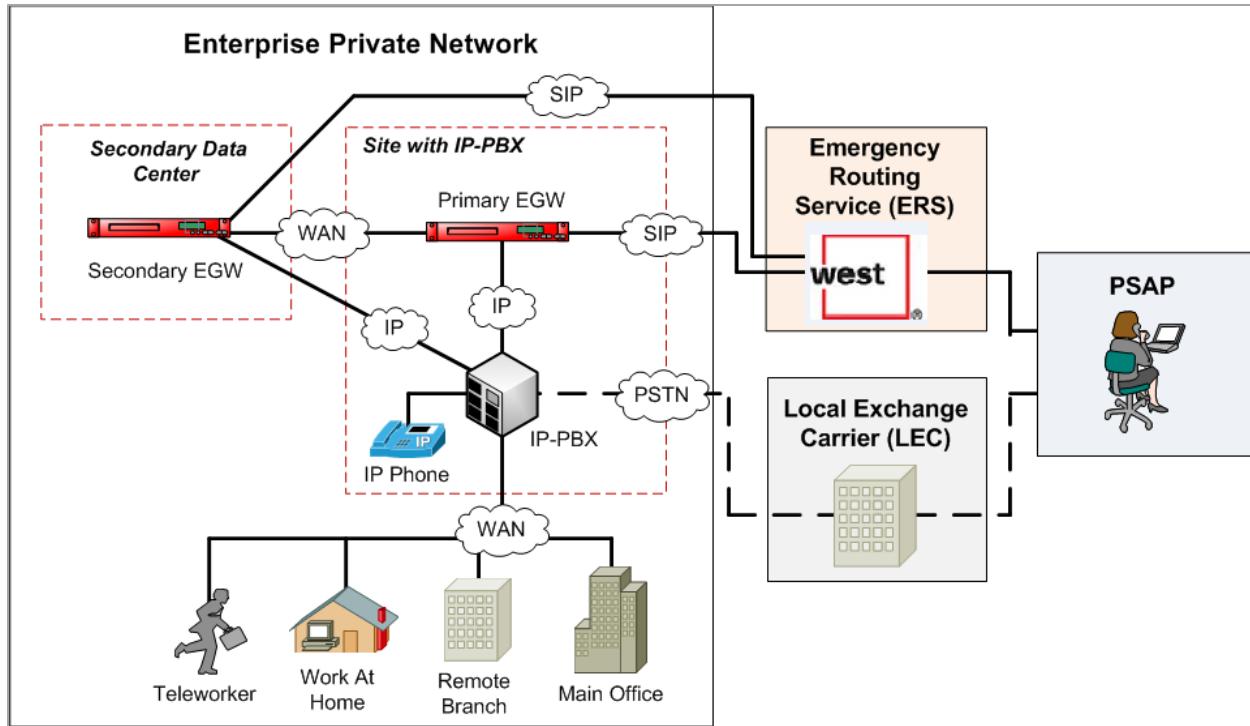


Figure 13: Distributed Call Processing

3.3.2 Cisco Extension Mobility Cross Cluster Deployments

In this deployment the phones register to their own clusters (eg. Phone from Site 1, registers to CUCM 1 and phone from site 2 registers to CUCM 2).

- One EGW pair can support both CUCM clusters, even when phones move cross cluster, or when employees use extension mobility cross cluster (EMCC) feature

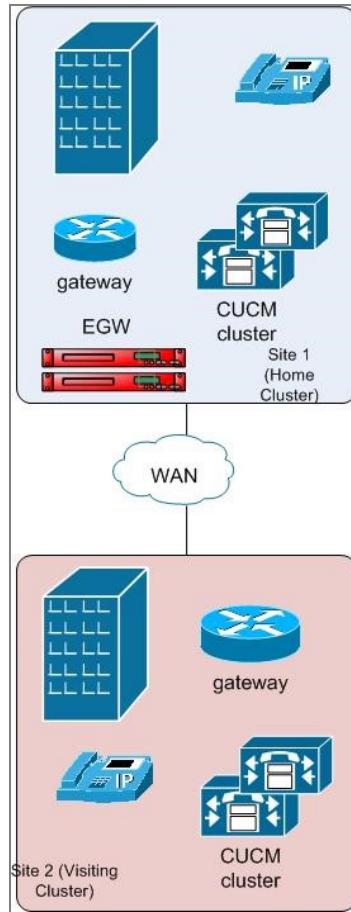


Figure 14: Cisco Cross Cluster Deployments

3.3.3 Centralized LIS Deployment

In the scenario where multiple sets of EGW server pairs are used to service a deployment, it may be necessary to direct the servers to communicate to a central pair of EGW appliances (hardware or virtual) with the Location Information Server (LIS) function.

This scenario is typically only seen with very large enterprises with a truly national or multi-national presence. The diagram below illustrates the deployment scenario. A load balancer is used to load balance traffic to the CPM between the redundant appliance servers.

Note: In this scenario, the parameter CPM local must be set to No on the Global settings. For more information 9.1 "Global Settings Screen."

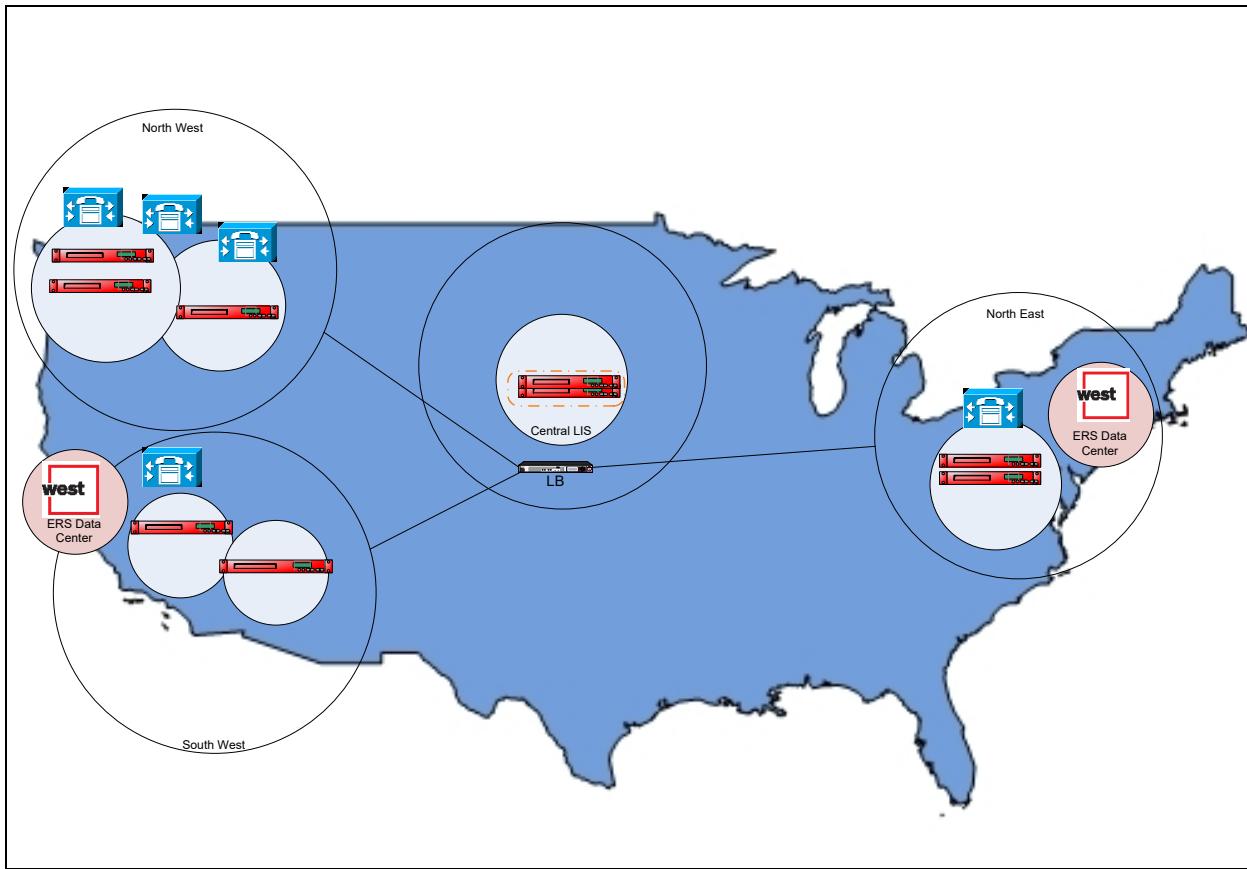


Figure 15: Centralized LIS Deployment

3.4 Call Routing

The EGW is capable of delivering emergency calls to the ERS or the Local Emergency Network (LEC) using local trunking. An emergency number can also be programmed to deliver calls to an on-site private answering point (e.g. security desk), with or without termination to the appropriate PSAP.

Additional dial plan numbers may also be programmed into the EGW to route calls to security desks or to test the system. A programmed test mode number will route to a test recording when dialed.

The following destinations are possible when a number is added to the EGW dial plan:

- ERS network
- Local emergency network (LEC)
- On-site security desk
- Test mode recording

3.4.1 Planning for Call Routing via the ERS

Call routing via the ERS is the preferred solution for enterprises with centralized IP-PBX deployments.

For call routing via the ERS, the following network requirements must be met:

Bandwidth Requirements

The enterprise must connect to the ERS through the public internet. Intrado recommends dedicating a minimum of 1.5 Mbps of bandwidth per 10 concurrent 911 calls for optimal call quality.

Security

Trusted IP security should be set up on all firewalls and packet-filtering devices.

An encrypted connection between the EGW and the ERS can be established using a VPN tunnel (optional). This connection guards against spoofing attacks and packet manipulation. Intrado supports IPSec VPN with the following authentication and encryption options:

Table 7: VPN Specifications

VPN Specifications
<p>Authentication methods:</p> <ul style="list-style-type: none"> • IKE* with pre-shared secret key • IKE* with third party certificate • Manual Key <p>*IKE V1 or V2 in either main mode or aggressive mode</p> <p>Supported encryptions:</p> <ul style="list-style-type: none"> • DES • 3DES • AES-128 • AES-192 • AES-256

Outbound data transmission to Intrado, such as location data, is encrypted using SSL version 3.0 using 128 bit RC4 as the stream cipher.

Network administrators must open specified ports on their firewalls and packet-filtering devices, and follow all Intrado security policies. Firewall rules and security policies must be applied to both the internal and external EGW interfaces.

For more information regarding EGW Security, see the document “EGW Networking Interface Description.”

Procurement of DIDs for Extension-Bind

The EGW can provide station-level identification for all phones, including those that do not have assigned DIDs. For endpoints without DIDs, Intrado’s “Extension-Bind” technology will dynamically assign a callback number during a 911 call.

It is necessary to procure DIDs from the local exchange carrier to act as Extension-Bind numbers for non-DID stations. A small pool of 10-15 DIDs is sufficient for the largest enterprise deployments.

For more information concerning Extension-Bind see section 5.1.2 “Callback Settings.”

3.4.2 Planning for Call Routing via the Local Exchange Carrier

Call routing via the local exchange carrier may be the preferred solution for an enterprise with a single, high-density deployment, located within one PSAP jurisdiction.

For call routing to the LEC, the following network requirements must be met:

Emergency Trunks

PRI or CAMA trunks are required to deliver emergency calls to the LEC for routing to the local PSAP. Capacity planning is required to prioritize emergency calls over regular voice traffic, if a PRI is used. CAMA trunks are dedicated for emergency calling purposes and do not require capacity planning. Trunking requirements vary depending on the location of satellite offices and the local layout of the emergency calling network. Enterprises should consult their local service provider to determine more specific requirements.

Note: SIP Trunking is also an option, provided that it is supported by your service provider (local exchange carrier).

Procurement of ELINs

Emergency Location Identification Numbers (ELINs) are 10-digit telephone numbers (DIDs) that must be purchased from the local carrier to route location data to the correct PSAP when 911 is dialed. ELINs are uploaded, along with the appropriate location records, to the LEC's ALI database.

You must upload your ELINs to the local ALI database in the appropriate carrier-specific format. It is also important that you test your ELIN configuration to ensure that the PSAP can callback a 911 caller through the local exchange carrier's network. You should consider assigning multiple ELIN records per ERL, to account for a situation where multiple callers from the same ERL simultaneously dial 911. In this scenario, ELINs are assigned to the 911 calls in the order in which they are placed. The EGW allows you to assign up to 3 ELINs per ERL record.

You can assign ELINs to your ERLs statically or dynamically. Dynamic ELIN assignment will automatically assign an ELIN number from the dynamic ELIN pool on the EGW. However, this is only appropriate if you are only routing calls to a single PSAP within one NPA-NXX. Otherwise, you can statically assign your ELINs to the ERLs. In this case, you can associate ELINs to ERLs at the local exchange carrier and then manually load this data into the EGW.

ALI Data Requirements

When locations are added or updated, these changes must be reflected in the carrier's regional ALI database. Format rules vary from carrier to carrier, and you must work with your LEC to upload the ALI data in the required format. It is also necessary to re-export ALI data anytime you update the ELINs for an ERL, or if you add or delete an ERL from the system. You may work in an ongoing fashion with the database provider to help ensure that your ERL/ELIN configuration matches the ALI data stored in the regional ALI.

The EGW also includes a NENA 2 file-generation feature. This feature automates the export of NENA 2 files on a periodic basis. These files can be used to update security desk P-ALI databases or LEC PS-ALI databases. For more information see section 16 "NENA 2 Provisioning."

Local Gateways

A local voice gateway is required to convert 911 calls from SIP/ H.323 to PSTN. IP-to-PSTN gateways must be maintained at every satellite office that uses local trunking. Resources are assigned at each site to perform troubleshooting and maintenance. Each PSTN gateway represents a single point of failure in the event of hardware or software malfunctions.

To configure the EGW to route calls to the local exchange carrier, see section 6 "Configuring Local Trunking (LEC Call Routing)."

Note: If SIP trunking to the local exchange carrier is used, local gateways are not required, and a session border controller (SBC) can be used instead.

3.4.3 Planning for Emergency Conferencing and Routing Calls to Security Desks

Emergency calls can be routed to one or many on-site participants, with or without termination to a public safety answering point (PSAP).

The EGW supports routing directly to a security desk, or routing to the PSAP while an on-site security desk monitors the call (with or without one way mute). You can also setup multi-party emergency conferences with multiple on-site participants, with or without termination to the PSAP.

The EGW supports multiple dial plan numbers which can be allocated to emergency calls, security desk calls, and non-emergency calls to security desks.

ERL records are used to indicate the name of the security desk that will route the call and the direct delivery or call monitoring settings. The dial plan can also be setup to support multiple numbers that route to different destinations. For multi-party emergency conferencing, security desk groups setup on the EGW specify the extensions and settings that will apply to participants in emergency conferences.

For more information, see section 5.4 “Configuring Emergency Conferencing and Security Desk Routing.”

Emergency Dial Plan Considerations

When an emergency number is dialed, an ERL record is used to determine the destination of the call. ERLs can be configured to initiate calls to an on-site security desk, with or without delivery to the appropriate PSAP. For example, you can set an emergency number to deliver calls to an onsite PEAP, and bypass call delivery to the PSAP.

You can also program a security desk number into the EGW that is different from your emergency number(s). A call to the security desk number always routes to an on-site security desk. A call to an emergency number can route to a PSAP and/or security desk, based on your configuration.

NENA 2 Files

The EGW can generate NENA 2 files on a periodic basis. This feature simplifies administration for enterprises that have on-site security desks with P-ALI databases. The files are exported from the EGW and added to the P-ALI, enabling the correct location to be displayed on the security desk monitor when the emergency number is dialed.*

*Not applicable for UK/Europe deployments.

For more information, see section 16 “NENA 2 Provisioning.”

3.4.4 Test Mode

The EGW test mode feature allows you to route calls to a test recording. The test recording indicates the status of the call (provisioned, unprovisioned) and reports the callback number associated to the call.

Test calls can also be routed to the ERS. Routing a test call to the ERS allows an end to end test of the EGW to ERS connectivity and provisioning. When the ERS answers the test call, it will playback the provisioning status, the address and the location assigned to the endpoint and the E911 coverage. Voice is also recorded and played back to test that audio is working in both directions.

The EGW also allows to select to which ERS SBC the test call is routed. This enables the ability to specifically test the connectivity to each ERS server without having to create conditions for failover to occur. This will be useful to verify all connectivity paths to ERS are maintained when network changes are made at the customer premise.

Please note that the EGW must be connected to ERS 3.x (not local trunking) for this functionality to be available.

There are a variety of ways to configure test mode based on the needs of your deployment:

- **Dial plan** - dialed number (e.g. 711) is configured to route to a test recording

- **Endpoints** - endpoints are individually assigned to test mode*
- **IP-PBX Servers**- entire call servers are assigned to test mode*

* When the number is dialed, call is sent to test recording.

The way in which test mode is implemented at the enterprise will reflect the nature of your deployment and testing needs.

For more information, see sections 5.3 “Test Mode,” and 5.2 “EGW Dial Plan.”

3.5 SIP and the EGW

The EGW SIP implementation uses a request/response method to establish communications between various components in the network and to establish a call or session between two or more endpoints.

A single session may involve several clients and servers. Identification of users in a SIP network works through

- A unique phone or extension number.
- Other network information that can be passed in the fields of the SIP request: eg. MAC address (layer 2 discovery), IP address (layer 3 discovery)

SIP trunks are established between IP-PBX systems and the EGW to provide E911 services. The EGW implements Emergency Routing using either SIP trunks to ERS or to a local trunking IP-PBX or local gateway.

The EGW listens for SIP messages on port 5060 and supports both UDP and TCP. Its supported audio media type is G.711 using PCMU encoding.

Refer to the EGW vendor-specific configuration guide for more information.

3.5.1 Redundancy and Failover

To insure maximum reliability of emergency call delivery, the EGW supports various levels of SIP component redundancy:

1. Redundant links to the ERS servers can be provisioned on the EGW.
2. Redundant PBX servers can be provisioned on the EGW or through DNS SRV.
3. 302 redirect with multiple contacts can be used to provide redundant alternate destinations.
4. If unable to reach any of the servers required for Emergency Routing the EGW will respond with a 503 Service Unavailable to allow the calling IP-PBX to failover to an alternate destination.

3.5.1.1 Redirection

The EGW supports SIP 3xx redirection responses (for example 302 temporarily moved).

In a typical SIP-capable enterprise PBX system, hosting server nodes are clustered for redundancy. In this scenario, the EGW network element will deliver a SIP request to a SIP server to deliver a call to a user@domain. The SIP server can return a 302 temporarily moved response with a list of contacts. The contacts represent the hosting nodes that can deliver the SIP call to the user.

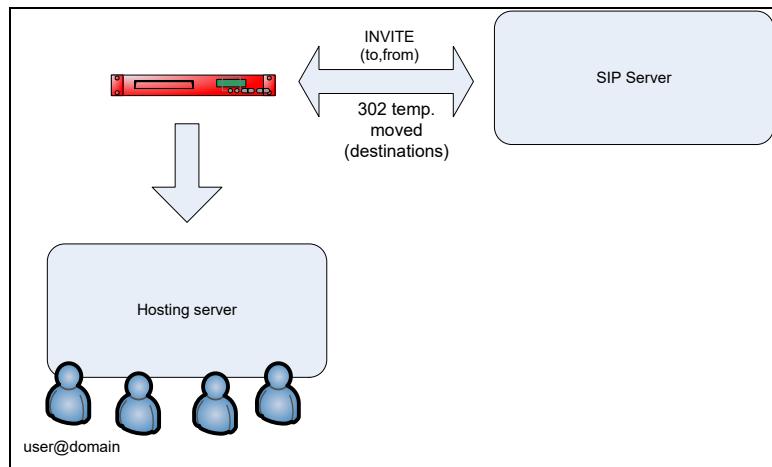


Figure 16: Support for Re-direction

3.5.1.2 SIP Routing Server Redundancy

The EGW redundancy solution for sip servers can use DNS, or it can use the EGW's domain configuration.

If DNS is used the EGW can reference DNS SRV records with cost and weight.

The DNS records resolve the routing server fqdn with the possible IPs which can be used to reach it.

3.5.1.3 Service Unavailable

The EGW supports SIP 503 server failure response messages.

Note: *SIP Options must be enabled on a SIP server at the EGW for the EGW to know the status of the sip peers. When the EGW knows the status of a sip peer it can send service unavailable 503 to the requester if the sip resource is unavailable. The status of the monitored servers is maintained in a SIP peer list by a scheduled task called **Peer Monitoring**, and dictates the behavior of SIP 503 service unavailable messages.*

The EGW will send a 503 failure response if it detects that all routes to the requested destination are down. For example, if both links to the ERS are down on a call destined to the ERS, the EGW will send a 503 back to the IP-PBX. However, if the EGW has already accepted a call, and a Peer fails it will not send the 503 failure response. In this case the call will be directed to a fallback DNIS (representing an IP-PBX server or gateway), if all the other routing peers at the EGW are unavailable. Note that the EGW will also send a 503 error message if no response is received from the fallback DNIS.

The monitored peers include the ERS SIP destinations (always enabled), and SIP signaling servers/gateways, provided that sip options monitoring has been enabled for these servers at the EGW.

For more information see IP-PBX configuration section that pertains to your IP-PBX version for configuration of the **Monitoring Enabled** parameter.

For more information concerning the **Peer Monitoring** task , see section 10 Task Scheduler.

When SIP options fails to detect the status of a SIP server a variety of alarms are possible. For a list of alarms, see section 20 "EGW Alarms."

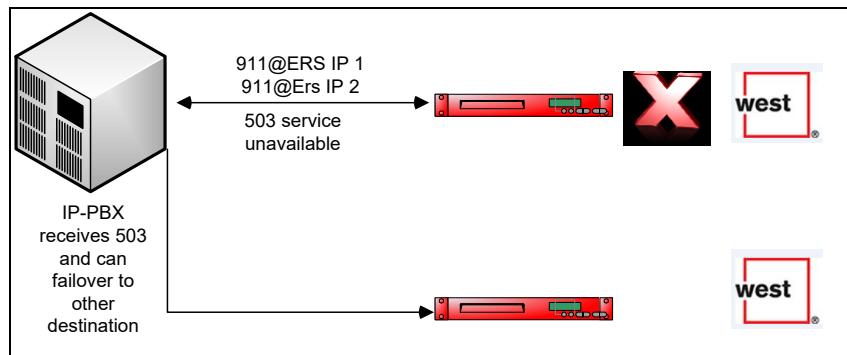


Figure 17: EGW Support for "503 Service Unavailable"

3.5.2 Supported SIP Standards

- RFC3261 (SIP)
- RFC4566 (SDP)
- RFC3550 (RTP)

3.5.3 Supported SIP Request Methods

The EGW interface provides a subset of supported SIP Request Methods.

- ACK
- INVITE
- OPTIONS
- BYE
- CANCEL

3.5.4 Call Failure Scenarios for Failed Calls

The EGW is deployed as a pair of redundant servers that can be deployed in separate data centers. The ERS service is deployed using geographically redundant data centers.

When SIP options monitoring is enabled at the EGW for a specific SIP server, the EGW will use SIP error codes 503, when required SIP peer destinations are not available. The SIP 503 service unavailable message is delivered to the requesting user agent, in order to communicate that the required service is not available.

The following call flow scenarios are possible for failed calls:



Note: To configure SIP Options monitoring for a SIP server, see section 7 "Configuring IP-PBX Settings".

1. EGW immediately sends service unavailable response based on peer status.
2. EGW tries ERS but call routing is unsuccessful.
3. EGW immediately sends service unavailable response based on peer status. (local trunking)
4. EGW tries destination but call routing is unsuccessful.
5. EGW tries destination but call routing is unsuccessful. (not monitored)

3.5.4.1 Scenario 1: EGW immediately sends service unavailable response based on peer status

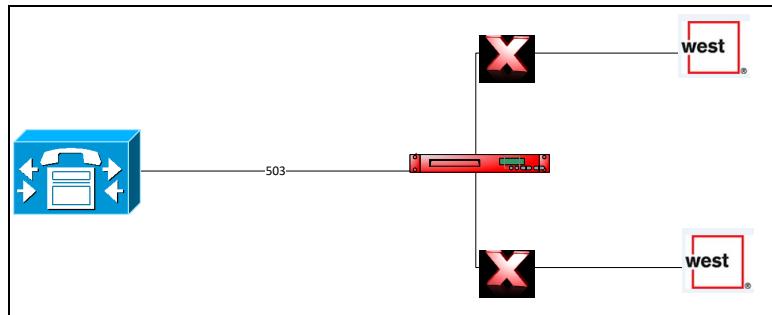


Figure 18: Service Unavailable Response

1. Call is delivered to EGW.
2. The ERS datacenters are both down in the peer list.
3. EGW sends sip 503 to the requesting SIP server. The IP-PBX will alternate route to the ERS or emergency call response center (ECRC).



Note: If misdial protection is configured, the recording is NOT played out. If multi-party routing is configured (security desk or emergency conferencing), the 911 caller is NOT joined to the EGW conference bridge and the extra call leg(s) is NOT initiated.

3.5.4.2 Scenario 2: EGW tries ERS but call routing is unsuccessful

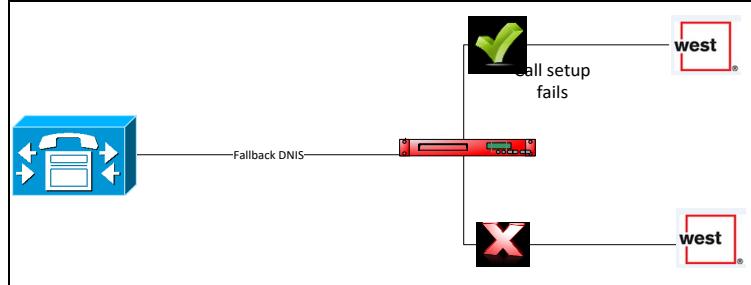


Figure 19: Call Routing Unsuccessful

1. Call is delivered to the EGW.
2. At least one ERS peer is up at call time.
3. The EGW tries to setup the call but the call fails.
4. The EGW directs the call to the fallback DNIS.



Note: If misdial protection configured, misdial recording is played out. If multi-party routing (security desk or emergency conferencing), is configured, 911 caller is joined to the EGW conference bridge immediately (or after misdial played out), and additional call leg(s) is initiated.

3.5.4.3 Scenario 3: EGW immediately sends service unavailable response based on peer status. (local trunking)

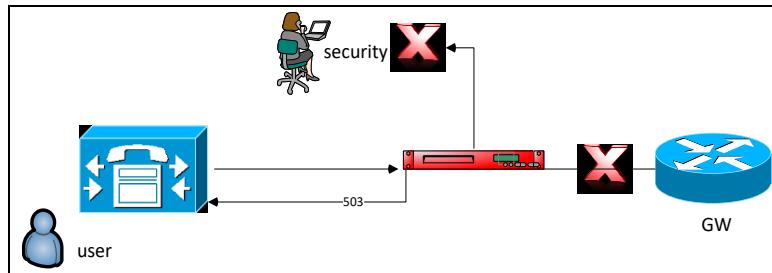


Figure 20: Service Unavailable Response - Local Trunking

1. Call is delivered to the EGW.
2. The local trunking or direct call delivery Peers are down in the peer list.
3. The EGW sends SIP 503 to the requesting sip server. The IP-PBX will alternate route to the ERS or the ECRC.

Note: If misdial protection is configured, the recording is NOT played out. If multi-party routing (security desk or emergency conferencing), is configured with local trunking, the 911 caller is NOT joined to the EGW conference bridge and additional call leg(s) is NOT initiated.

3.5.4.4 Scenario 4: EGW tries destination but call routing is unsuccessful.

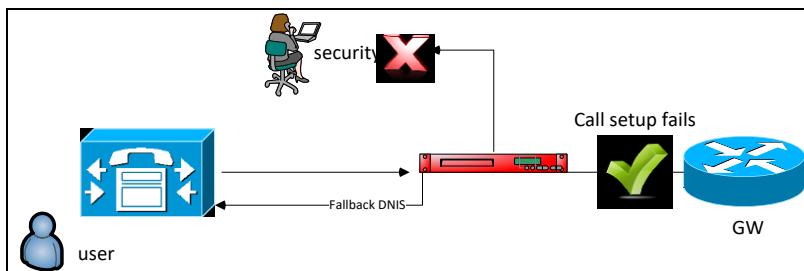


Figure 21: Call Routing Unsuccessful

1. Call is delivered to EGW.
2. At call time, the appropriate SIP peer is up in the peer list, but the call fails.
3. The EGW directs the call to the fallback DNIS.

Note: If misdial protection configured, misdial recording is played out. If multi-party routing (security desk or emergency conferencing), is configured with local trunking, 911 caller is joined to the EGW conference bridge immediately (or after misdial played out), and additional call leg(s) is initiated.

3.5.4.5 Scenario 5: EGW tries destination but call routing is unsuccessful. (not monitored)

If PBX servers are configured with monitoring disabled, the EGW will answer the originator's call before initiating the emergency call towards the emergency responder.

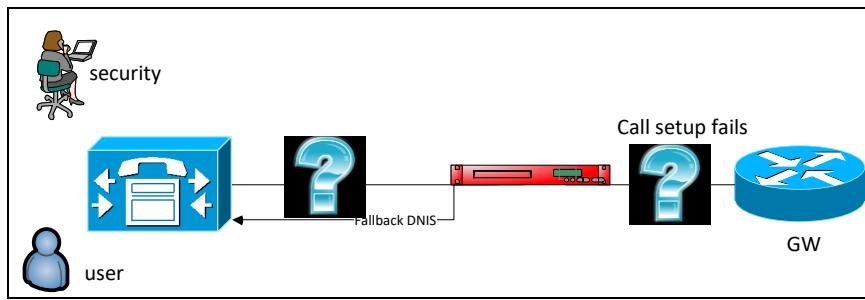


Figure 22: Call Routing Unsuccessful

1. Call is delivered to the EGW.
2. When call arrives at EGW the peer status is unknown.
3. The EGW answers the call and immediately sends 180 ringing.
4. If call setup fails, the EGW directs the call to the fallback DNIS.

Note: If misdial protection configured, misdial recording is played out. If multi-party routing (security desk or emergency conferencing), is configured with local trunking, 911 caller is joined to the EGW conference bridge immediately (or after misdial played out), and additional call leg(s) is initiated.

3.5.5 Restrictions

The EGW does not support call transfer capabilities provided by the SIP Refer method.

3.6 Notification Capabilities

The EGW will send notification events for alarms and alerts.

The alerts are created when emergency calls are made:

Crisis alerts: Report that a user made an emergency call.

Unprovisioned alerts: Report that an emergency call was made from a user that is not provisioned in the EGW endpoints inventory.

Off-campus alerts: Report that an emergency call was made from an off-campus user (off-site).

Please note that while setting up the dial plan, you can choose to have the notifications disabled. By default, they are enabled for the above alerts. For more information on how to disable this, please refer to section 5.2.2 Configuring the Dial Plan.

The alarms report on EGW application, host and service error events. For example, the alarms report on error conditions pertaining to the application modules of the EGW (CTI, CPM, SNMP etc.)

The alarms and alerts can be sent as email notifications or SNMP traps.

To configure notification settings, see section 8 “Configuring Alerting, Notification.”

For more information about alarms, see section 20 “EGW Alarms.”

3.6.1 Planning for Sending SNMP Traps

The EGW uses a proprietary MIB to send SNMP traps for alarms and notifications to your network management system (NMS).

The proprietary MIB can be obtained here: <http://<egwip>/mibdefinitions/WEST-EGW-MIB.my>

For more information, see section Appendix C: EGW Proprietary MIB Reference.

where “egwip” is the IP address of your EGW on the network

In order to allow your management stations to receive SNMP trap notifications from the EGW, the EGW proprietary MIB must be loaded into your MIB browser, or network management system (NMS).

To configure SNMP trap receivers, see section 8.2 “Configuring SNMP Traps Settings.”

3.6.2 Mail Server Settings

Email alerts and notifications are sent from the EGW using your mail server. A mail server IP address is also specified for the Remote Access Controller (RAC) alerts.

3.6.3 Crisis Alerts

The crisis alert email feature allows email notifications to be sent to your personnel when 911 is dialed.

The crisis alert email may include a URL link to additional information such as a campus map or database query. You must decide how to best use the URL link, based on your organization’s emergency response policies and existing systems. At the very least, all personnel should be aware of their individual responsibilities when they receive crisis alerts. The naming of fields displayed within crisis alert emails may be customized to ensure that personnel are familiar with the terminology used.

3.6.4 Desk Alert

Desk Alert is software that is installed on security desk workstations. It notifies security desk personnel of 911 calls in progress.

You should consider the impacts that Desk Alert will have on your existing emergency response procedures. Security staff should be well-prepared to respond when Desk Alerts appear on their workstations. This includes:

- Properly acknowledging alerts.
- Properly interpreting alert fields.
- Understanding location information.

In addition, security desk staff should be able to use the Desk Alert interface. The interface allows you to:

- Configure settings
- View history
- Access the help pages

Desk Alert is administered using the EGW Dashboard. You may use the interface to create Desk Alert accounts, configure settings, and monitor performance. A separate account is created for each workstation operator, and pertinent statistics are logged. For each user, it is possible to view alerts received and acknowledged, and the average acknowledgement time.

You may also send test alerts to Desk Alert workstations by configuring test endpoints. Test notifications are used to ensure that alarm notifications are working properly.

For information about Desk Alert, see “Desk Alert Administrator User Guide.”

For more information about Test Mode, see Section 5.3 “Test Mode.”

3.6.5 URL Variables and URL Template Editor

You can customize the variables in the url link that is sent in Desk alert and crisis alert notifications. These variables will also output to the crisis alert SNMP traps.

You can configure and test the url variables using the Dashboard. You can provision the url and its variables using the EGW's provisioning interfaces: GUI, batch, or SOAP.

For more information, see section 11.2.2.3 "URL Template Editor."

For more information, see section 11.3 "ERL Batch File Format."

For more information, see the document "Desk Alert Administrator User Guide."

3.7 Preparing Your Users for the EGW

EGW administrators, in conjunction with network and telephony staff, are assigned the tasks of system management, using the administrative interface, and overseeing the functioning of the 911 system.

Ongoing responsibilities for network and telephony staff are outlined in the document "EGW Appliance Standard Operating Procedures."

EGW administrators log into the Dashboard and obtain access to its features based on their assigned access level. The Dashboard is regulated by three different levels of access - Limited, Provisioning, Full - which are assigned to users by the primary administrator.

It is up to the discretion of the primary administrator to assign administrative access levels to EGW users, based on the tasks that they must complete. Enterprises will designate these tasks based on their existing emergency response procedures and the capabilities of the EGW. A suggested approach is to provide Limited access to users who will be contacted under exigent circumstances to search for a specific ERL or endpoint record. Other users may be assigned Provisioning access, in order to assist employees with address validation and provisioning issues. Full access is reserved for users that will configure, monitor, and troubleshoot the EGW.

For a complete itemization of the access privileges that apply to each level of access, see section 4.3.3 "User Management."

3.8 Planning for Unified Communications

Unified Communications is a broad term that takes in employee mobility, mobile endpoints, cutting edge applications, and new ways of improving workplace efficiency through real-time collaborations. Intrado provides a variety of applications which can work with your EGW to meet the needs of your unified communications deployment. The following table summarizes the applications available, basic features, and their intended use.

Table 8: How to Plan for Unified Communications

Application	Description	What is It For?
Remote Location Manager (RLM)	The RLM is a service running on the EGW that is accessible to a variety of IP phones from different vendors (Cisco, Avaya, Microsoft). The service enables a user to use their IP hardphone or Microsoft Office Communicator to access an EGW self-provisioning page using their phone's native browser capabilities (XML, WML etc.)	<ul style="list-style-type: none"> -Cisco IP hardphones and IP communicator -Avaya 46xx and 96xx IP phones -Microsoft Lync client <p>Enables self-provisioning for off-campus IP phones, or for on-site phones in networks that don't support automatic discovery (eg. Layer 2, 3, or WLAN).</p> <p>For more information 17 "Provisioning Off-Campus Users."</p>

RLM for softphones	<p>The RLM for softphones is a service running on your machine, which communicates with the EGW. It triggers a provisioning pop-up window, in response to IP softphone events (i.e. Start-up), prompting the user to confirm/self report their emergency location.</p> <p>RLM is available for both Windows and Mac OS environments. However, only Cisco Jabber softphone client installed in a Mac OS environment is supported by RLM.</p>	<p>Enables self-provisioning for users of IP softphones (eg. Avaya softphone). Provides self-provisioning capability for off campus users with softphones on their laptops.</p> <p>For more information see section 17 "Provisioning Off-Campus Users."</p>
E911 Softphone Locator (ESL)	<p>The E911 Softphone Locator (ESL) is a service that enables provisioning data to be automatically sent from softphones to the EGW. The provisioning data allows the EGW to support automatic discovery of softphones using Layer 2, 3, or WLAN Discovery. It also enables the EGW to track softphones in advanced unified communications networks that use features such as concurrent logins, shared workspaces, extension mobility, and shared line appearance.</p> <p>ESL is available for both Windows and Mac OS environments. However, only Cisco Jabber softphone client installed in a Mac OS environment is supported by ESL.</p>	<p>Provides automatic discovery (Layer 2, 3 or WLAN) for based softphones that are located on-site.</p> <p>For more information see section 17 "Provisioning Off-Campus Users."</p>
Automatic Discovery	<p>Layer 2 Discovery uses SNMP to scan network switches in order to identify the locations of IP phones. Layer 3 Discovery works by associating IP subnets to ERLs. If an enterprise has geographically assigned subnets, Layer 3 discovery is an accurate way of providing location discovery to the floor level. WLAN Discovery tracks wireless phones using the BSSID of the nearest wireless access point.</p>	<p>Intended for on-site phones.</p> <p>For more information, see section 17 "Provisioning Off-Campus Users."</p>

4 Configuring Basic Settings

This section provides detailed instructions on how to configure the EGW. The web-based administrative Dashboard is used for many configuration tasks.

4.1 Configuration Overview

This table provides information on the tasks necessary to configure the EGW system. References to more detailed information are provided.

Table 9: Configuration Steps

Task	Description and Reference
Perform first run configuration and activation	
Obtain access to the EGW Dashboard If you are the primary administrator, assign log-in credentials and the correct access level (Full, Limited, Provisioning) to other users.	<ul style="list-style-type: none"> • Browser Requirements • Logging On • Access Level Management See section 4.3 “Web-Based Dashboard.”
Add EGW Users <ul style="list-style-type: none"> • Users may be authenticated remotely via LDAP using MS Active Directory. Users may also be authenticated locally by the EGW. The two methods work together. 	For user management and LDAP setup see section 4.3.3 User Management.
Understand and perform planning requirements <ul style="list-style-type: none"> • Obtain and review local ordinances pertaining to ERLs. • Determine ERL granularity and network suitability for layer 2/layer 3, and WLAN discovery. • Determine if phones support automatic discovery, or if they will need to be manually added to the EGW configuration. • If ELINs are required, procure them from the LEC. • Review EGW licensing requirements. Ensure that you obtain an appropriate license that will match your current and projected endpoint count. Also, ensure that licenses are procured for additional features such as Desk Alert. • Decide if you will deploy the EGW as a hardware or virtual appliance. If you will deploy the EGW as a virtual appliance, ensure that your hardware meets the EGW requirements for virtualization. For more information see section, 2.2 “Emergency Gateway Specifications.” • Determine what features and application will be used to meet the requirements of unified communications in your deployment. The EGW includes a variety of services and applications, including the Remote Location manager (RLM), and E911 Softphone Locator (ESL). For more 	For basic system planning tasks, see section 3 “System Planning.” For ERL related tasks, see section 11 “Emergency Response Locations (ERLs).” For automatic discovery, see section 12.4 “Layer 2 Discovery”Layer 2 Discovery and section 14 “Layer 3 Discovery.” For WLAN Discovery, see section 15 “WLAN Discovery.”

Task	Description and Reference
<p>information, see section 3.8 “Planning for Unified Communications.”</p>	
<p>Configure telephony settings on the EGW to establish connectivity to ERS or local trunking*</p> <p>*If local trunking is in use, additional configuration work is required. It is also necessary to export location records to the LEC in the appropriate format.</p> <ul style="list-style-type: none"> Program the emergency number and any additional numbers into the EGW’s dial plan. 	<ul style="list-style-type: none"> Emergency Routing Service (ERS) connectivity Callback settings Emergency numbers (EGW Dial Plan) Misdial protection feature Test Mode <p>See section 5.1 “Configuring Basic Telephony and Networking Settings.”</p> <p>See section 6 “Configuring Local Trunking (LEC Call Routing).”</p> <p>See section 16 “NENA 2 Provisioning.”</p> <p>See section 5.2 “EGW Dial Plan.”</p>
<p>On-site alerting and notification</p> <ul style="list-style-type: none"> Determine how you will enable on-site notifications (if applicable) Determine if your on-site alerting system will require the Desk Alert application (screen pop application for security desk users) Determine if you will setup your EGW alerting system using email messages or SNMP traps. 	<ul style="list-style-type: none"> Security desk routing Mail server Alarm email distribution lists Crisis Alert emails Desk Alert <p>See section 8 “Configuring Alerting, Notification.”</p>
<p>Configure IP-PBX settings on the EGW Dashboard</p> <ul style="list-style-type: none"> These settings allow the EGW to communicate with your IP-PBX. It is important that every signaling server capable of routing calls to the EGW be added to the EGW configuration (e.g. Server Proxies, Session Border Controllers, etc.). 	<ul style="list-style-type: none"> Vendor-specific settings (Cisco, Avaya, Microsoft, etc.)
<p>Provision ERLs</p> <ul style="list-style-type: none"> Upload location records to the EGW, including ELINs, local trunking settings, security desk routing settings, etc. (depending on applicability). 	<p>See section 11 “Emergency Response Locations (ERLs).”</p>
<p>Provision Layer 2 Switches and WLAN Controllers (if applicable)</p> <ul style="list-style-type: none"> Define the SNMP connections and LAN switch details in the EGW. Ensure that a Default ERL is assigned to each switch. 	<ul style="list-style-type: none"> Multiple records may be uploaded using batch files. Individual switches can be added from the Dashboard interface. <p>See section 15 “WLAN Discovery.”</p>

Task	Description and Reference
<ul style="list-style-type: none"> Determine if the EGW will scan all of the switches or only a subset of all possible switches. Set the Scan enabled parameter for the switches accordingly. Define SNMP connections for WLAN Controllers Ensure that a Default ERL is assigned to each WLAN controller. 	
Define layer 2 port discovery interval and SNMP Task Scheduler settings (if applicable) <ul style="list-style-type: none"> Define the intervals at which the EGW will discover the ports on the switches and the phones attached to these ports. 	See section 13 "Layer 2 Discovery".
Define WLAN Task Scheduler settings <ul style="list-style-type: none"> Define the intervals at which the EGW will discover the devices attached to wireless access points on your network. 	See section 15 "WLAN Discovery."
Install additional applications and services <p>If Intrado applications will be used to track users or respond to emergency calls (eg. ESL, RLM, Desk Alert) the applications must be installed in your Windows environment. For Desk Alert, security desk staff need to be trained on how to properly respond to alerts.</p>	<p>For more information see the document "Desk Alert Administrator User Guide."</p> <p>For more information concerning the ESL, see the document "ESL Installation and Configuration Guide."</p>
Identify unprovisioned phones (status=Call Center mode) <ul style="list-style-type: none"> Work to resolve problems that are preventing the EGW from locating these phones. Possible problems include: <ul style="list-style-type: none"> Phone is attached to a switch that is not defined in the EGW. Phone is attached to an unreachable switch. <p>Note: For Cisco deployments, provisioned layer 3 endpoints display as unprovisioned on the administrative Dashboard. Location routing is determined when 911 is dialed, using the phone's IP address.</p>	
Assign ERLs to specific switch ports that are different than the Default ERL for the switch.	<ul style="list-style-type: none"> Multiple records may be uploaded using batch files. Individual switch ports may be configured from the Dashboard interface. <p>See section 13 "Layer 2 Discovery".</p>

Task	Description and Reference
Assign ERLs to Access Points that are different then the default ERL for the WLAN Controller.	<ul style="list-style-type: none"> See section, 15.3 "Provisioning WLAN Discovery."
Add unsupported phones to the configuration (endpoints that are not automatically discovered by the EGW).	See section 12 "Endpoints."
Assign ERLs to IP subnets.	See section 14 "Layer 3 Discovery."
Work with off-site users to provision off-site ERLs using the RLM/ESL or other tools.	See section 17 "Provisioning Off-Campus Users."
<p>Adjust Advanced Settings</p> <p>If you will be using Layer 2 Discovery, ensure that the task is enabled. The task also needs to be enabled for third party SNMP data loaded via the Dashboard or FTP. For third party SNMP data ensure that the task Batch SNMP is also enabled to process data at the FTP.</p>	<ul style="list-style-type: none"> Enabling services (RLM, Layer 2, AXL, etc.) Timer settings Batch settings Task Scheduler <p>See section 9 "Advanced Settings."</p>

4.2 First Run Configuration/Activation

During first run activation you will configure the network settings, and apply your EGW license code in the feature activation screen. When you click on **Activate**, your license is validated by the Intrado Services licensing server. A manual activation process is also available for EGW servers that do not connect outside the corporate network.

For more information about Licensing, see section 2.3 "Licensing."



Note: If you are upgrading from a version previous to EGW 3.0, you will need to activate the EGW after you have completed the upgrade. The operation will be seamless and will simply require clicking on the Reactivate button. You can also perform a manual upgrade if you do not provide internet access to your EGW servers. For more information concerning upgrades, see section 19 "Maintenance."

To complete the first run activation, the following is required:

1. Configure network settings
2. Configure replication setup
3. Apply license code to the EGW Activation screen and click on **Activate**

4.2.1 Configure Network Settings

To configure the network settings

1. Click on **Network Configuration**
2. Configure the information included in the table below
3. Click on **Apply Settings**

Table 10: Network Settings

Field	Description	Note
-------	-------------	------

Server Type	Select primary, secondary, or standalone. Delegates the EGW instance as either the primary or secondary for redundancy. The EGW can also be activated without a Peer, in standalone mode.		If you are operating in Redundant mode, ensure that you configure one primary EGW server and one secondary EGW server. In standalone mode, only one EGW server is necessary, and replication setup is not required.
Hostname	Hostname for the EGW server. Eg. CompanyXEGWPrimary, CompanyXEGWSecondary.		
Domain name	Domain name for the EGW server. Eg. www.egw.com		
Interface 0	IP address	IP address assigned to Interface 0 on the EGW	The EGW has two NIC cards that can be configured to suit the needs of your networking environment. For more information see section 3.1.1 "Network Interfaces."
	Network mask	Network mask for Interface 0	
	Default gateway	Default GW for Interface 0	
Interface 1 (optional)	IP address	IP address assigned to Interface 1 (optional)	The EGW has two NIC cards that can be configured to suit the needs of your networking environment. For more information see section 3.1.1 "Network Interfaces."
	Network mask	Network mask on Interface 1	
	Default gateway	Default Gateway of Interface 1	
Primary DNS	IP address or FQDN of the primary DNS server for the EGW.		
Secondary DNS	IP address or FQDN of the secondary DNS server for the EGW.		
NTP Server	NTP server name(s) added to the pool. The format name: centos.pool.ntp.org. To add new server name click on Add Server. To delete server name click the delete button next to the server name.		

4.2.2 Configure 911 Administrator Password

After activating the EGW, the password for the "911admin" user must be configured. This is the password required to interface with the EGW via secure shell or SSH. Upon initial activation, the EGW is setup with the user name as **911Admin**.

Important: This is different from the user name and password that is required to log into the EGW dashboard.

Note: It is mandatory to setup a new password for EGW Releases 5.6 and above. For EGW releases below 5.6, it is not mandatory, but is highly recommended for security purposes.

To set the password:

1. Go to **System Status** → **Maintenance** → **Network Settings** → **911admin Password**.
2. Enter your new password in the **New Password** text box and confirm the password in the **Confirm Password** text box.

Password requirement: The password must contain a minimum of one character. There is no limit to the maximum number of characters. Alphanumeric and special characters are accepted.

3. Click the **Apply Settings** button.
4. If you have deployed the EGW as a redundant pair, then you must perform the above steps also on the Secondary EGW. The passwords must be kept identical.

Following the above configuration, to interface with EGW via SSH, you must enter the **User Name** as **911admin** and password as the one setup in Step 2.

4.2.3 Replication Setup

If you will be using the EGW in redundant mode, replication setup must be successfully completed before the activation process can take place. Replication setup is not required in standalone mode.

To enable replication setup

1. Enter the **Peer IP**
2. Enter the **Peer Hostname**
3. Provide the 911admin password that was configured in [4.2.2 Configure 911 Administrator Password](#).
4. Click on **Apply settings**

4.2.4 First Run EGW Activation

To activate the EGW

1. Copy the license key into the box provided
2. Click on **Activate**

If everything is ok, the EGW login page will be displayed and you will be prompted to login to the system using your default credentials.

If there was a problem with your license, the appropriate error notification is returned. You should contact your Intrado deployment engineer to resolve the licensing problem as expediently as possible.

4.2.4.1 Manual Activation

If you do not allow your EGW servers to connect outside of the corporate network you can manually activate the EGW.

To manually upgrade the EGW

1. Click on **Manual Activation**.
2. Copy the key displayed in the **Manual Activation Authentication** screen.
3. Provide this key to your Intrado support technician.
4. Obtain the Activation code from Intrado.
5. Paste the activation code into the appropriate field on the **Manual Authentication** screen.
6. Click **OK**.

4.3 Web-Based Dashboard

The EGW includes a web-based Dashboard which is used to provision/configure the system. System administrators may be assigned different administrative privileges based on the tasks they need to complete. The EGW is administered using three levels of access: Full, Provisioning and Limited (for more information see section 4.3.3 “User Management.”)

The EGW is assigned a default administrative account. The primary administrator has Full access privileges and is responsible to create administrative accounts with appropriate access levels for other system administrators.

4.3.1 Browser Requirements



Important: Please note that JavaScript must be enabled on every browser.

The Emergency Gateway administrative Dashboard can be accessed by many of today's popular web browsers. This section describes how to configure internet browser settings for use with the EGW.

Table 4-11 Web Browser Settings

Web Browser	Task	Steps
Internet Explorer 9, 10, 11	Set Browser Cache	<ol style="list-style-type: none"> 1. Click on Tools > Internet Options > Browsing History > Settings > Check for newer versions of stored pages 2. Click on the radio button Every time I visit the webpage
	Turn on active scripting	<ol style="list-style-type: none"> 1. Click on Tools > Internet Options > Security > Custom level > Scripting > Active Scripting 2. Set active scripting to Enable
Firefox 12 to 35	Enable java script	<ol style="list-style-type: none"> 3. Click on Tools > Options > Content. Click on Enable JavaScript
Windows 10 (Edge)	Default settings	

4.3.2 Logging On

The EGW administrator uses the default credentials (**username**: admin, **password**: admin) to login to the Dashboard for the first time.

To log on to the Dashboard

1. Type the IP of the EGW into your web browser
2. Enter the default username and password.



Note: Once the admin has logged in for the first time, LDAP directory authentication can be configured using MS Active Directory. To ensure that access to the EGW is maintained at all times, LDAP directory authentication cannot be used to authenticate the EGW administrative account.

4.3.2.1 Passwords

The EGW user passwords can be between 1 and 35 characters and no spaces are permitted. Passwords can contain alphanumeric characters, hyphens, and underscores.

4.3.3 User Management

The EGW administrator can define new users locally and assign them credentials and the necessary access level privileges (Limited, Provisioning, Full).

You can also setup Microsoft Active Directory authentication. In this case, the LDAP directory server authenticates the users and maps them to the correct access levels on the EGW. You can use existing user groups or create new user groups to map AD user group privileges to EGW access levels.

To manually add a user and assign to the appropriate access level

1. Click on **Configuration>Add an account**
2. Enter user information, username password and access level
3. Click on **Create**

For information concerning mapping LDAP Directory users to EGW access levels see section 4.3.4 “LDAP System, Directory and Authentication Settings.”

4.3.3.1 Access Levels

Access to the administrative Dashboard is regulated by three different levels of access (Limited, Provisioning, Full), which may be assigned by the default administrative account.

Table 12: Default Access Levels

Role	Description
Limited	Access to Provisioning Read only and Help
Provisioning	Includes same privileges as Limited, with additional access to validation and provisioning screens, reports, and status counters.
Full	Access to entire interface.

The following table illustrates the Dashboard resources available to the three default access levels:

X denotes that access is provided

Table 13: Access Level Resources

Privilege	Limited	Provisioning	Full
Provisioning	X	X	X
• ERLs	X*	X	X
• Endpoints	X*	X	X
• ELIN Pool		X	X
• NENA 2			X
Auto Discovery		X	X
• Layer 2 Discovery		X	X
• Layer 3 Discovery		X	X
• WLAN Discovery		X	X
System Status			

Privilege	Limited	Provisioning	Full
• Status		X	X
• Logs			X
• Reports		X	X
• CDRs			X
• Alarms			X
• Maintenance			X
Configuration			X
• Dashboard			X
Account			
• IP-PBX			X
• Security Desk			X
• Notification			X
• Advanced			X
• Access Management			X
• Task Scheduler			X
• Certificates			X
Test Mode			X
Desk Alert			X
Help	X	X	X

*Search and View More Details only. Add, Edit, delete or ERLs and endpoints is prohibited for the Limited user.

4.3.4 LDAP System, Directory and Authentication Settings

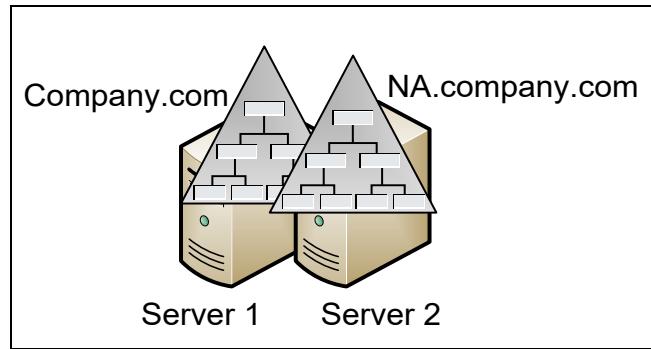
A Microsoft Active Directory (LDAP directory) server can be used to authenticate the users and map them to the appropriate access level group on the EGW.

You can continue to use the local directory to define EGW users, in conjunction with using LDAP for authentication and access level management. For example, the default administrative account on the EGW is granted Full access privileges and cannot be deleted or managed via LDAP.

4.3.4.1 LDAP Directory settings

You can use the directory settings to configure the network and authentication settings for your LDAP servers.

The EGW can support multiple LDAP directories running on redundant servers. The EGW can be configured to find the directory's LDAP servers using DNS SRV, or the directory's LDAP servers can be specified manually by IP or fqdn.



To add a new LDAP directory and configure the settings:

1. Click on **Configuration>Access Management>LDAP**
2. Click **Add**
3. Specify the settings based on the parameter definitions in the table

Table 14: LDAP Configuration

Domain name	Domain name of the LDAP directory.
Default directory	Specify if this is the default LDAP Directory. The default directory is the directory the EGW will query first when users are authenticated remotely. This is also the domain that will be used if no domain is specified by the user when they try to login to the EGW.
Use DNS SRV	If checked, the EGW will use DNS SRV to lookup the servers that are associated to the domain. This depends on a valid DNS SRV configuration at the EGW network settings. For more information see section network settings
Base DN	This parameter is used to restrict the scope of the LDAP search.
LDAP Servers	If DNS SRV is unchecked, you can manually specify the fqdn or IP of the servers assigned to the LDAP directory domain. You can specify what port to connect on. By default, TLS communication runs over port 389 and SSL communication over port 636. These port numbers can be changed according to the LDAP server configuration. You can choose any of the LDAP protocols, either TLS or SSL, for a secure communication. If you choose none of them (none is selected by default), the transmission is not encrypted (and the communication is not secure). Refer to section 4.3.6 "LDAP Server Certificates", if you choose none . You can add as many LDAP Servers as you want.



Note: For the LDAP authenticated user the "Dashboard Account" tab under "Configuration" is not available.

When an LDAP user signs in to the EGW dashboard, he is not allowed to create or edit dashboard accounts. On the Configuration/Dashboard Account page, he will just see the details of his own account, without having the option to add a new account or modify his own account.

4.3.4.2 LDAP Field Equivalence

You can use these settings to specify the LDAP field equivalence to be used when granting user access to the EGW. The settings are also used to map corporate directory Groups to the existing access level groups at the EGW (Full, Provisioning, Limited).

To configure the field equivalence

1. Click on the domain to be edited
2. Click on **Edit**
3. Uncheck the Use Defaults parameter to make changes
4. Enter the field equivalence mappings as required

EGW to LDAP field equivalence:

The default setting is specified in the table below. You can change the default settings to specify the fields which will be used during remote user authentication.

Table 15: EGW to LDAP Field Equivalence

Username	SAMAccountname
First name	given name
Last name	last name
email	mail

If you uncheck the **Use Defaults** box, the table expands and you can see and modify the specified values.

EGW access level equivalence:

The default setting is specified in the table below. If the default setting is used, the EGW will expect user groups with the same naming to exist in the LDAP directory. You can also use pre-existing LDAP directory groups, or create new groups by specifying them here.

Table 16: EGW Access Level Equivalence

Full	E911AccessLevelFull
Provisioning	E911AccessLevelProvisioning
Limited	E911AccessLevelLimited

4.3.5 Modifying Default Access Levels for Limited and Provisioning

It is possible for the main administrator to modify the default access levels for Limited and Provisioning. This is done by configuring **Menu Access** and **User Access** settings. **Menu Access** settings control access to the Dashboard menu items. **User Access** settings control access to downloadable media that are available from the various Dashboard screens (e.g. call recordings from the CDRs screen).

To configure **Menu Access** settings

1. Click on **Configuration > Access Management > Menu Access**
2. Click the access level that you would like to modify. Choose **Limited** or **Provisioning**.
3. In the **Menu Access Management** table select the items you want to assign to the Access Level role* (Limited or Provisioning).



Note: The default values for each Access Level are highlighted in blue. To add items to the Access Level, select the value(s) with CTRL+click.

4. Click on **Save**.

*selection of a child menu will automatically result in the selection of the parent menu (s).

To configure **User Access** settings

1. Click on **Configuration > Access Management > User Access**
2. Check the dialog box for the resource(s) that you would like to enable for the Limited or Provisioning Role eg. "Display CDR Call Recordings".



Note: You can allow access to both Limited and Provisioning user in the same time.

3. Click **Save**.

4.3.6 LDAP Server Certificates

LDAP Certificate can be installed through the EGW Dashboard. The certificates can be added or removed at the level of LDAP directory.

Browse for the certificate you want to install and click on **Install Certificate**. The certificate will be installed at the right place for the chosen LDAP directory. If you click on **Remove Installed Certificates**, all previously installed certificates for the chosen directory will be removed.

Installing a LDAP Certificate is required only if the LDAP communication is not encrypted.

4.4 Server Certificates

The EGW supports SSL authentication and encryption, allowing clients to identify the EGW server over the network. The EGW server can be identified using a default self-signed certificate, or a certificate signed by a trusted third-party Certificate Authority (CA). If a trusted CA certificate will be used, it is necessary to generate a certificate request via the EGW Dashboard. Once the certificate has been obtained from the CA, it is uploaded to the Dashboard.

The use of trusted CA certificates has the following steps:

- Generate the certificate request
- Submit the certificate request to the CA
- Install the server certificate from the CA

4.4.1 Generate the Certificate Request

A server certificate request generates a .csr file which may be delivered to the CA of your choice to obtain a signed certificate.

To generate a .csr file, it is necessary to enter descriptive information used to identify your organization at the CA. The CA will use the submitted information to positively confirm the identity of your organization. The information is described in the following table.

Table 17: Generate Server Certificate

Parameter	Description	Notes
Common name	Should be filled in with the server name (FQDN) on which the web site will be answering requests. Ensure that the information is entered	e.g. A certificate for the domain "domain.com" will receive a warning if accessing a site named

	correctly. If the server's name in the URL being requested by a client does not match the common name in the certificate presented by the server, the client will show an error to the user.	"www.domain.com" or "secure.domain.com", because "www.domain.com" and "secure.domain.com" are different from "domain.com".
Domain name	Name that will be used as the filename of the generated certificate request files (.key, .crt, .csr). In most cases, the domain name will correspond with the common name. Some CAs stipulate that the common name and domain name must be identical.	e.g. If you intended to secure the URL https://www.egw.com, then the domain name is usually egw.com. However, any valid filename is accepted. Do not use the character /
Organization	Name that is associated with the organization.	e.g. ABC Telecom Inc.
Organization unit	You may use this field to further distinguish the group that is using the certificate.	e.g. Marketing department, or sales.
Country	Country where the organization is located.	Use the 2-character ISO format country code. Do not use punctuation.
State or province	State or province in which the organization is located.	Do not use abbreviations.
City or locality	City or locality in which the organization is located.	Do not use abbreviations.
Email	Email address that will be associated with the certificate request.	Optional.

To generate a certificate request

1. Click on **Configuration > Certificates > Generate Server Certificate**
2. Fill in the fields of the Generate Server Certificate request form (see table)
3. Click on **Generate Server Certificate**.

When you click on **Generate Certificate Request**, the EGW will generate three separate files, which will be accessible from the **Generate Server Certificate** screen: Key file, Certificate file (.crt) and Certification Request File (.csr). The .csr file is the file that will be provided to the CA for verification.

Table 18: Server Certificate Files

Parameter	Description	Notes
Key file	Private key file that is generated for the certificate request. Must be paired with a public key for SSL encryption to function correctly.	Egw.com.key
Certificate File	Self-signed certificate file that is generated by clicking on Generate Certificate Request . To obtain a signed certificate, you must submit the .csr file to the trusted CA of your choice.	Egw.com.crt
Certificate Request File	Certificate request file that can be sent to the trusted root CA. The public portion of the public/private key pair.	Egw.com.csr

--	--	--

4.4.2 Submit the Certificate Request to the CA

After you have generated the certificate request file, the next step is to submit this file to a third party CA of your choosing (VeriSign, GoDaddy etc.).

To submit the .crt file

1. Make contact with a trusted CA and familiarize yourself with the methods which are required to submit the .crt file.
2. Open the .crt file that was previously generated (click the link directly from the Dashboard interface).
3. Copy the contents of the certificate request file.
4. Paste the contents into the appropriate submission form provided by your CA.
5. Follow all remaining CA procedures to finalize your submission.

4.4.3 Install the Server Certificate

Once the CA has confirmed the identity of your organization, they will issue you the certificate that was requested (this is typically performed via email). The email sent from the CA will include the certificate, which can be uploaded to the EGW.

Note: The recommended format for certificate download from the CA is Base 64 encoded. It is especially important to download the certificate in Base 64 encoded format if you are using Windows IIS Server.

To upload the signed certificate:

1. Click on **Configuration > Certificates > Install Server Certificate**
2. In the Certificate file field, click **Browse**
3. Browse to the location of the certificate and upload
4. Upload the private key file and/or chain file if required*
5. Click on **Install Server Certificate**
6. You should see the message “The current EGW certificate will be overwritten. Would you like to proceed?”
7. Click **Yes** and the new certificate is installed

The table below describes the **Install Server Certificate** options:

Table 4-19 Upload Server Certificate Files

Parameter	Description	Notes
Private key file (optional)	Upload saved private key, in the scenario where the certificate file does not match the current private key.	You can upload a private key if the current private key does not match the certificate issued by the CA. This scenario occurs when multiple certificate requests have been made to a CA. The EGW creates a new private key for each certificate request, and can only manage one private key at any one time. The default setting should be to leave this field blank. You should only upload a private key if your certificate and current private key do not match.
Certificate file	Upload the signed certificate issued by the CA.	

Chain file	Only to be used if your CA is part of a web-of-trust (WOT) network. In this case, the CA that issued the certificate is not the root CA. There is at least one other CA that is more trusted in the chain-of-trust.	
------------	---	--

Revert to default certificate: In the absence of a trusted CA certificate, a self-signed certificate can be used. In this scenario, the server signs its own certificate: no other machines trust the signer of the certificate by default.

5 Configuring Call Routing

Once the network infrastructure has been put in place for your EGW, you will need to setup the EGW with the call routing applications, components, and services that are required to meet the needs of your environment. There are numerous applications and features that can, and in some cases must, be deployed on the network infrastructure.

The following call routing components and features are available

- Call routing to the ERS
- Local trunking
- Callbacks
- Security desk call routing
- Multiple dial plan
- Test mode
- Mis-dial protection
- Nat Traversal

5.1 Configuring Basic Telephony and Networking Settings

You must configure the EGW so that it knows where to route emergency calls. It is also necessary to configure the EGW with the numbers that will be used for emergency calls (e.g. 911) and the phone numbers it should use as callback numbers and/or Emergency Location Identification Numbers (ELINs).

5.1.1 ERS Account Settings

Organizations that deploy the ERS must configure the appropriate settings in the EGW. The ERS Account settings establish connectivity between the EGW and the ERS for provisioning and call routing. A SIP connection is used for 911 call routing, and SOAP is used to validate emergency records (ERLs) with the address validation service.

To access the ERS Account settings

- Click on **Configuration > Advanced > ERS Account**

Table 20: Account Settings

Parameter	Description
Log SOAP Calls	Yes/No If enabled, a log of all SOAP calls between the EGW and ERS are logged.
ERS Primary IP/ FQDN/ Hostname	Primary call route for SIP 911 calls.
ERS Secondary IP/ FQDN/ Hostname	Failover call route for SIP 911 calls.
ERS Tertiary IP/ FQDN/ Hostname	Secondary failover for SIP 911 calls.
Network Protocol	TCP or UDP For customer that sends a location object (LO) to ERS using EGW (eg. PIDF-LO), setting must be TCP.
ERS Version	Dropdown will select either ERS 2.x or 3.x
SOAP Username	Username that is used to identify the EGW client in order to establish the web services interface with Intrado.
SOAP Password	Password that is used to identify the EGW as a trusted client.
Account ID	This is the Account ID generated for this EGW Customer on ERS 3.x. Its format is 12 hexadecimal characters, followed by a hyphen, followed by 4 hex characters, followed by a hyphen, followed by 4 hex characters, followed by a hyphen, and followed by 12 hex characters. It is required for authentication with ERS 3.x.
Token	This is the Token generated for this EGW Customer on ERS 3.x. It has the same format as the Account ID.
Location Determination Method	SIP Field used by the ERS to identify the location of the subscriber: <ul style="list-style-type: none"> • EGW_LK • FROM_EXT Dropdown will select either: EGW_LK, FROM_EXT LDP specifies the SIP field which will be used by ERS 3.x to identify the location of the EGW subscriber.
Default Customer Name	Default Name for the customer. Only available if ERS 3.x is selected. A maximum of 32 characters are accepted in this field.
SOAP Authentication Username	Basic Auth Username to connect to Intrado.
SOAP Authentication Password	Basic Auth Password to connect to Intrado.
SOAP Server URL	URL of Intrado Provisioning server.
CPM Unprovisioned Calls Route	Parameter that determines the route to the ECRC for unprovisioned calls. If PBX is selected, the call will be routed back to the PBX system for delivery to the ECRC via the PSTN. If Intrado is selected the call will be routed to the ECRC via the ERS using SIP.
Proxy Enabled	Setting that enables/disables the EGW to connect via web proxy.

ECRC (Emergency Call Response Center) List

911 calls are sent to the Emergency Call Response Center (ECRC) when call routes between the EGW and the ERS are unavailable. The numbers displayed in the **ECRC List** are used by the EGW to route the call to the ECRC. You can provision more than one ECRC number and it can have varying digit lengths.

In addition, using the ECRC List, you can prioritize which ECRC you want the unprovisioned call to reach first, second and so on.

In local trunking deployments the ECRC numbers can be used to deliver unprovisioned calls to the local emergency network, or to an on-site security desk. In this scenario, the ECRC number can represent the extension of a

security desk, or the Local gateway prefix for a route to a PSTN gateway or session border controller (SBC). When the local gateway prefix is used, the ELIN is not sent to the gateway.



Note: In worldwide mode, only the ECRC List is available. The ECRC numbers are meant to specify phone numbers that route to the local PBX for termination (eg. To an on-site private answering point or other fallback destination).

5.1.2 Callback Settings

The callback settings allow you to configure the 10-digit phone numbers that will be used for the Extension-Bind feature.

When you configure Extension-Bind numbers and callback settings you can specify the following:

- DID numbers that will be used for 911 callbacks.
- Duration of time that a DID will remain bound to the telephone that dialed 911.
- “Use 10 digit for Callback” setting. If a phone has a 10 digit DID then the 10 digit number sent to the EGW will be used as the callback number if this parameter is set to Yes.
- RegEx exceptions to “Use 10 Digit for Callback” parameter setting (digit match on regex string will invoke Extension-Bind, even if the phone has a ten digit number)

To configure callback settings

1. Click on **Configuration > Advanced > Callback**
2. Click **Add a number** under **Extension-Bind Numbers**. You can specify an individual number or a range of numbers. For example, if you enter 123456789x the following range is added: 1234567890-1234567899
3. Configure the **Extension-Bind Duration** and **Use 10 Digit for Callback** settings
4. Configure RegEx exceptions (if applicable)

The Extension-Bind duration should be set with consideration given to the size of the deployment and the amount of Extension-Bind numbers. Capacity requirements dictate that 10-15 Extension-Bind DIDs should be allocated for up to 20,000 users. The recommended duration setting is 15 minutes.

The **Use 10 digit for Callback** parameter determines how callback numbers will be provided to the PSAP.

- If a phone is assigned to an ERL with an ELIN, the ELIN is used as the callback number, regardless of the parameter setting.
- If there is no ELIN, the Extension-Bind feature is used for the callback unless **Use 10 digit for Callback** is enabled.
- If **Use 10 Digit for Callback** is enabled, the phone’s 10-digit number is used as the callback number (unless the 10 digit number is included in the specified RegEx). This setting is only applicable if the phone is assigned a 10-digit number.



Note: If your deployment includes ELIN numbers and no Extension-Bind numbers, then the Extension-Bind duration parameter is used to govern the amount of time that ELIN numbers remain bound to the stations (phones) that dial 911.



Note: In worldwide mode, there is no Callback Settings screen. The Extension Bind duration parameter is available from the Global settings screen, and determines the amount of time that ELIN numbers remain bound to the stations that dialed 911. The Extension-Bind feature is not available in worldwide mode.

5.1.2.1 RegEx Exclusion List

The specified exclusion list takes precedence and is triggered by the specified RegEx digit strings. For

Example: `^89(\d){8,8}$`

In this example, the EGW recognizes any CLIDs that begin with 89 and applies the Extension-Bind setting, regardless of the “Use 10 Digit for Callback” setting.

The feature is useful in circumstances where the global Callback configuration does not capture exceptions such as a main number (billing number) phone mask being sent to the PSAP as the callback number. With the exception list configured, the EGW recognizes the main number and dynamically binds an Extension-Bind number, enabling the PSAP to callback the station directly.

Another typical use case is a deployment with a range of valid DIDs mixed with a range of DIDs that you would like to apply ELINs to. In this case, for the ELIN phones, a regex exception to the “Use 10 Digit for Callback” setting.

For example: A company has a range of phones that should use ELINs. The range of numbers comprises any numbers that match the following NPA NXX (XXX-0XX-XXXX or XXX-1XX-XXXX).

The following regex can be used:

`^([0-9])\{3,3\}([0-1])\{1\}([0-9])\{6,6\}$`

Description:

(^ Matches at the start of the string, ([0-9]) Accept anything from 0-9, {3,3} use only for the first three numbers, ([0-1]) Accept Anything from 0-1 only, {1} use only for 1 digit, ([0-9]) Accept anything from 0-9, {6,6} use only for six digits, \$ Matches at the end of the string)

To configure a Regex exclusion list

1. Click on **Configuration>Advanced>Callback**
2. Configure Extension-Bind settings as elsewhere described
3. Under **Callback Settings** click **Edit**
4. Using the field **Except for numbers in this RegEx**, configure the applicable Regex. Example: `^89(\d){8,8}$`

5.1.2.2 Digit Manipulation

You can configure the EGW to perform digit manipulation on the DNIS for incoming calls from the IP-PBX to the EGW (eg. Callbacks). The digit manipulation can be used to map an incoming digit string to the callback number of the station that dialed 911. This will allow you to either append/prepend, or trim digits to/from the digit string that reaches the EGW to accommodate PBX or gateway needs.

The following diagram illustrates an example scenario:

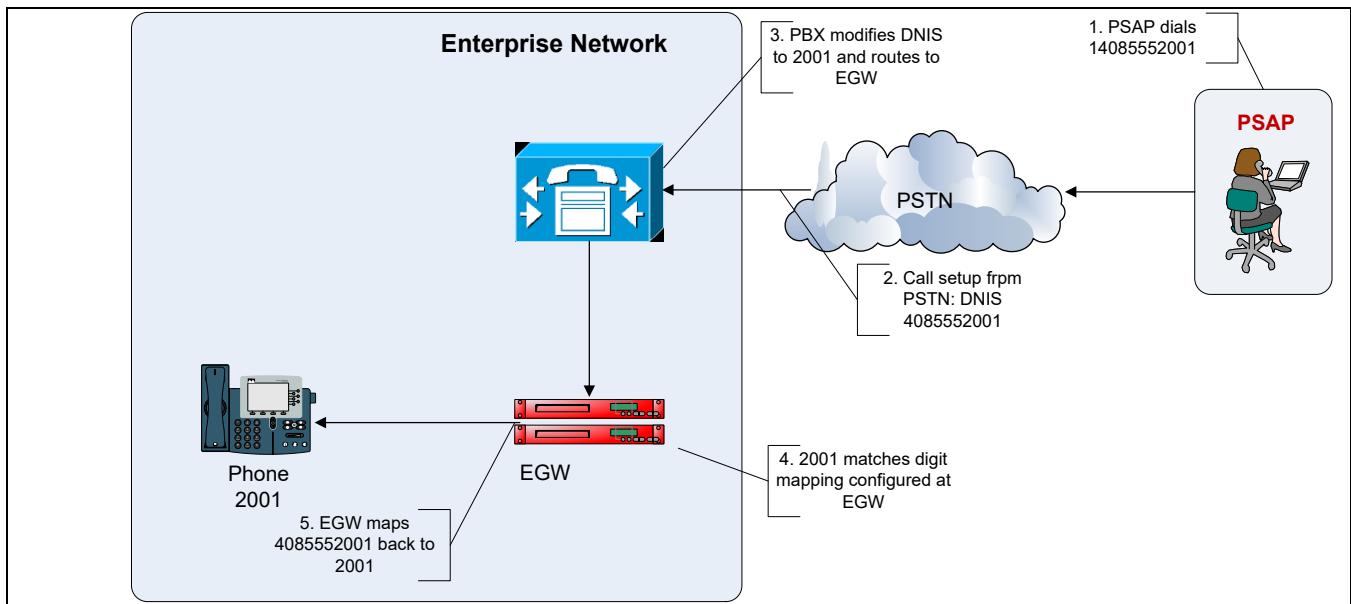


Figure 23: Digit Manipulation Configuration

To configure digit manipulation at the EGW

1. Click on **Configuration>Advanced>Callback>Add a Digit Map**
2. Configure the fields as described in the table below

Table 21: Configuring Digit Manipulation

Field	Description	Example
Pattern	Must be regular expression (RegEx).	[0-9] {4} -this regex would match any 4 digit extension.
Left Trim	Enter number of digits to trim from left of DNIS	Eg. Digit strip
Right Trim	Enter number of digits to trim from right of DNIS	Eg. Digit strip
Prepend	Enter digits to prepend to the DNIS.	Eg. Prefix. Original DNIS: 888 Prepend: 21 Result: 21888
Append	Enter digits to append to the DNIS.	

5.1.3 Understanding How Callbacks work with the ERS

To understand how callbacks work, it is instructive to examine both an outgoing and incoming call. During the outgoing call, the EGW stores a mapping between the extension that dialed 911 and its Extension-Bind number (if Extension-Bind is enabled). Route patterns are configured on the IP-PBX for each Extension-Bind number, directing callbacks to the EGW when they enter the enterprise calling network. When the callback arrives at the IP-PBX, it is routed on IP trunks to the EGW. The EGW then initiates a new call leg to the extension that dialed 911.

The following diagrams illustrate how callbacks work using the ERS.

For information on callbacks and local trunking, see section 6 “Configuring Local Trunking (LEC Call Routing).”

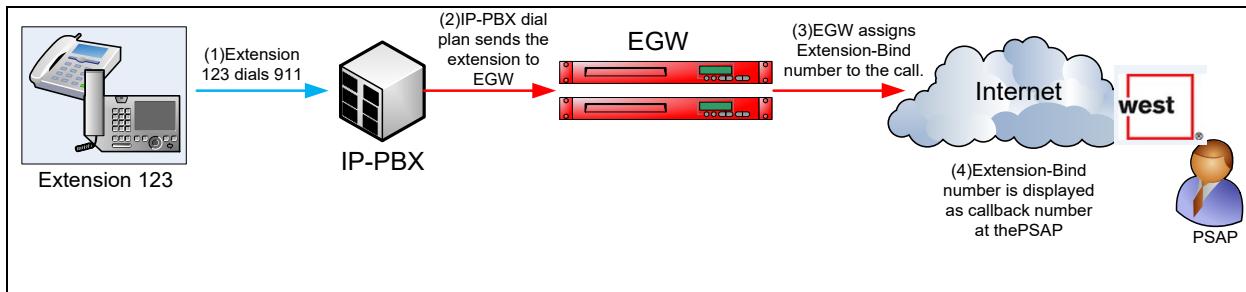


Figure 24: Outbound 9-1-1 Call to ERS

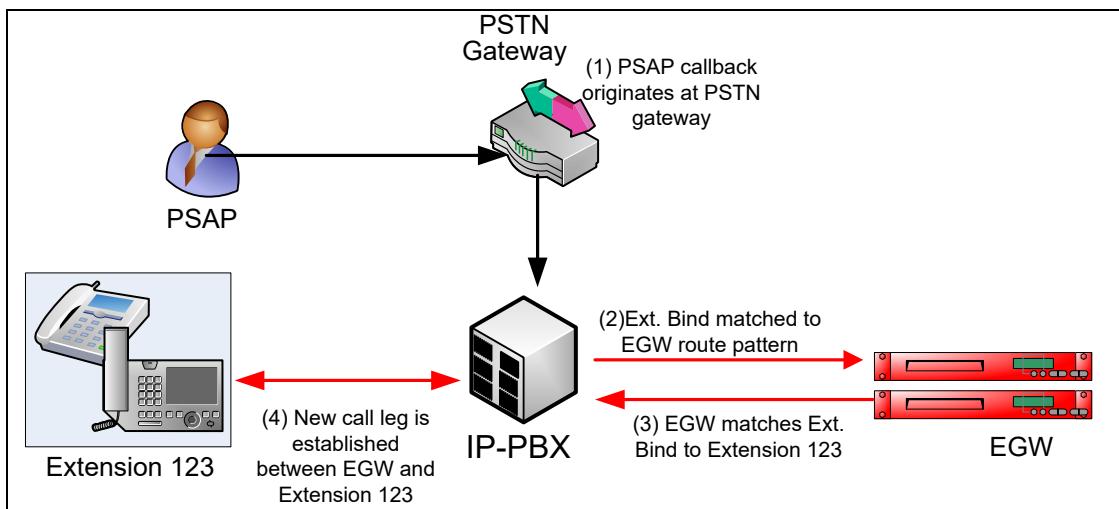


Figure 25: Inbound Call from PSAP to Extension

5.1.4 NAT Traversal

Depending on how you have deployed the EGW in your network, the transparent NAT traversal feature may be useful if your firewall/packet filter is unable to support application layer inspection of SIP packets. The inability of the corporate firewall to inspect SIP traffic often leads to blocked or dropped SIP packets and interferes in establishing connectivity between the EGW and the ERS.

To enable the Transparent NAT Traversal feature, the EGW is deployed using a single internal (inside) interface with a private IP. The public IP of the packet filter/firewall is configured at the EGW. The EGW is also configured with standard internal/private subnet ranges to enable communications with inside resources (eg. PBX systems during 3 way calling etc.). Custom inside subnets may also be added.

5.1.4.1 Configuring Transparent NAT Traversal

To configure Transparent NAT Traversal

1. Click on **Configuration>Advanced>NAT Traversal**
2. Configure the parameters as described in the table below

The following table describes the parameters that are configured to enable Transparent NAT Traversal at the EGW.

Table 22: Transparent NAT Traversal Configuration

Parameter	Description	
Transparent NAT Traversal	Yes or No. No is Default and Recommended setting.	
Primary Public IP	Public IP of the firewall. The EGW will send the SIP packets to the firewall with the source address as the appropriate public IP (public IP of the firewall).	When SIP/RTP returns from the ERS to the Enterprise network, communications are addressed to the public IP of the firewall, enabling SIP to pass “transparently” through the firewall back to the EGW.
Secondary Public IP	Public IP of the firewall serving the secondary EGW server. If both EGWs are in the same data center will be the same as Primary Server Public IP. If secondary EGW is at another data center, will take the public IP of the firewall serving that EGW.	
PBX Subnet	Inside Subnets from which PBX communications can originate to the EGW. Enables EGW to communicate with inside resources without using NAT.	The following standard ranges are the Default setting. From 10.0.0.0 to 10.255.255.255 From 172.16.0.0 to 172.31.255.255 From 192.168.0.0 to 192.168.255.255

5.2 EGW Dial Plan

The EGW is capable of supporting multiple emergency numbers with unique destinations and call route policies. Calls to emergency numbers can egress the corporate network for delivery to the ERS network or to the local emergency network via the LEC. It is also possible to configure an emergency number that only routes calls to an on-site responder such as a PEAP. In addition to emergency numbers, you may also add non-emergency numbers to the EGW's dial plan for security desk call routing, or routing to a test mode recording.

5.2.1 What Happens when a Dial Plan number is dialed?

When a number from the dial plan is dialed, the EGW determines the call route associated with that number. There are three possibilities: emergency routing, security desk, or test mode. The EGW then attempts to reference the call to the appropriate ERL record. The ERL record contains the emergency location for the call and may also contain specific call route policies. Based on the dialed digits and the ERL, the EGW completes the call to the appropriate destination.

The diagram below illustrates a sample configuration. The configuration has the following dial plan numbers:

- 911 is the emergency number (ERS routing)
- 711 is a test mode number
- 511 is a security desk number

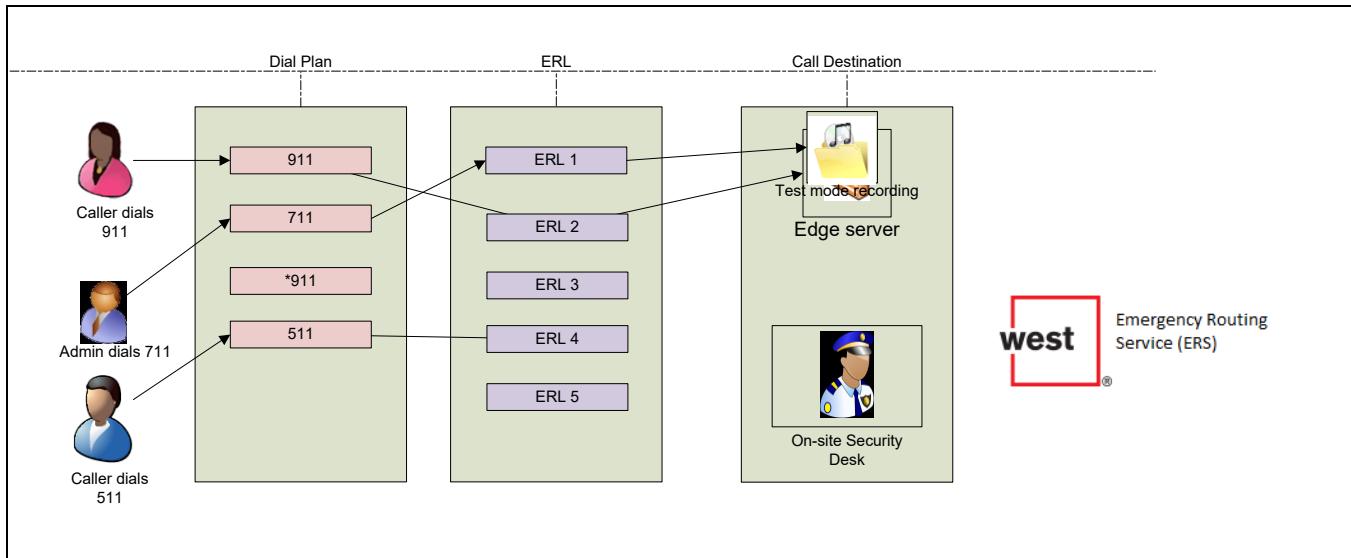


Figure 26: Call Instances

5.2.2 Configuring the Dial Plan

Dial Plan numbers are added to the system and configured with a specific destination (emergency routing, security desk, or test mode).

To add a number to the dial plan:

1. Click on **Configuration > Advanced > Dial Plan**
2. Click on **Add a number**
3. Enter a Dial Plan **Number***
4. Select the appropriate **Route Plan** (emergency routing, security desk, test mode)
5. Select **Yes** or **No** for **Notifications Enabled**.

Enabling/ Disabling Notifications

The **Notifications Enabled** parameter enables you to choose whether notifications are sent. The parameter chosen in the **Route Plan** combined with the **Yes** or **No** in the **Notifications enabled** section will determine if Crisis Email Alerts/ Unprovisioned Email/ Off Campus email alerts or Test Mode email alert are sent.

For example, when the **Notifications Enabled** is set to **No** and an unprovisioned call is made, an email alert will not be sent.

Also, if for Test Mode Route Plan, the **Notifications Enabled** is set to **Yes** and test calls are made, a Test Call Notification email will be sent. Alternatively, for a Test Mode Route Plan, if the **Notifications Enabled** is set to **No**, and test calls are made, the Test Call Notification email will not be sent but the Test Mode email alert will be sent.

*For Cisco deployments, enter the **CTI DNIS** that applies to the Emergency Number (e.g. *511)

Note: For Cisco deployments with the CTI DNIS Redirected per dial plan, in addition to entering the **CTI DNIS**, you also need to add a **CTI Redirect DNIS** or the **RDNIS**.

Security Desk

If the setting is security desk, a **Default Security Desk** can be selected in the event that the call is unprovisioned. The default security desk field can also be set to **None**. This may be the preferred setting for large multi-site deployments with multiple security desks, where it may not be helpful to send unprovisioned calls to the default security desk (e.g. security desks/operators are only equipped to handle calls from a specific location).

5.2.3 Misodial Protection

In many enterprises, callers must dial “9” to reach an outside line and “1” for long distance. This can result in instances where “911” is dialed by mistake, and an emergency call is routed.

The Misodial Protection feature works by playing a short recording in advance of setting up the emergency call to the ERS. If the caller hangs up before the recording expires, the 911 call is not routed.

The recording says “Please stay on the line as we connect you to Emergency Services.” Optionally, the recording can include the line “You have dialed 9-1-1.”

This feature is available on all PBX systems, including generic PBXs. The following characteristics are applicable:

- Feature can be enabled for calls to the PSAP, or for calls routed to both the PSAP and Security Desk.
- “You have dialed 911” recording can be turned-on/off (for enterprises that use an emergency number other than “911”).
- Misodial protection recording is included in CDRs and test mode CDRs.

To configure Misodial Protection

- Click on **Configuration > Advanced > Dial Plan**.
- Select a value from the **Enable Misodial Protection** drop down box: **Disabled**, **Enabled (exclude Direct Delivery Calls)***, **Enabled**.
- Set **Prepend “You have dialed 911” Recording** to Yes or No**

*If **Enabled (exclude Direct Delivery Calls)** is selected, the Misodial Protection feature will not work for 911 calls that are only routed to on-site security desks (e.g. no PSAP call routing).

** Enterprises with dial plans that do not use 911 as the emergency number do not use this feature.

5.2.4 Override ERL Security Desk Number

Many enterprises would like to have the ability to specify a Security Desk number at the dial plan level. This will enable the EGW to send calls to different groups in order to prioritize them accordingly.

This feature will prevent all the calls from going to the unique Security Desk number specified in the ERL.

This feature is available on all PBX systems, including generic PBXs. This feature enables the EGW to use the default security desk defined at the dial plan when the route plan is selected to be Security Desk when either of the following case applies:

- The ERL does not have a Security Desk number configured
- The ERL does have a Security Desk number configured but the override functionality is enabled.

To override the ERL Security Desk Number:

- Click on **Configuration > Advanced > Dial Plan**.
- Select **Security Desk** from the **Route Plan**.

- Select the **Default Security Desk**.
 - Set **Override ERL SD** to **Yes**.

This will override the ERL Security Desk number

5.3 Test Mode

The EGW contains a **Test Mode** functionality enabling users to verify call flow through the EGW, verify 2-way audio quality and also verify location information. Test calls are typically routed to a recording through the EGW or the ERS.

Users can also configure to receive email notifications when a test call is made. Test calls are recorded under **Test Mode** → **CDRs**. The CDRs report the call as provisioned or unprovisioned and also report the call destination as EGW or ERS. Users can also enable the security desk to monitor the test calls.

The following test mode types are available. Users can choose one or multiple selections based on the needs of a specific deployment:

- **Endpoint:** Endpoints are assigned for making test calls. When callback settings are configured (i.e. assigned ELIN or Extension-Bind feature is enabled), it is possible to callback this test endpoint.
 - **Dial Plan:** Dialed number is configured to route the test call to the test recording.
 - **IP-PBX Server:** Entire PBX Servers are added to the test mode. Whenever a call is made from this PBX Server, it will be treated as a test call and routed accordingly.

General Settings: Enter email addresses here if you wish to receive email notifications when a test call is made. When entering two or more email addresses, they need to be separated by a comma but a space is not allowed. For example: JohnSmith@abc.com,JaneSmith@abc.com

Test Modes List: This section displays all the test modes that are configured in the EGW.

The following points apply when configuring the Test Mode:

- When the call destination is chosen as EGW, a voice recording with the following message is heard: *"You have successfully placed a 911 test call, your callback number is #####.###."*
 - When the call destination is chosen as ERS, a voice recording similar to the following message is heard: *"Welcome to the automated test system. Your account is in Live (Demo or Maintenance) mode. Your location is provisioned. The location coverage is Public Safety Answering Point. Your address is <House Number>, <Street Name>, <City>, <Province>, <Country>, <ZIP Code>."*



Note: Address information in test notification emails takes on the settings of the multiline address template. You can customize the multiline address template to add address field labels, or to modify the PIDF-LO address fields which comprise the address information output. For more information see section 8.7 "Customize Address."

5.3.1 Configuration

Click on **Add** under **Test Modes List** to add a test mode.

The menu selections will change depending on the choice you make under **Test Mode Type**.

The following fields should be configured:

Table 23: Test Mode Configuration

Field	Description
Test Mode Name	Enter a name to easily identify the test mode
Test Mode Type	Choose from Endpoint and IP-PBX Server <ul style="list-style-type: none"> • To add a test endpoint, refer to 5.3.1.2 Adding Test Endpoint • To add a test IP-PBX Server, refer to section 5.3.1.1 Adding a Test IP-PBX Server • To add a test Dial Plan, refer to section 5.3.1.3 Adding Test Dial Plan
Test Mode Enabled	Setting to enable or disable test mode.
Call Destination	Determines which IVR to route the test call. Choose from EGW, ERS, ERS Primary, ERS Secondary and ERS Tertiary. <p><i>Note: When ERS is chosen, the calls can failover to the ERS Primary, Secondary or the Tertiary. However, when the ERS Primary, ERS Secondary or ERS Tertiary is chosen, failover is not possible.</i></p>
Security Desk Monitoring Enabled	Setting to enable or disable the security desk from monitoring the test calls.

5.3.1.1 Adding a Test IP-PBX Server

When **IP-PBX Server** is chosen as the **Test Mode Type**, the following additional fields become available for configuration:

- **IP-PBX**: Choose from the list of IP-PBXs already configured.
- **IP-PBX Server**: Choose from the list of IP-PBX servers

5.3.1.2 Adding Test Endpoint

When **Endpoint** is chosen as the **Test Mode Type**, the following additional fields become available for configuration.

- **Extension (range allowed)**: Enter a single extension or an extension range here. To add a range, separate the values by a hyphen (-). For example, 20500-20505
- **Username or MAC address**: Enter the username or the MAC address or both. All the valid entries here will be set to test mode. When adding multiple usernames or MAC addresses, separate them with a comma.

When a range of endpoints are added, they will appear as distinct rows in the **Test Modes List**.

Please note that when an endpoint is edited, the **Extension**, **Username** and **MAC address** fields collapse into the **Endpoint** field. Here, only a single extension, username or MAC address can be added.

5.3.1.3 Adding Test Dial Plan

Test dial plan is added through the Dial Plan tab (**Configuration** → **Advanced** → **Dial Plan**).

For detailed information on this procedure, please refer to section [5.2.2 Configuring the Dial Plan](#).

After the test dial plan is configured, it appears under the **Test Modes List**. To edit this test dial plan:

1. Click on the dial plan from the list
2. Only the following fields can be edited:
 - a. **Call Destination**
 - b. **Security Desk Monitoring Enabled**.

Please note that test dial plans cannot be deleted from the **Test Mode** tab.

5.3.2 CDRs

Test mode CDRs report on the same parameters as standard CDRs. Test mode CDRs may be viewed by clicking on **Test Mode > CDRs**.

5.4 Configuring Emergency Conferencing and Security Desk Routing

The EGW supports various emergency call routing use cases such as Security Desk Call Routing and Emergency Call Conferencing (multi-party emergency call bridging).

The EGW supports the following features:

- Creating a single or multi party emergency conference call with or without call termination to the PSAP
- 3 way calling (security desk routing)
- Support for Land Mobile Over Radio (LMR) trunks
- Misdial Protection
- Call recording
- Capability for Users to put call on/off hold
- Support for Multiple Dial Plans (emergency and non-emergency numbers)

This section covers the following

- Understanding Emergency Conferences and Security desk call routing
- Configuration Requirements
- Limitations

5.4.1 Understanding Security Desk Call Routing and Emergency Call Conferencing

The EGW can bridge emergency calls to multiple parties. For an emergency call, it is possible to route calls to one or more participants (security desk, medical, facilities etc.), with or without termination to the public safety answering point (PSAP).

This flexibility allows the EGW to support various emergency call routing use cases such as Security Desk Call Routing and Emergency Call Conferencing (multi-party emergency call bridging). The scenarios are explained below.

Security Desk Call Routing:

This is a common scenario, in which an emergency call needs to be routed to a single on-site security desk, with or without termination to the appropriate PSAP. The ERL configuration at the EGW indicates the security desk and call routing settings for the call, and the dialed digits (DNIS) can also be used to distinguish between both emergency or non-emergency security desk calls. Additional settings at the Dashboard specify more granular call routing behaviors. For more information see section 5.4.2 “Security Desk Routing and Emergency Call Conferencing Configuration Requirements.”

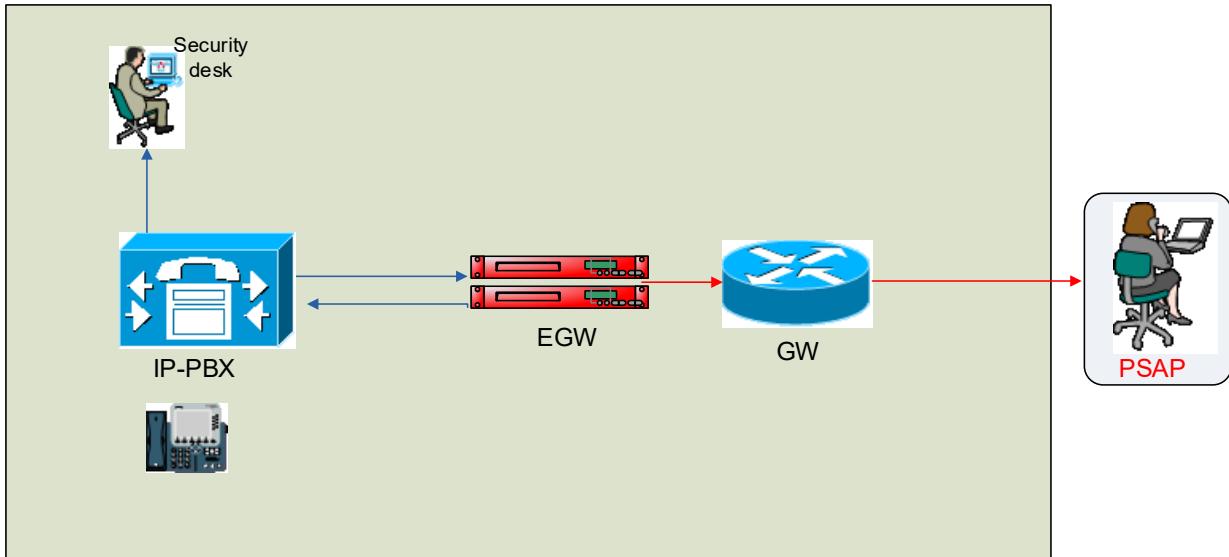


Figure 27: Security Desk Call Routing

In the diagram, an emergency call is routed to the PSAP with an additional security desk call leg. The security desk will be monitoring the call, and the settings at the Dashboard indicate that the conference should only be started when the PSAP answers the call.

Emergency Call Conferencing:

In emergency call conferencing, the emergency call needs to be routed to multiple on-site participants, with or without call termination to the PSAP.

The ERL configuration at the EGW specifies the name of the security desk that will be used to route the call, and specifies the call delivery settings. A security desk group is created using the Dashboard that includes the extensions and settings that apply to the parties that will be conferenced together. For more information see section 5.4.2 “Security Desk Routing and Emergency Call Conferencing Configuration Requirements.”

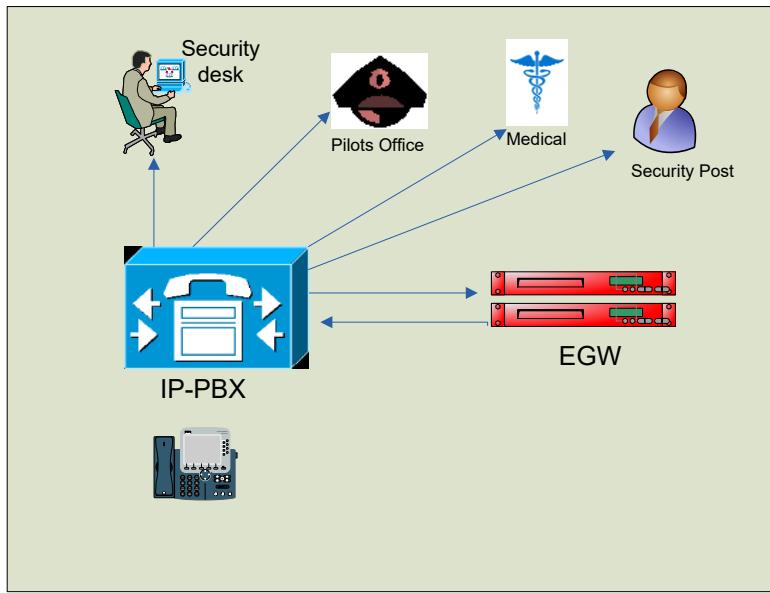


Figure 28: Emergency Call Conferencing

5.4.1.1 Configuration Checklists and Scenarios

The table below describes the supported multi-party call routing scenarios and their configuration requirements.



Note: For ERL Provisioning either the Dashboard or batch file processing can be used.

Table 24: Configuration Checklists and Scenarios

Desired Outcome	Recommended/Required Configuration			
	ERL	Dial Plan	Dashboard	
Security desk call monitor.	Dashboard: <ul style="list-style-type: none"> - Name of the security desk - Call Delivery Type: ERS or local trunking Batch file: <ul style="list-style-type: none"> - Name of the security desk - Direct call delivery setting is set to 0: Call Monitoring. 	- 911 is set to emergency routing	Global	Group
Route a call to a PSAP and a security desk with call monitoring enabled.	Dashboard: <ul style="list-style-type: none"> - Name of the security desk - Call Delivery Type: ERS or local trunking Batch file: <ul style="list-style-type: none"> - Name of the security desk - Direct call delivery setting is set to 0: Call Monitoring. 	- "Wait for PSAP to start conference" set to Yes - End conference when PSAP hangs up set to Yes (recommended setting)	- Configure a Group with one extension - Extension should be set to Required=No	
Direct call delivery.	Dashboard: <ul style="list-style-type: none"> - Name of the security desk - Security desk Mode: Direct Call Delivery Batch file: <ul style="list-style-type: none"> - Name of the security desk - Security desk Mode: Direct Call Delivery 	911 is set to emergency routing	- "Wait for PSAP to start conference" set to No	- Configure a Group with one extension - Extension should be set to Required=Yes.

	<ul style="list-style-type: none"> - Name of the security desk - Direct call delivery setting is set to 1: Direct Call Delivery. 			
Multi-Party Emergency Bridging Route an emergency conference call to multiple actors	<p>Dashboard:</p> <ul style="list-style-type: none"> - Name of the security desk - Security desk Mode: Direct Call Delivery <p>Batch File:</p> <ul style="list-style-type: none"> - Name of the security desk - Direct call delivery setting is set to 1: Direct Call Delivery 	911 is set to emergency routing	<ul style="list-style-type: none"> - "End conference when caller hangs up" set to No - "Wait for PSAP to start conference" set to No 	- Configure a Group with multiple extensions
Route a call to the PSAP and an emergency call conference with multiple actors	<p>Dashboard:</p> <ul style="list-style-type: none"> - Name of the security desk - Call Delivery Type: ERS or local trunking <p>Batch file:</p> <ul style="list-style-type: none"> - Name of the security desk - Direct call delivery setting is set to 0: Call Monitoring. 	911 is set to emergency routing	<ul style="list-style-type: none"> - "Wait for PSAP to start conference" set to Yes 	- Configure a group with multiple extensions

5.4.1.2 Security Desk Call Leg Feature Codes

The following feature codes are available on the security desk call leg during security desk calls and emergency conferences.

To activate a feature using a code, it is necessary to press * followed by the appropriate number:

- 1: Mute/unmute
- 4 and 6 – decrease or increase the conference volume
- 8 – exit
- 7 and 9 to decrease or increase your volume

5.4.2 Security Desk Routing and Emergency Call Conferencing Configuration Requirements

The following is required to configure three way calling or emergency conferencing

- ERL configuration: Configure the name of the security desk for the ERL, as well as the call delivery type setting, and security desk mode.
- Dial plan configuration. For more information, see section 5.4.2.2 “Dial Plan Settings.”
- Configure Dashboard settings. For more information see section 5.4.2.3 “Dashboard Settings.”

5.4.2.1 ERL Configuration

5.4.2.1.1 Batch file

Using batch files the security desk call delivery type is controlled by the direct call delivery parameter. There are three possible direct call delivery settings:

1. Call Monitor (Emergency calls are routed to the PSAP, using three-way call conference with optional one-way mute. This allows the security desk agent to answer the call for monitoring purposes).
2. Direct Delivery (Calls are directed to a specific security desk number. The call is not routed to a PSAP).
3. Security Desk Dial Plan Only (A call to the ERL will route as an emergency call (e.g. 911) unless the dialed number is a security desk dial plan number. In this case, the call routes to an on-site security desk).

A single enterprise location (eg. ERL) can route both emergency and security desk calls. For example, in deployments with a specific security desk number (e.g. 511) it is often the case that calls to the emergency number (e.g. 911) do not route to a security desk. To support this scenario, configure your ERLs in the security desk location with a setting of “Security Desk Dial Plan Only”. When this setting is configured for an ERL, only calls to the security desk number (e.g. 511) will route to the security desk. The call route destination for 911 calls is the appropriate PSAP.

The following table illustrates this configuration.

Table 25: Security Desk Routing Configuration Scenarios

Dialed Number	Security Desk Call Route Setting per ERL	Result
Emergency (911)	Security Desk Dial Plan Only	911 calls only route to the PSAP.
Security Desk (511)	Security Desk Dial Plan Only	User is routed to the security desk using direct delivery.

The diagram below illustrates a common scenario, where calls from the same ERL have a different destination depending on the dialed digits. In this example, security desk calls (511) are programmed to route to an on-site security desk, while emergency calls (911) have been programmed to route to the PSAP.

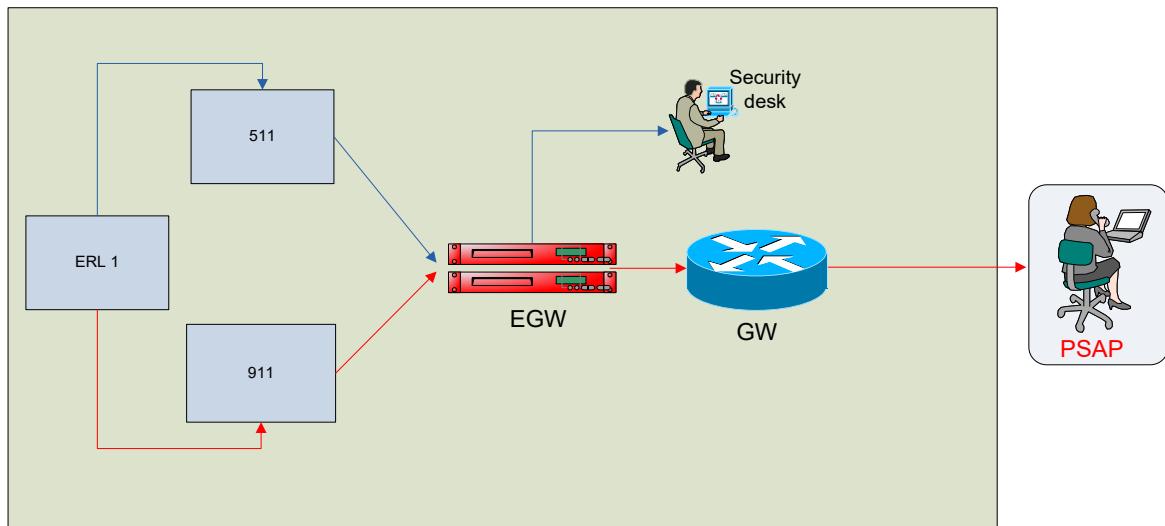


Figure 29: Call Destination for Calls from Same ERL but Different Dialed Digits

The batch location file specifies the security desk name and indicates the direct call delivery setting (Monitor, Direct Delivery, Security Desk Dial Plan Only) that will apply per ERL. The **Security Desk Name** references the settings of the security desk.

For more information, see section 11 “Emergency Response Locations (ERLs).”

5.4.2.1.2 Dashboard Interface

On the Dashboard, an ERL can have 2 different settings for Call Delivery Type: ERS, or Local trunking.

For Security Desk Mode, there are three possible settings:

- Call Monitoring
- Direct Call Delivery
- Security Desk Dial Plan Only

If Direct Call Delivery is specified, the Call will route to the selected security desk.

If Call Delivery Type is set to ERS or local trunking, a security desk is specified, and Call Monitoring is set for Security Desk Mode, the call will route to the PSAP and the security desk using Call Monitoring.

Security Desk Dial Plan Only:

To support this scenario through the Dashboard, you will need to configure an ERL and specify the “Security Desk Dial Plan Only” setting for **Security Desk Mode**. In the dial plan, enter the dialed digits that will ring the security desk, and specify the security desk using the parameter “Default Security Desk.”

5.4.2.2 Dial Plan Settings

Security desk dial plan numbers do not route calls to the local PSAP and are not considered to be emergency numbers.



Note: An emergency number may route a call to an on-site security desk if the ERL is so configured (direct delivery or call monitor).

To add a security desk number to the dial plan

1. Click on **Configuration > Advanced > Dial Plan**
2. Click on **Add a number**
3. Enter a Dial Plan number
4. Select Security Desk as the **Dial Plan**
5. Select a **Default Security Desk** or set the parameter to **None**.

The default security desk is the default route in the case that the call is unprovisioned. The default security desk field can also be set to **None**. This may be the preferred setting for large multi-site deployments with multiple security desks, where it may not be helpful to send unprovisioned calls to the default security desk (e.g. security desks/operators are only equipped to handle calls from a specific location).

In the diagrams below, 511 is used as the security desk dial plan number. These diagrams illustrate the two settings of the **Default Security Desk** parameter.

Default Security Desk is configured on the EGW

- The default security desk can provide call handling for unprovisioned security desk calls from any ERL.
- Any unprovisioned calls to 511 are routed to the default security desk.
- Appropriate for centrally-managed, multi-site security desk deployments

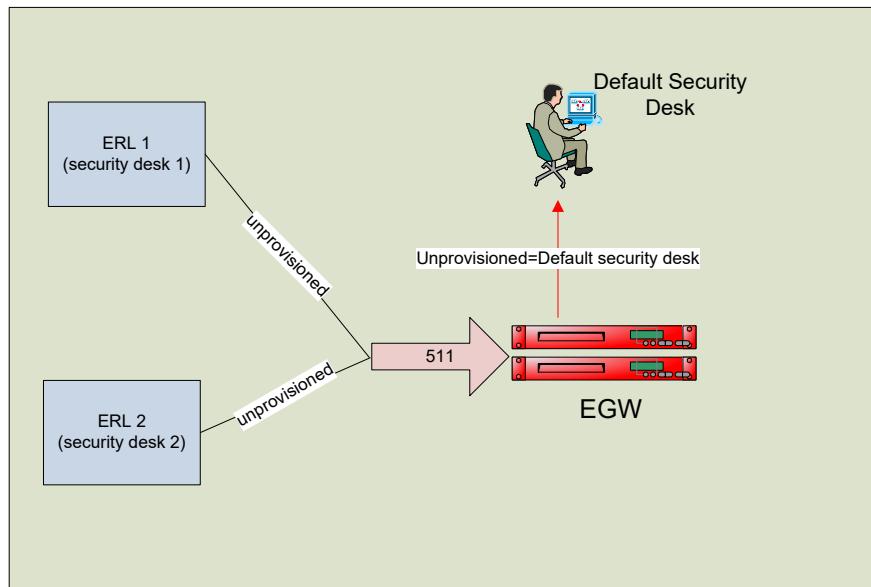


Figure 30: Unprovisioned Call with Default Security Desk

No Default Security Desk

- Each security desk is only capable of handling calls from a single location, or specific group of locations.
- Any unprovisioned calls to 511 are blocked.
- Appropriate for security desk “islands” that are not capable of handling unprovisioned calls.

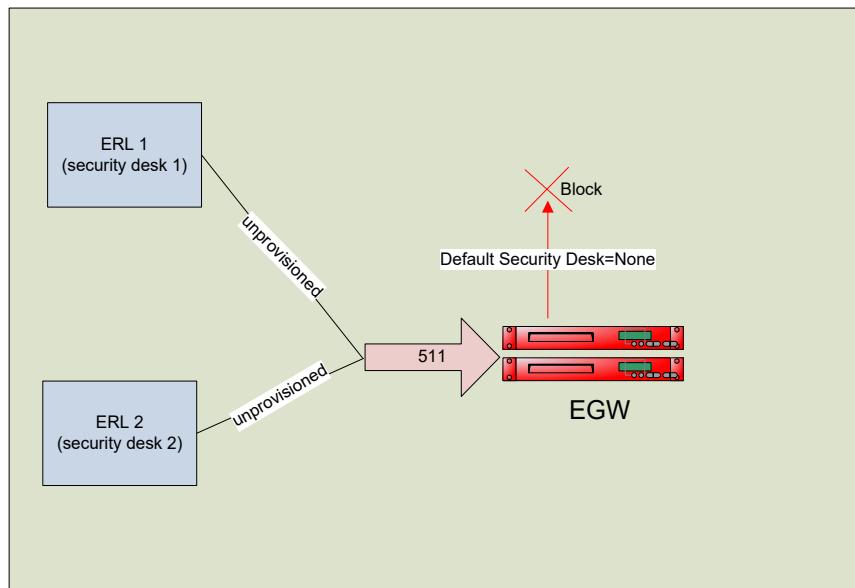


Figure 31: Unprovisioned Call with Default Security Desk Set to None

5.4.2.3 Dashboard Settings

The Dashboard is used to make global settings and configure security desk Groups that determine the settings for security desk call routing and multi-party emergency bridging.

The security desk groups reference the name of the security desk (specified at the ERL), and indicate what IP-PBX system will be used to route the calls. Each security desk group can have one or multiple extensions.

Security Desk Groups:

This feature is used when you have more than one security desks that can respond to emergencies.

To add Security Desk Groups:

1. Click on **Configuration > Security Desk > Groups > Add a Security Desk Group**.
2. Enter the appropriate settings as described in the following table:

Table 26: Configuring Security Desk Groups

Parameter	Description
Security Desk Name	Name of the security desk. Alphanumeric characters and underscores (_) supported. Max 50 characters.
IP-PBX	IP-PBX system that routes the call to the security desk.
Use only for Desk Alert	Check this box to enable the security desk to be used for the Desk Alert feature only. Desk Alert is enabled on a per-ERL basis. If the parameter is enabled, the EGW will reference the security desk name of the ERL for the call, in order to trigger Desk Alert notifications on workstation screens.  Note: The Use Only for Desk Alert checkbox is only viewable if the Desk Alert feature has been enabled.

Display PAI as Caller ID.	<p>When the parameter is enabled, the EGW will send the contents of the Asserted identity (PAI) field as Caller ID to the security desk. The PAI is used by the EGW to convey station callback information to the security desk or PSAP.</p> <p>The following priority order is used by the EGW to populate the PAI header with callback information.</p> <ol style="list-style-type: none"> 1) ELIN 2) Original PAI (if any) 3) Ten digit number (of an extension) 4) Extension Bind 5) Caller Extension
Display misdialed calls on Desk Alert	<p>If you are using the Misdial protection feature you can configure the security desk by checking the parameter box "Display misdialed calls on Desk Alert". This configuration will send desk alert pop-up notifications to the desk alert clients when calls are canceled within the misdial protection recording duration (indicates a potential misdial may have occurred).</p> <p> Note: The Display misdialed calls on Desk Alert checkbox is viewable only if the Desk Alert feature has been enabled.</p>
Wait for the PSAP to start conference	If set to true, the conference is not setup until the PSAP answers.
Enable SIP with PIDF-LO	If set to true, the PIDF-LO will be send to the Security Desk destination clients.

Security Desk Extensions:

Table 27: Configuring Security Desk Extensions

Parameter	Description
Name (Security Desk Extensions)	Name of the security desk extension. Optional field which can be left blank.
Security Desk Number	<p>DID or extension number that rings the security desk.</p> <p>For Lync IP-PBX: Notice that for Lync PBX, if you try to reach an external extension that follows the E.164 format, the + sign is required.</p> <p>i.e. 5146667777 (local extension) +5146667778 (external extension)</p>
Mode Participant	Joins unmuted, can mute and unmute.
Mode Monitor	Joins muted, can unmute and mute.
Mode Monitor only	Joins muted, can't unmute.

The table below shows the different values allowed for the Mode parameter of the security desk extensions and the associated behavior of the extension:

Table 28: Mode Parameters and Values

Mode value	Participant type	Initially Muted	Allowed to mute/unmute	Can answer call	Keep call active
Participant	Active	No	Yes	Yes	Yes
Monitor	Active	Yes	Yes	No	Yes
Monitor Only	Passive	Yes	No	No	No

The participant type indicates how the extension can influence the conference termination.

- Active: The conference is maintained as long as two or more active extensions are present.
- Passive: Passive extensions are ignored in the process that determines whether the conference should be terminated.

The caller and PSAP are always considered active participants. When the conference is initiated for an emergency call, the PSAP has a special status that requires it to answer for the conference to be considered answered. This prevents the conference from being terminated if the security desk hangs up before the PSAP answers.

5.4.3 Limitations of Emergency Call Conferencing

The limitations of the emergency conferencing feature are related to the hardware and software specifications of your hardware or virtual appliance.

For standard hardware EGW

The EGW supports up to 20 concurrent calls. Each participating extension in an emergency conference counts as one concurrent call.

For virtual EGW, the amount of supported concurrent call legs is dependent on the hardware infrastructure of your virtual environment. Consult the v-EGW sizing recommendations in section 2.2.3 “Hardware Requirements for EGW Virtual Appliance.”

6 Configuring Local Trunking (LEC Call Routing)

6.1 Overview

The EGW may be configured to route calls to the LEC emergency network instead of to the ERS. In order to use local trunking, ELIN numbers must be procured from the LEC and provisioned in the EGW and IP-PBX system. ELINS are 10-digit DIDs used to call into the LEC's local emergency network and identify the location of the caller at the PSAP. They are also used by the PSAP to callback into your network, if a 911 call is dropped.

EGW call route policies are configured on a per ERL basis: ERL settings must specify the local trunking setting and the ELINs that will be assigned to the ERL.

To set up local trunking, the following tasks are performed

- Provision ERLs with the local trunking setting and ELIN numbers.
- Configure EGW local trunking settings.
- Configure IP-PBX systems and local gateways to use the ELIN numbers.
- Export location records (in the appropriate format) to the local carrier for upload to the regional ALI database.

6.2 Understanding What Happens When a Local Trunking Call is Made

When the EGW processes a local trunking 911 call, there are two possibilities: the EGW can route the call back to the IP-PBX for termination to the appropriate local gateway, or the EGW can deliver the call directly to the PSTN gateway.

The EGW can be configured to send the call to the IP-PBX or Gateway with prefixes and/or ELINs which are required to complete the call properly. This supports the need to have multiple inbound and outbound route patterns on PBX servers or gateways to support emergency calls and callbacks from the PSAP.

The following scenarios illustrate supported deployments and configurations for local trunking.

In order to correctly configure the route patterns for ELIN numbers:

1. Allocate ELINs and add them to the EGW
2. Configure PBX settings for local trunking (see section 6.4 "Configuring EGW Local Trunking Settings").
3. Configure route patterns on the PBX or PSTN gateway (outbound for emergency calls and inbound for callbacks from the PSAP. Note that these patterns must be unique)

6.2.1 Supported Deployments

6.2.1.1 PSTN Gateways in Multiple Locations

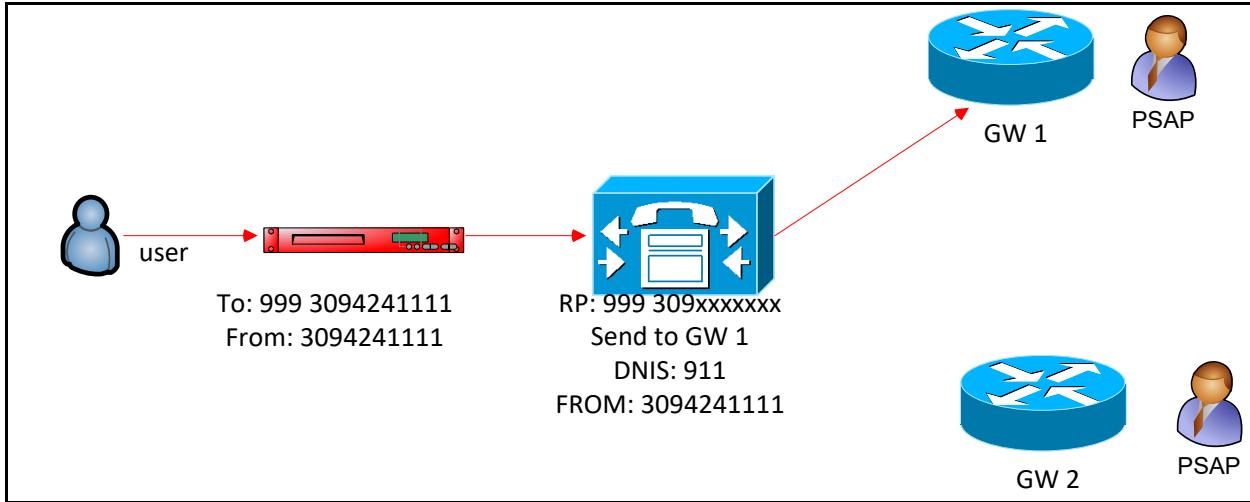


Figure 32: Outgoing Call - Local Trunking

1. User makes emergency call
2. EGW receives call and appends “Local Gateway Prefix” 999. Redirected DNIS (RDNIS) is set to ELIN (see section 7 “Configuring IP-PBX Settings”). FROM field includes the ELIN for the call.
3. Call is sent to the PBX/GW. Route pattern matches Prefix + ELIN. Rules send the call to GW 1 with DNIS as 911 and FROM set to the unmodified ELIN number. The GW completes the call to the PSAP.
4. If the PSAP needs to callback, the corresponding ELIN route pattern (without the prefix) on GW 1 will deliver the call back to the EGW.

6.2.1.2 Support for Multiple Emergency numbers in Local Trunking

In countries like Switzerland, there are multiple emergency numbers; 112 for the Global EMEA number, 117 for Police, 118 for Fire Department, etc. Special support is required for these types of deployments.

In such a case, the emergency number is saved in the forwarded SIP invite so that the PBX is able to choose the accurate destination for the emergency call.

6.2.1.3 Single Gateway or SBC

In this scenario there is no need to differentiate between multiple outbound gateways.

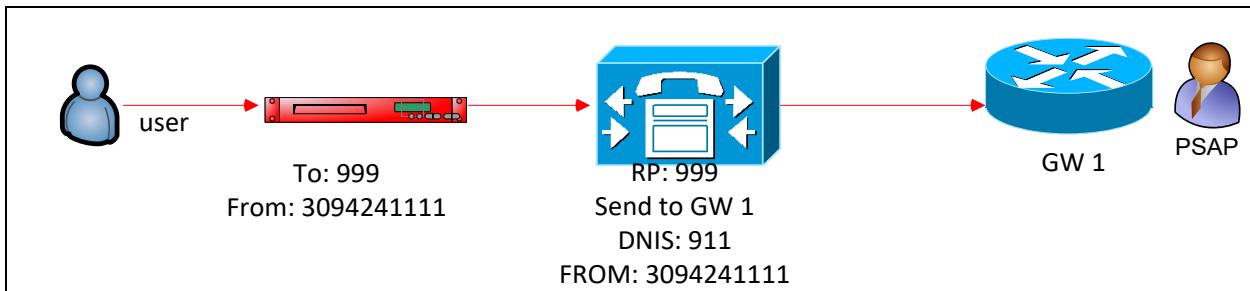


Figure 33: Local Trunking Outgoing Call Prefix-Only

1. User makes emergency call
2. EGW receives call and appends “Local Gateway Prefix” 999. Redirected DNIS (RDNIS) is set to None (see section 7 “Configuring IP-PBX Settings.”). FROM field includes the ELIN of the caller

3. Call is sent to the PBX/GW. Route pattern matches Prefix. Rules send the call to GW 1 with DNIS as 911 and FROM set to the unmodified ELIN number. The GW completes the call to the PSAP.
4. If the PSAP needs to callback, the corresponding ELIN route pattern on GW 1 will deliver the call back to the EGW.

6.3 Provisioning ERLs for Local Trunking

The Local Trunking setting is applicable on a per-ERL basis. The setting is made during the batch provisioning of ERL records. See section 11 “Emergency Response Locations (ERLs).”

6.4 Configuring EGW Local Trunking Settings

Local trunking settings are configured during IP-PBX configuration, to allow the EGW to send the appropriate ELIN route patterns to the IP-PBX/PSTN GW when 911 is dialed. In deployments that use ELINs, a prefix/suffix can be used to differentiate the outgoing ELIN route pattern from the inbound ELIN

For more information, see section 6.2 “Understanding What Happens When a Local Trunking Call is Made.”

To configure the EGW

1. Click on **Configuration > IP-PBX**
2. Click on the name of your IP-PBX in the **IP-PBX List**
3. Configure **Local Gateway Prefix** and **Local Gateway Suffix**
4. Choose **None, ELIN or DNIS+ELIN** for the **Redirected DNIS (RDNIS)**.

Local Gateway Prefix/Suffix: A prefix/suffix combination can be appended to the ELIN, in order to differentiate the outgoing ELIN route pattern (EGW to IP-PBX) from the inbound ELIN (PSAP callback to IP-PBX). It is also possible to send an emergency call from the EGW with only the Local Gateway Prefix. The corresponding route pattern must be programmed into the PBX/local gateway for termination to the LEC emergency network.

Note: To send only the prefix to the PBX/GW, add the “Local Gateway Prefix” and do not enable the “Redirected DNIS (RDNIS)” parameter.

Use ELIN as Redirected DNIS (RDNIS): If you choose, ELIN as Redirected DNIS (RDNIS), the ELIN is sent to the IP-PBX/GW as the DNIS for outgoing 911 calls.

Use DNIS+ELIN as Redirected DNIS (RDNIS): If you choose DNIS+ELIN as Redirected DNIS (RDNIS), the DNIS alongwith the ELIN is sent to the IP-PBX/GW as the DNIS for outgoing 911 calls.

PSTN Gateway: Specify the PSTN gateway that will be used to route local trunking calls, if applicable.

For more information see section 7 “Configuring IP-PBX Settings” that applies to the vendor of your IP-PBX equipment.

6.5 Working with NENA 2 Files

To enable local trunking, your location records (ERLs) must be uploaded to the LEC’s regional ALI database in the correct format. The NENA 2 format is a standard file format for emergency database data transfer. The EGW contains a NENA 2 file generation feature which automatically generates NENA 2 files for export to the local LEC.

The feature works as a scheduled task, and can be configured to run multiple times per day. This feature helps to simplify administration.



Note: The EGW supports both NENA 2 and 2.1 files.

To understand how NENA 2 file generation works, and to learn how to configure the feature, see section 16 “NENA 2 Provisioning.”

6.6 ELIN Management

ELINs must be programmed into the EGW’s configuration. You can do this manually, as part of ERL batch processing, by adding individual ELINs to ERLs. For more information, see section 11.2 “Provisioning ERLs.”

It is also possible dynamically manage ELINs on the EGW. In this case, the ELINs are simply added to the EGW’s ELIN pool. The EGW automatically adds or releases ELIN numbers when ERLs are added or removed from the system.



Note: Dynamic management is applicable to enterprises with a Private ALI database or a PS-ALI that serves a single PSAP jurisdiction. In the case of PS-ALI, the ELINs must be from the same NPA-NXX for termination to a single LEC emergency network. Dynamic ELIN management is also only available to customers in US/Canada.

6.6.1 Uploading ELINs to the EGW’s ELIN Pool

Before the EGW can dynamically assign ELINs to ERLs, the ELINs must be added to the EGW’s ELIN pool.

To upload ELINs to the ELIN pool on the EGW:

- Click on **Provisioning > ELIN Pool**
- Click on **Add ELIN**
- Enter the ELINs to add to the ELIN pool

Wildcard Masks

ELINs can be added to the EGW configuration using wildcard masks to simplify administration.

DID ranges are typically purchased from the LEC for use as ELINs. DID ranges are assigned using standard North American Numbering Plan form (NPA NXX Station). For example, you might receive the following range of numbers:

514-745-2141	514-745-2146
514-745-2142	514-745-2147
514-745-2143	514-745-2148
514-745-2144	514-745-2149
514-745-2145	514-745-2140

You may provision this DID range in the EGW by using a single entry: 514-745-214x

Mass deletions may also be performed from the Dashboard interface using wildcards.

You may easily track which ELINs are available and which ELINs are assigned. Using the **Search** screen, you may search for a specific ELIN, or ELIN mask, and view the assigned ERLs. The **Search** screen may also be used to delete ELINs from the system.

To access the Search screen:

1. Click on **Provisioning > ELIN Pool**
2. Type your query into the **ELIN Pool Search** box
3. View the **ELIN Pool Search Results**
4. Click on **View All** to see all of the individual ELINs contained within a specific mask.

6.6.2 Understanding Multiple ERLs per ELIN

It is possible to assign the same ELIN number to more than one ERL using the EGW. In this case, because a single ELIN is associated to multiple location records in the EGW, it cannot be used as a reference to location. Therefore, if this configuration is implemented, it is not possible to use the dynamic ELIN management or NENA 2 file generation features. Each individual ERL is associated to the ELIN of choice during the batch processing stage.

The table below compares various ELIN management capabilities of the EGW and illustrates if they support the following: Private ALI, PS-ALI, and Multiple ERLs per ELIN.

Table 29: ELIN Management Scenarios

ELIN management	Private ALI	PS-ALI	Multiple ERLs per ELIN
Static ELIN	Yes	Yes	Yes
Dynamic ELIN	Yes	Yes. Only supports a single PSAP jurisdiction (NPA-NXX)	No
NENA 2 file generation	Yes	Yes	No

Enterprises will typically assign multiple ERLs to the same ELIN under the following scenarios:

1. An enterprise would like to enable centralized callbacks to a single location.
2. An enterprise with an on-site security desk prefers to send the billing number associated with the trunk to the LEC emergency network.

Centralized Callbacks

In the centralized callbacks scenario, the enterprise would like all 911 callbacks from the PSAP to route to a single centralized location (e.g. on-site security desk). For this scenario to work correctly, it is necessary to configure the IP-PBX with route patterns that deliver 911 callbacks to the central answering point.

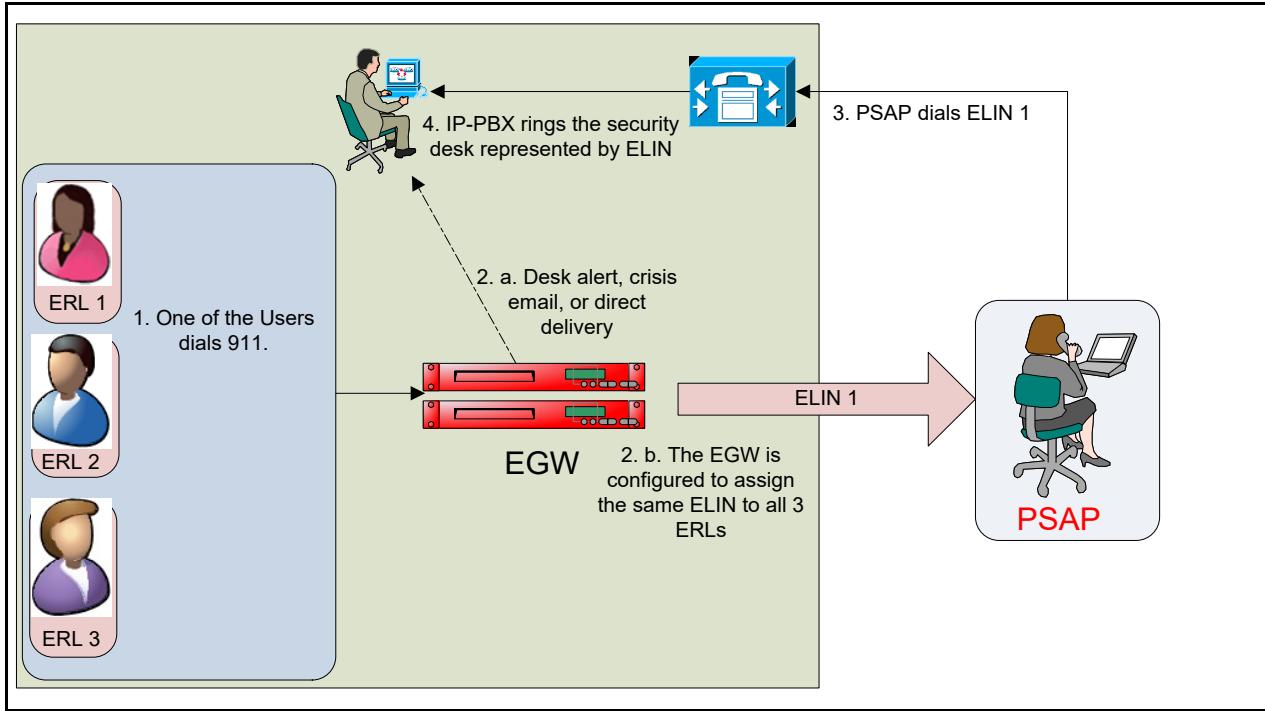


Figure 34: Centralized Callbacks

On-site Security Desk with Trunk Billing Number sent to PSAP

In this scenario, the enterprise is not concerned with sending a granular location to the PSAP.

- No PS-ALI is in place to provide granularity to the PSAP.
- The EGW is used to send the same ELIN (billing number associated to the trunk) for each 911 call.
- When 911 is dialed, the EGW can send a security desk call, Desk Alert screen pop, and crisis email.
- The security desk can receive either the ELIN or caller's extension in the Call Display.

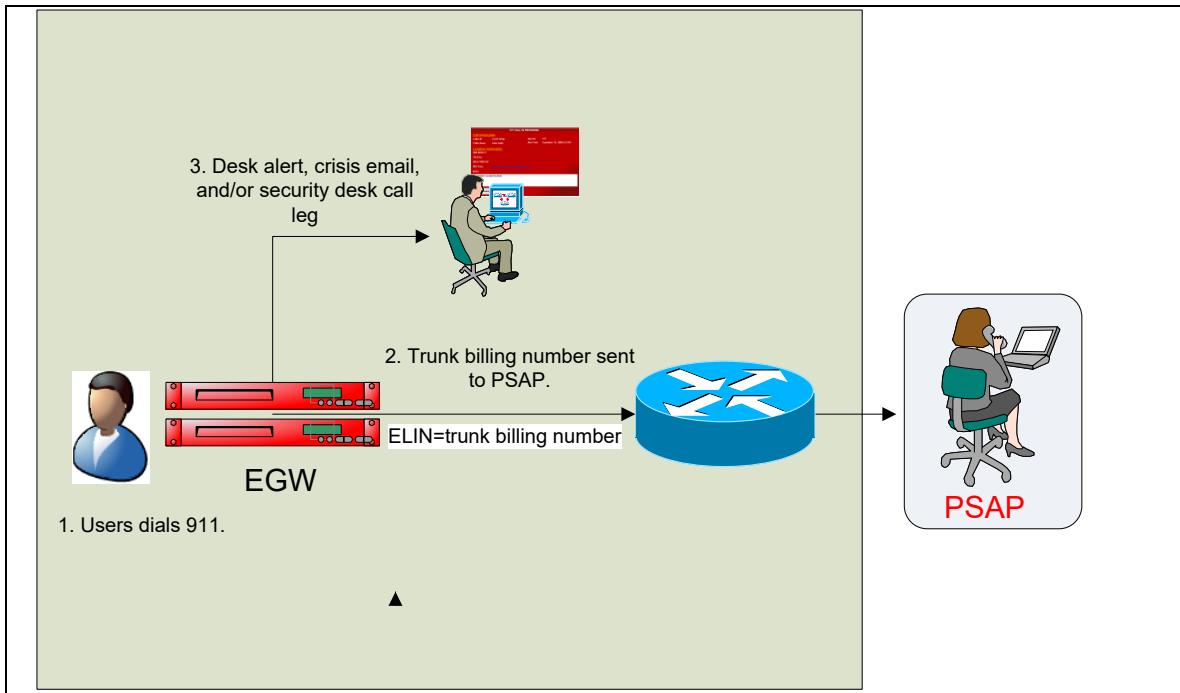


Figure 6-35 Trunk Billing Number Sent to PSAP for all Calls

6.6.3 Configuring Multiple ERLs per ELIN

You can configure multiple ERLs per ELIN using batch or SOAP provisioning. The ELINs are associated to the ERL records following the ERL batch file format or locations SOAP interface specifications.

There are certain restrictions that apply to this configuration. If you attempt to assign ERLs to an ELIN that is in either the dynamic or Extension-Bind pool, an error will be generated.



Note: The assignment of multiple ERLs to the same ELIN depends on the global setting of the NENA 2 feature. If NENA 2 is enabled, you will not be able to assign the same ELIN to more than one ERL. Likewise, if you have assigned a single ELIN to more than one ERL, the global configuration for NENA 2 will be unavailable from the Global configuration screen.

7 Configuring IP-PBX Settings

The IP-PBX configuration establishes the networking protocols and various custom settings that will be used for communication between the EGW and your telephony servers.

The configured settings vary by PBX Vendor (Cisco, Avaya, Microsoft, etc.). Generic PBX settings can be configured to establish basic connectivity between the EGW and any SIP/H.323 compatible phone system.

Note: The DNIS prefix allows multiple IP-PBX servers sharing the same IP address to be identified uniquely. If your deployment consists of multiple IP-PBX servers that connect to a session border controller (SBC), you can configure each server with a unique DNIS prefix.

Note: Local trunking settings are used to route 911 calls to the local exchange carrier. These settings enable the EGW to route the 911 call to the appropriate local gateway for termination to the correct regional PSAP.

To configure the EGW and your network for call routing to the local exchange carrier, see section 6 “Configuring Local Trunking (LEC Call Routing).”

7.1 Configuring Cisco UCM Settings

7.1.1 Understanding How the EGW works with Cisco Unified Communications Manager (CUCM) Deployments

7.1.1.1 Call Routing Overview

When 911 is dialed, the EGW uses a CTI route point to obtain a phone’s MAC, IP address, and extension. These parameters are used to make routing decisions.

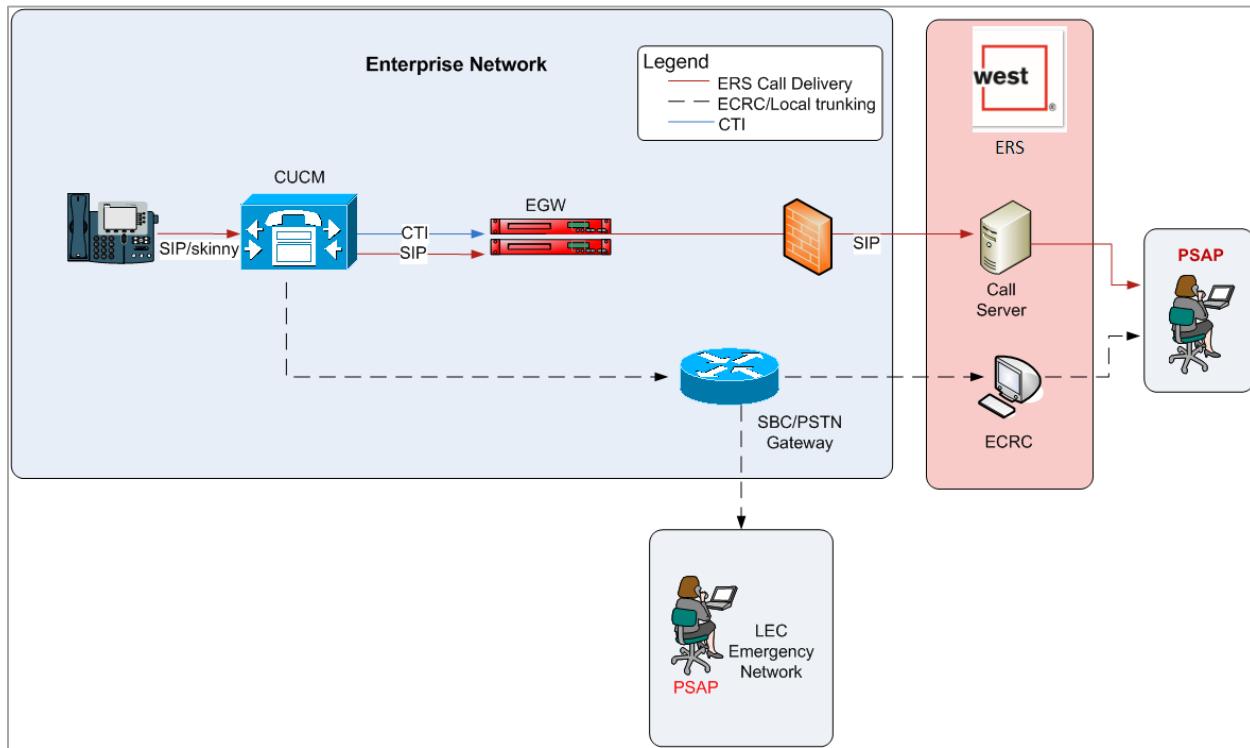


Figure 36: Cisco Call Routing

1. Cisco IP phone initiates a 911 call.
2. CUCM dial plan forwards the call and provisioning data (MAC, IP, extension) to the EGW using a CTI Route Point.
3. EGW retrieves the appropriate ERL and routing information for the call, before sending the call back to the CUCM with a new Redirect DNIS (RDNIS).
4. The CUCM dial plan contains a route pattern for the RDNIS that sets up a SIP call between the CUCM and the EGW. The endpoint's extension or 10-digit number is sent to the EGW in the SIP call.* If the extension is sent, the EGW Extension-Bind feature provides the callback number for the call.
5. The EGW delivers the call to the ERS over a SIP trunk or to the LEC's emergency network using gateways and dedicated 911 trunks. **

*If an external phone mask is in use, the EGW is configured with the appropriate extension numbering length.

** If local trunking is in use, calling prefixes and/or suffixes may need to be configured on the EGW.

Call Routing for Deployments Using Extension Mobility Cross Cluster (EMCC):

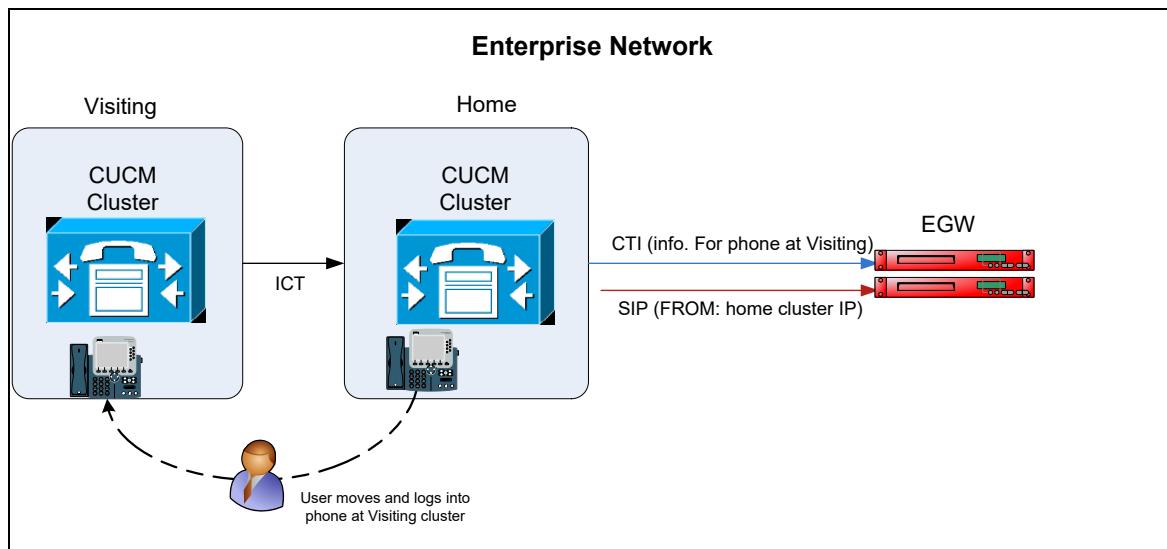


Figure 37: Call Routing for EMCC Deployments

When a user logs in to a visiting cluster, the phone registers with the EGW with its endpoint info. (MAC, extension, IP) associated to the Visiting cluster. When 911 is dialed, the CTI sent from the home cluster to the EGW includes the endpoint info for the endpoint at the Visiting cluster and the IP address of the IP-PBX system at the Home cluster. The IP-PBXs that participate in EMCC are grouped at the EGW, to enable the EGW to match the endpoint parameters received during a 911 call with the endpoint registration information in the database.

For more information, see section 7.1.3.2 “Configuring Extension Mobility Cross Cluster.”

7.1.2 Device Inventory

The device inventory can be discovered using Cisco proprietary AXL, or using other discovery methods. For more information see section 12 “Endpoints.”

The EGW is populated with the inventory for the devices that need to be discovered for emergency services (IP phones, SIP phones, digital/analog phones). It is preferable that other devices be excluded.

7.1.2.1 AXL Filtering

It may be the case that not all endpoints discovered by AXL should be enabled for emergency services. In this case you can filter these endpoints out of the EGW inventory using **AXL Filtering**.

AXL filtering is enabled by configuring the **AXL Device Name Filter**. For more information see section 7.1.3 “Configuring the EGW for the CUCM.”

7.1.2.2 Understanding the Endpoints Count on System Status

The endpoints are calculated as follows:

Endpoints Count:

- The endpoint has a PBX-ID
- The endpoint has an extension or device name.

Provisioned Endpoints Count:

- The endpoint has a PBX-ID
- The endpoint has an extension or device name.
- The endpoint has a location ID.
- The endpoint does not have a location ID but the IP address of the endpoint matches one of the configured subnets. The endpoint will get the location of the subnet.

Billable Endpoints:

- The endpoint has a PBX-ID.
- The endpoint has a location ID and the location is not set to local trunking or direct call delivery.
- The endpoint does not have a location ID but the IP address of the endpoint matches one of the configured subnets. The endpoint will get the location of the subnet and the location must not be set to local trunking or direct call delivery.

Other:

Devices discovered using batch or SOAP that are assigned to an ERL.

For more information see section 12 “Endpoints.”

For more information see section 18 “System Status.”

The **Last 12 months Endpoints Peak reported** count at **System Status** will display the peak number of billable endpoints detected for the given month.

7.1.2.3 Automatic Phone Inventory

The feature is enabled by specifying a MAC address mask (configured using regular expressions) on a per IP-PBX basis. For the group of endpoints discovered within the group during a Layer 2 scan, the EGW adds the endpoints to the inventory, and assigns them to the connected switch/switch port and ERL.

Note: *In the case where both methods are used simultaneously, the vendor proprietary method will take precedence and will overwrite data for the subset of MAC addresses included for both inventory discovery methods.*

The regular expression will specify the MAC address Organizational Unique Identifier (OUI) as the first 3 bytes (octets). The second group of three octets will be used to specify the range that should be included for automatic phone inventory.

Example for Cisco:

- 00036B - Assigned to Cisco IP Phones.

00036B[0-9a-fA-F]{6}

Where 00036B are the three octets of the OUI. The [0-9a-fA-F]{6} means to match any three octets for the non-OUI part of the MAC address.

7.1.3 Configuring the EGW for the CUCM

A CUCM IP-PBX system at the EGW refers to a Cisco cluster, a collection of servers that implement the CUCM's call processing capabilities. The primary node, or Publisher server, contains the CUCM database which is replicated to the subscriber nodes. The Cisco IP-PBX settings specify the settings that apply globally to the cluster. Each individual signaling server configured at the EGW is specified as a Publisher or subscriber server. There is only one Publisher per cluster.

CTI Preferences

Some of the servers in the CUCM cluster run the CTI Manager service, which enables them to establish communication with CTI-enabled applications such as the EGW. CTI routepoints are established between the primary and secondary EGWs and the subscribers running CTI Manager. The secondary route point is required for redundancy. For optimal redundancy, the subscribers associated with the primary EGW routepoint should be different from the subscribers registered with the secondary routepoint.

The route points can be restarted on a per IP-PBX (Cisco cluster) basis. When the CTI service is restarted for the primary route point of a cluster on the EGW, the backup route point maintains CTI service to the EGW.

For more information, see section 18 "System Status."

RLM Preferences

The Remote Location Manager is a phone service on the EGW that is available to Cisco IP phones equipped with an XML browser. By configuring the URL of the EGW via CUCM Administration, the RLM provisioning page will be displayed on Cisco IP phones when the **Services** button is pressed.

The RLM Notifier uses CTI to listen for IP phone registration events on the network. When an IP phone registration event is detected, the RLM Notifier instructs the IP phone to request the RLM phone service from the EGW. The RLM provisioning page is then displayed on the phone's XML browser, prompting the user to verify that the location is up-to-date.*

*Max phones monitored is 10,000.

For more information, see the document "Configuring the CUCM for the EGW Appliance" and see section 17 "Provisioning Off-Campus Users."

AXL Preferences

The EGW communicates with the CUCM using AXL to obtain the inventory of IP phones. The Administration XML is used to access configuration data on the CUCM database to build the inventory of IP endpoints. The AXL IP address at the EGW must specify the IP of the publisher server, which has the authoritative database.

SNMP Preferences

The EGW polls the CUCM servers to monitor the devices enabled for 911 service. Each server supporting device pools enabled for 911 call routing should have SNMP services enabled.

Advanced Settings

If your phone system employs external phone number masks, this must be reflected in the configuration between the EGW and the CUCM.

A mask can be accounted for by either using the EGW's "Use External Phone Number mask" setting or by configuring the Calling Party External Phone mask setting on the CUCM.

For more information about CUCM configuration, see the document “Configuring the CUCM for the EGW Appliance.”

If you will use the EGW instead, you must indicate the length of your extension numbering plan on the EGW by configuring the Extension Number Length setting. The EGW uses this configuration to match the provisioned extension of the phone with the digits that present to the EGW when an emergency number is dialed. If your deployment includes dynamic phone masks, you must indicate the highest extension number length in the deployment. For example, if your deployment includes both 6 and 4 digit extensions, you must configure a value of 6 for **Extension Number Length**.

IP PBX Preferences

Endpoint Determination directs the EGW on which parameter to acquire the endpoint information. The default settings are as follows:

- extension
- mac
- ip
- devicename

The above settings mean that the extension of the device is first used to acquire the endpoint information.

Location Determination directs EGW on which parameter to acquire the location information. The default settings are as follows:

- static
- l2_wlan
- l3

Even though the default is as above, if the user sets a remote location, this takes precedence over the above preferences.

The “Found By” column in the **Endpoints** page is populated by the entity that was used to determine the location.

Static PBX Preferences

The settings here define the default behavior when you assign a location to the endpoint in a static setting. Use this setting to prioritize the static assignment. The default settings are as follows:

- mac
- extension
- devicename

The other advanced settings are applicable to the supported configurations for local trunking. For more information see section 6 “Configuring Local Trunking (LEC Call Routing).”

To configure a Cisco IP-PBX:

1. Click on **Configuration > IP-PBX > Add a New IP-PBX**
2. Enter the appropriate settings as described in the table below

Table 30: CUCM IP-PBX Configuration

Parameter	Description
IP-PBX ID	Unique numerical identifier of the IP-PBX
IP-PBX Name *	Name of the IP-PBX. Must not contain any spaces.
IP-PBX Type	Cisco.
IP-PBX Version	Version number of the IP-PBX.

Parameter	Description
Protocol	Protocol that will be used to communicate between the IP-PBX system and the EGW (SIP UDP or SIP TCP).

* Note: The IP-PBX Name should not contain any spaces and cannot be empty. It can be a string of alphanumeric characters up to 70 characters in length. Special characters such as (underscore) and – (hyphen) are also accepted.

CTI Preferences:

Table 31: CTI Preferences

Parameter	Description
CTI Username	CTI credentials for primary CTI routepoint.
CTI Password	CTI credentials for primary CTI routepoint.
CTI Routepoint name	Default value is “911RoutePoint1” Must match naming from IP-PBX configuration. For more information, see the document “Configuring the CUCM for the EGW Appliance.”
Secondary CTI Username	CTI credentials for secondary CTI routepoint. Enter the user name.
Secondary CTI Password	CTI credentials for secondary CTI routepoint.
Secondary CTI Routepoint name	Default value is “911RoutePoint2” Must match naming from IP-PBX configuration. For more information, see the document “Configuring the CUCM for the EGW Appliance.”
CTI Redirect DNIS (RDNIS)	Default RDNIS (Redirected DNIS) is *913. The matching route pattern must be configured during IP-PBX configuration. See the document “Configuring the CUCM for the EGW Appliance” for more information.
CTI Append MAC	Setting which enables the EGW to append the MAC address of the device to the Dialed Number (DNIS). The MAC address can be used to identify the location of the caller.
Primary Routepoint	List of subscribers running CTI Manager assigned to the primary CTI routepoint on the primary EGW. List also determines priority ordering.
Secondary Routepoint	List of subscribers running CTI Manager assigned to the secondary CTI routepoint on the secondary EGW. List also determines priority ordering.

RLM Preferences:

Table 32: RLM Preferences

Parameter	Description
RLM Notifier IP Address	IP address of the Cisco CTI server used for RLM Notifier.
RLM Notifier Username	Username of the Cisco CTI server used for RLM Notifier.
RLM Notifier Password	Password of the Cisco CTI server used for the RLM Notifier service.

AXL Preferences:

Table 33: AXL Preferences

Parameter	Description

AXL IP Address	IP address of the AXL server. Only one server can be configured with an AXL IP address per IP-PBX.
AXL Username	Username to establish connection with AXL server. Note: CUCM 4.x requires the AXL username and password of the CUCM administrator.
AXL Password	Password used to establish connection with AXL server. Note: CUCM 4.x requires the AXL username and password of the CUCM administrator.
AXL Device Name Filter	<p>Filter(s) which will exclude devices discovered using AXL from being added to the devices inventory.</p> <p>Eg.</p> <p>SEP%</p> <p>Any device starting with SEP</p> <p>JOHN_SMITH??</p> <p>JOHN_SMITH device with 2 extra char. E.g. JOHN_SMITH01, JOHN_SMITH_A</p> <p>Up to 32 filters can be configured.</p> <p>Note: When AXL Filtering is enabled, it will also filter out any endpoints already added using AXL that match the filter settings.</p>

Advanced Settings:

Table 34: Advanced Settings

Endpoint ID Field	Setting that determines which SIP field will be used to deliver the extension number or DID to the EGW. Please use default values or consult with Intrado technical personnel prior to making changes.
DNIS Prefix	This setting is used for topologies that proxy calls through a session border controller. The DNIS prefix allows multiple IP-PBX servers to share the same signaling IP address.
Local Gateway Prefix	Prefix which is used to deliver a unique ELIN to the IP-PBX for an outgoing 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.
Local Gateway Suffix	Suffix which may be used in conjunction with Prefix, in order to deliver a unique ELIN to the IP-PBX for an outbound 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.

Redirected DNIS (RDNIS)	<p>Setting which enables an ELIN or an ELIN + DNIS to be used as the RDNIS. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX.</p> <p>The available values for updating the IP-PBX:</p> <ul style="list-style-type: none"> • None (selected by default) : Not a local trunk • ELIN: Local trunking use case with one Emergency number. One possible Emergency termination. • DNIS+ELIN: Local trunking use case with multiple Emergency numbers. Multiple possible Emergency terminations depending of the DNIS.
Callback Use VIA Header	If this field is set to Yes, the EGW will look at the VIA Header in the SIP Invite message, in order to obtain the IP address of the signaling server for the call. This may be the preferred setting in deployments where the IP included in the endpoint's SIP URI does not accurately represent the signaling server for the call.
Callback Use Original PAI	Setting which enable the EGW to use the PAI to obtain the station's callback number. The P-Asserted Identity is a field in the SIP INVITE sent to the EGW that can contain a 10 digit callback number. If this setting is Yes, the EGW will use the PAI as the callback number, unless an Extension-Bind or ELIN number is applicable for the call. If the parameter is Yes and the PAI field is empty, the EGW will use the original SIP URI From or Contact to obtain the callback number.
Use External Phone Number Mask	Setting that is enabled if your deployment includes external phone number masks.
Extension Number Length	The length of the extensions in your dial plan. If your deployment includes dynamic extension numbering lengths enter the highest value. For example if you deployment includes both 6 and 4 digit extensions, you must configure a value of 6.
IP-PBX Preferences	<p>Settings that direct the EGW on the parameters to use to acquire the endpoint and location information.</p> <p>Uncheck "Use Default Settings" to view and/or change the IP-PBX preferences. The order can be changed by picking the parameter and moving it to your preferred location.</p> <p>Endpoint Determination Order that determines how the EGW will retrieve the endpoint information at call time. Default is as follows: -extension -mac -ip -devicename</p> <p>Location Determination Preferences that determine the order in which EGW will retrieve the location from the endpoint information at call time. Default is as follows: -static -l2_wlan -l3</p>

Static PBX Preferences	<p>Uncheck “Use Default Settings” to view and/or change preferences. Default is as follows:</p> <ul style="list-style-type: none"> -mac -extension -dn <p>The order can be changed by picking the parameter and moving it to its preferred place.</p>
SIP Extension-IP Match Preferences	<p>Preferences that determine the order in which the EGW will extract the Extension and the IP of the caller. Each entry corresponds to a predefined REGEX. As soon as a REGEX matches the SIP URI, we record the Extension and the IP assuming the generic format:</p> <p><code>sip:[User];ext=[Extension]@[Host]</code></p> <p>Default is as follows:</p> <ul style="list-style-type: none"> - Extension: User [Ext] ; IP: Host - Extension: User ; IP: Host - Extension: Host[:*] - Extension: Host <p>Explanations of the available REGEX can be found below.</p>

REGEX Definitions:

Table 35: Regex Definitions

REGEX	SIP URI match description
Extension: User [Ext] ; IP: Host	Format detected : <code>sip:[User];ext=[Extension]@[Host]</code> Extension = [User] IP = [Host]
Extension: [User] Ext ; IP: Host	Format detected : <code>sip:[User];ext=[Extension]@[Host]</code> Extension = [Extension] IP = [Host]
Extension: User ; IP: Host	Format detected : <code>sip:[User]@[Host]</code> Extension = [User] IP = [Host]
Extension: Host[:*]	Format detected : <code>sip:[Host]:</code> Extension = [Host]
Extension: Host	Format detected : <code>sip:[Host]</code> Extension = [Host]
IP: Host[:*]	Format detected : <code>sip:[Host]:</code> IP = [Host]
IP: Host	Format detected : <code>sip:[Host]</code> IP = [Host]

7.1.3.1 CUCM server settings

To configure a Cisco server:

1. Click on **Configuration** → **IP-PBX** → **Add a Server**

2. Configure the server information explained in the following table:

Table 36: CUCM Server Configuration

Parameter	Description
IP-PBX ID	Select the IP-PBX system to which you want to associate the server.
IP-PBX name	Name of the IP-PBX to which this server is assigned. For more information on the acceptable characters for this field, click here.
Server Name**	Name of the server. Click here for limitations on the naming strategy.
Server Type	Publisher or subscriber. The publisher is the primary node and stores the authoritative database for CUCM. The subscribers store a replicated database.
Signaling Option	Setting which enables the server to act as a signaling server. In some circumstances CUCM publisher servers may also handle call processing/signaling.
Signaling IP Address/FQDN	IP address or FQDN of the signaling server.
Callback Port	Default is 5060. Must match SIP trunk Destination Port entered during IP-PBX configuration. Value of 0 will bypass use of callback port. For more information, see the document "Configuring the CUCM for the EGW Appliance."
Connection timeout	Amount of time in seconds that will elapse before the EGW issues a connection timeout alarm.
Monitoring Enabled	Setting which enables SIP Options monitoring for the SIP signaling server. When monitoring is enabled, the EGW will maintain the peer status as up or down for the server, and send SIP options alarms and notifications accordingly. The monitoring enables the EGW to send proactive service unavailable SIP 503 response messages when a SIP user agent requests a service from a server that is known to be in a down state. For more information, see section 3.5 "SIP and the EGW."

***Note: The Server Name should not contain any spaces and cannot be empty. It can be a string of alphanumeric characters up to 50 characters in length. Special characters such as _ (underscore) and – (hyphen) are also accepted.*

7.1.3.2 Configuring Extension Mobility Cross Cluster

To configure the EGW to support EMCC, you need to add all of the IP-PBX systems that participate in EMCC to an IP-PBX Group. The IP-PBX Group allows the EGW to:

- Uniquely identify endpoints that present phone information from a visiting cluster while the IP for the call originates from the home cluster IP-PBX
- Eliminate duplicate endpoint entries in the subscriber DB if phones physically move between clusters

To configure the IP-PBX Group:

1. Click on **Configuration>IP-PBX>IP-PBX Groups**
2. Click **Add a Group**
3. Select the IP-PBX systems that participate in EMCC from the Available Group Members list
4. Click **Save**

Once IP-PBX systems are grouped together, the EGW will ensure that all endpoints are unique across the grouped IP-PBX systems.

Note: Please consult Cisco documentation to determine requirements for supporting EMCC. An Intercluster SIP Trunk (ICT) is required between your Cisco clusters to enable the Visiting cluster to route E911 calls to the Home Cluster.

7.2 Configuring Avaya Communications Manager (CM) Settings

7.2.1 Understanding How the EGW works with Avaya CM Deployments

7.2.1.1 Call Routing Overview

When 911 is dialed, the call is routed from the Avaya CM to the EGW using H.323. If SIP is used, an Avaya SES server is required.

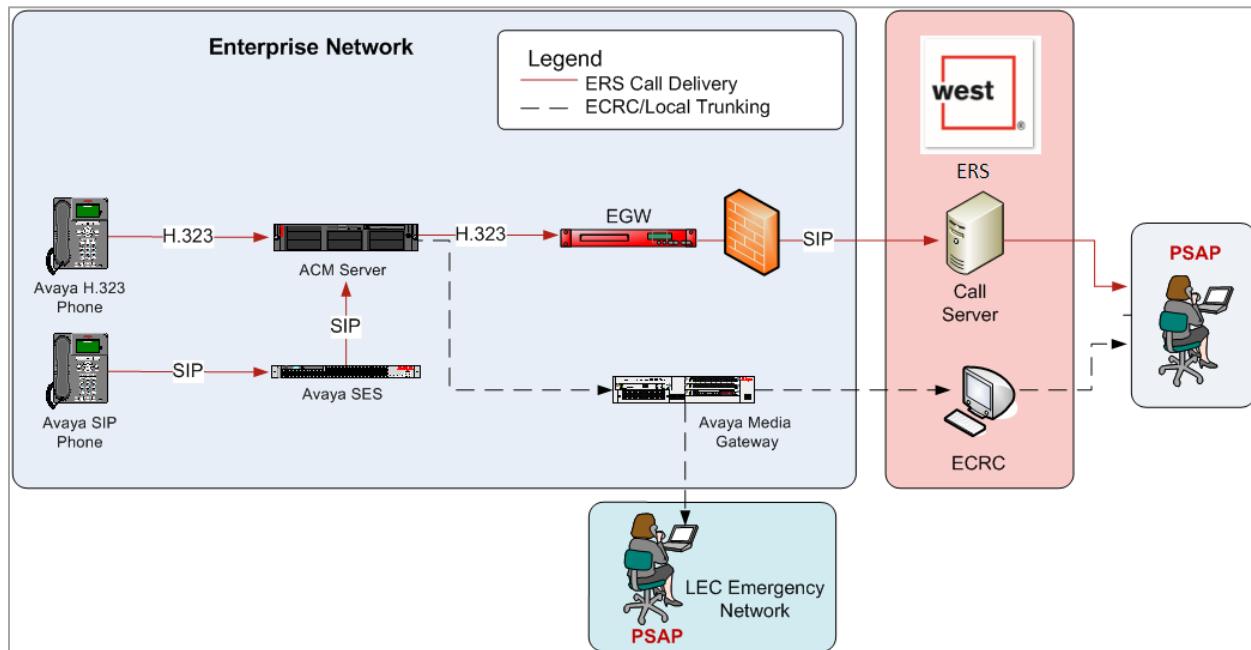


Figure 38: Avaya Call Routing

1. Avaya H.323/SIP phone dials 911.
2. Avaya CM dial plan forwards the call and extension/10-digit number to the EGW.* If the extension is sent, the EGW Extension-Bind feature provides the callback number for the call.
3. EGW retrieves the appropriate ERL and routing information for the call.
4. The EGW delivers the call to the ERS or to the LEC's emergency network.**

* If the Avaya dial plan appends digits to outgoing extensions, the EGW is configured with the appropriate extension numbering length.

** If local trunking is in use, calling prefixes and/or suffixes may need to be configured on the EGW.

7.2.1.2 Provisioning

The endpoint inventory can be discovered using Avaya proprietary methods (Avaya Push) or by using the automatic phone inventory feature for Layer 2 Discovery.

Avaya Push

The EGW communicates with the Avaya CM using the Avaya Push interface, in order to automatically obtain the inventory of Avaya IP phones (16xx, 46xx, 96xx). The Avaya Push interface includes a subscription service that allows the EGW to build a database of Avaya IP phones when they boot up or re-register. Each time that a phone

boots up or re-registers, the following information is provided to the EGW: IP address, extension number, and MAC address.

This feature is configured by adding the URL of the EGW to the settings text file (46xx) of the IP phones.

Automatic Phone Inventory

The feature is enabled by specifying a MAC address mask (configured using regular expressions) on a per IP-PBX basis. For the group of endpoints discovered within the group during a Layer 2 scan, the EGW adds the endpoints to the inventory, and assigns them to the connected switch/switch port and ERL.

Note: *In the case where both methods are used simultaneously, the vendor proprietary method will take precedence and will overwrite data for the subset of MAC addresses included for both inventory discovery methods.*

The regular expression will specify the MAC address Organizationally Unique Identifier (OUI) as the first 3 bytes (octets). The second group of three octets will be used to specify the range that should be included for automatic phone inventory.

Example for Avaya:

- 00040D - Assigned to Avaya IP Phones.

00040D[0-9a-fA-F]{6}

Where 00040D are the three octets of the OUI. The [0-9a-fA-F]{6} means to match any three octets for the non-OUI part of the MAC address.

Remote Location Manager (RLM)

The EGW also uses the Avaya Push interface to support the Remote Location Manager feature.

The RLM is a phone service on the EGW that is available to Avaya 46xx and 96xx phones. When a user requests the service, the RLM uses the Display Push capabilities of the Avaya CM to send the RLM provisioning page to the WML browser of the Avaya IP phone.

This feature is configured by adding the URL of the EGW to the settings text file (46xx) of the IP phones.

For more information, see the document “Configuring the Avaya Communication Manager for the EGW Appliance,” and section 17 “Provisioning Off-Campus Users.”

IP PBX Preferences

Endpoint Determination directs the EGW on which parameter to acquire the endpoint information. The default settings are as follows:

- extension
- mac
- ip
- devicename

The above settings mean that the extension of the device is first used to acquire the endpoint information.

Location Determination directs EGW on which parameter to acquire the location information. The default settings are as follows:

- static
- l2_wlan
- l3

Even though the default is as above, if the user sets a remote location, this takes precedence over the above preferences.

The “Found By” column in the **Endpoints** page is populated by the entity that was used to determine the location.

Static PBX Preferences

The settings here define the default behavior when you assign a location to the endpoint in a static setting. Use this setting to prioritize the static assignment. The default settings are as follows:

- mac
- extension
- devicename

Remote Location Manager (RLM) for Avaya Softphone

The RLM for Avaya softphone is a client for Windows workstations that prompts users to confirm or self-provision an emergency location. The RLM will pop up if an Avaya softphone is launched, or the network settings of an IP softphone are changed. The RLM then sends the softphone data and self-reported location to the EGW.

For more information, see the document “RLM for Windows Softphone Installation and Configuration Guide.”

7.2.1.3 Extension Numbering in the Avaya Dial Plan

If your phone system presents a full calling party number (CPN) to the EGW when an emergency number is dialed, you must indicate the length of your extension numbering plan on the EGW by configuring the Extension Number Length setting. The EGW uses this configuration to match the provisioned extension of the phone with the digits that present to the EGW when an emergency number is dialed. If your deployment includes dynamic phone masks, you must indicate the highest extension number length in the deployment. For example, if your deployment includes both 6 and 4 digit extensions, you must configure a value of 6 for Extension Number Length.

For more information, see the document “Configuring the ACM for the EGW Appliance.”

7.2.1.4 Understanding the Endpoints Count on System Status

The endpoints are calculated as follows:

Endpoints Count:

- The endpoint has an PBX ID
- The endpoint has an extension

Provisioned Endpoints Count:

- The endpoint has a PBX ID
- The endpoint has an extension
- The endpoint has a location ID
- The endpoint does not have a location ID but the IP address of the endpoint matches one of the configured subnets. The endpoint will get the location of the subnet.

Billable Endpoints:

- The endpoint has a PBX ID
- The endpoint has an extension.
- The endpoint has a location ID and the location is not set to local trunking or direct call delivery.
- The endpoint does not have a location ID, but the IP address of the endpoint matches one of the configured subnets. The endpoint will get the location of the subnet and the location must not be set to local trunking or direct call delivery.

7.2.2 Configuring EGW for the Avaya Communications Manager

To configure an Avaya IP-PBX

1. Click on **Configuration > IP-PBX > Add a New IP-PBX**
2. Enter the appropriate settings as described in the table below:

Table 37: Avaya IP-PBX Configuration

Parameter	Description
IP-PBX Name*	Name of the IP-PBX. Must not contain any spaces. <i>Note: The IP-PBX Name should not contain any spaces and cannot be empty. It can be a string of alphanumeric characters up to 70 characters in length. Special characters such as (underscore) and – (hyphen) are also accepted.</i>
IP-PBX Type	Avaya Aura
Protocol	Protocol that will be used to communicate between the PBX system and the EGW. Must be H.323. SIP/TCP is reserved for Avaya Session Manager deployments.
IP-PBX Version	Version number of the PBX.

Advanced Settings:**Table 38: Advanced Settings**

DNIS Prefix	This setting is used for topologies that proxy calls through a session border controller. The DNIS prefix allows multiple IP-PBX servers to share the same signaling IP address. Consult with Intrado staff before attempting to configure this section.
Local Gateway Prefix	Prefix which is used to deliver a unique ELIN to the IP-PBX for an outgoing 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.
Local Gateway Suffix	Suffix which may be used in conjunction with Prefix, in order to deliver a unique ELIN to the IP-PBX for an outbound 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.
Redirected DNIS (RDNIS)	Setting which enables an ELIN or an ELIN + DNIS to be used as the RDNIS. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. The available values for updating the IP-PBX: <ul style="list-style-type: none"> • None (selected by default) : Not a local trunk • ELIN: Local trunking use case with one Emergency number. One possible Emergency termination. • DNIS+ELIN: Local trunking use case with multiple Emergency numbers. Multiple possible Emergency terminations depending of the DNIS.
Security Desk for unprovisioned calls	Setting that enable the EGW to choose which security desk will be reached when an unprovisioned call is made. The dropdown menu will list all the security desks that are available for your organization. These would have been set up when Security Desk Groups were configured.
Use Home Numbering Plan	Setting which enables the EGW to match station extension with the calling party number (CPN) sent when 911 is dialed. Only applicable if ACM appends digits to the station extension for calls to the EGW. Choosing Yes enables you to specify the extension number length as well.
Extension Number Length	Setting used to match the station extension with the CPN sent when 911 is dialed. Comparison is made from right to left, using the configured Extension Number Length value. If the values match, the endpoint can be identified and appropriate call routing can be initiated.

IP-PBX Preferences	<p>Settings that enable the EGW to determine the endpoint and location information. Uncheck “Use Default Settings” to view and/or change the IP-PBX preferences. Change the order by picking the parameter and dropping it to the desired location in the list.</p> <p>Endpoint Determination Order that determines how the EGW will retrieve the endpoint information at call time. Default is as follows:</p> <ul style="list-style-type: none"> -extension -mac -ip -devicename <p>Location Determination Preferences that determine the order in which EGW will retrieve the location from the endpoint information at call time. Default is as follows:</p> <ul style="list-style-type: none"> -static -l2_wlan -l3
Static PBX Preferences	<p>Uncheck “Use Default Settings” to view and/or change preferences. Default is as follows:</p> <ul style="list-style-type: none"> -mac -extension -dn
SIP Extension-IP Match Preferences	<p>Preferences that determine the order in which the EGW will extract the Extension and the IP of the caller. Each entry corresponds to a predefined REGEX. As soon as a REGEX is matching the SIP URI, we record the Extension and the IP assuming the generic format:</p> <p>sip:[User];ext=[Extension]@[Host]</p> <p>Default is as follows:</p> <ul style="list-style-type: none"> - Extension: User [Ext] ; IP: Host - Extension: User ; IP: Host - Extension: Host[.*] - Extension: Host <p>Explanations of the available REGEX can be found below.</p>

REGEX Definitions:

Table 39: Regex Definitions

REGEX	SIP URI match description
Extension: User [Ext] ; IP: Host	<p>Format detected : sip:[User];ext=[Extension]@[Host]</p> <p>Extension = [User]</p> <p>IP = [Host]</p>
Extension: [User] Ext ; IP: Host	<p>Format detected : sip:[User];ext=[Extension]@[Host]</p> <p>Extension = [Extension]</p> <p>IP = [Host]</p>
Extension: User ; IP: Host	<p>Format detected : sip:[User]@[Host]</p> <p>Extension = [User]</p> <p>IP = [Host]</p>

REGEX	SIP URI match description
Extension: Host[:*]	Format detected : sip:[Host]: Extension = [Host]
Extension: Host	Format detected : sip:[Host] Extension = [Host]
IP: Host[:*]	Format detected : sip:[Host]: IP = [Host]
IP: Host	Format detected : sip:[Host] IP = [Host]

To configure an Avaya server:

1. Click on **Configuration > IP-PBX > Add a Server**
2. Configure the server information explained in the following table

Table 40: Avaya CM Server Configuration

Parameter	Description
IP-PBX	Select the IP-PBX system to which you want to associate the server.
Server Name	Name of the server. <i>The Server Name should not contain any spaces and cannot be empty. It can be a string of alphanumeric characters up to 50 characters in length. Special characters such as _ (underscore) and – (hyphen) are also accepted.</i>
Signaling IP Address/FQDN	IP address or FQDN of the signaling server.
Callback Port	Default is 1720. Must match the near end and far end listen port entered during IP-PBX configuration. Value of 0 will bypass use of callback port. For more information, see the document “Configuring the Avaya Communication Manager for the EGW Appliance.”
Connection Timeout	Amount of time in seconds that will elapse before the EGW issues a connection timeout alarm.

7.3 Configuring Avaya Session Manager

7.3.1 Understanding How the EGW works with Avaya Session Manager Deployments

7.3.1.1 Call Routing Overview

When 911 is dialed, the call is routed from the Endpoints to Session Manager. The Session Manager then routes the call to the EGW using SIP. The EGW terminates the call to the ERS using SIP. In the event of multiple machine or network failure, the Session Manager routes the call to the PSTN, via a PSTN gateway.

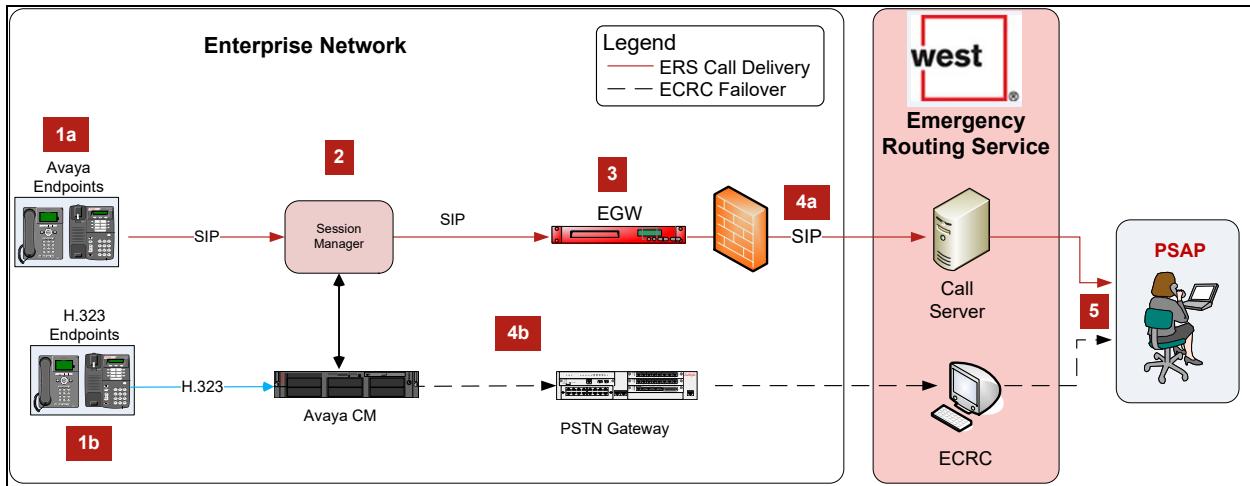


Figure 39: Avaya Call Routing Overview

1. Avaya H.323/SIP phone dials 911. Call is routed to the SM.
2. Session Manager dial plan forwards the call and extension/10-digit number to the EGW using SIP.* If the extension is sent, an Extension-Bind or ELIN number is assigned for the call.
3. EGW retrieves the appropriate ERL and routing information for the call.
4. The call is routed to the appropriate PSAP via SIP (4a) or PSTN (4b)**

* If the Avaya dial plan appends digits to outgoing extensions, the EGW is configured with the appropriate extension numbering length.

** If local trunking is in use, calling prefixes and/or suffixes may need to be configured on the EGW.

7.3.1.2 Provisioning

The endpoint inventory can be discovered using Avaya proprietary methods (Avaya Push) or by using the automatic phone inventory feature for Layer 2 Discovery.

Avaya Push:

The EGW communicates with the Avaya CM using the Avaya Push interface, in order to automatically obtain the inventory of Avaya IP phones (16xx, 46xx, 96xx). The Avaya Push interface includes a subscription service that allows the EGW to build a database of Avaya IP phones when they boot up or re-register. Each time that a phone boots up or re-registers, the following information is provided to the EGW: IP address, extension number, and MAC address.

This feature is configured by adding the URL of the EGW to the settings text file (46xx) of the IP phones.

Automatic Phone Inventory:

The feature is enabled by specifying a MAC address mask (configured using regular expressions) on a per IP-PBX basis. For the group of endpoints discovered within the group during a Layer 2 scan, the EGW adds the endpoints to the inventory, and assigns them to the connected switch/switch port and ERL.

Note: In the case where both methods are used simultaneously, the vendor proprietary method will take precedence and will overwrite data for the subset of MAC addresses included for both inventory discovery methods.

The regular expression will specify the MAC address Organizational Unique Identifier (OUI) as the first 3 bytes (octets). The second group of three octets will be used to specify the range that should be included for automatic phone inventory.

Example for Avaya:

- 00040D - Assigned to Avaya IP Phones.

00040D[0-9a-fA-F]{6}

Where 00040D are the three octets of the OUI. The [0-9a-fA-F]{6} means to match any three octets for the non-OUI part of the MAC address.

Remote Location Manager (RLM)

The EGW also uses the Avaya Push interface to support the Remote Location Manager feature.

The RLM is a phone service on the EGW that is available to Avaya 46xx and 96xx phones. When a user requests the service, the RLM uses the Display Push capabilities of the Avaya phones to send the RLM provisioning page to the WML browser of the Avaya IP phone. The user can then self-provision emergency locations.

This feature is configured by adding the URL of the EGW to the settings text file (46xx) of the IP phones.

For more information, see the document “Configuring the Avaya Communication Manager for the EGW Appliance,” and section 17 “Provisioning Off-Campus Users.”

IP PBX Preferences

Endpoint Determination directs the EGW on which parameter to acquire the endpoint information. The default settings are as follows:

- extension
- mac
- ip
- devicename

The above settings mean that the extension of the device is first used to acquire the endpoint information.

Location Determination directs EGW on which parameter to acquire the location information. The default settings are as follows:

- static
- l2_wlan
- l3

Even though the default is as above, if the user sets a remote location, this takes precedence over the above preferences.

The “Found By” column in the **Endpoints** page is populated by the entity that was used to determine the location.

Static PBX Preferences

The settings here define the default behavior when you assign a location to the endpoint in a static setting. Use this setting to prioritize the static assignment. The default settings are as follows:

- mac
- extension
- devicename

Remote Location Manager (RLM) for Avaya Softphone

The RLM for Avaya softphone is a client for Windows workstations that prompts users to confirm or self-provision an emergency location. The RLM will pop up if an Avaya softphone is launched, or the network settings of an IP softphone are changed. The RLM then sends the softphone data and self-reported location to the EGW.

For more information, see the document “RLM for Windows Softphone Installation and Configuration Guide.”

7.3.1.3 Extension Numbering in the Avaya Dial Plan

If your phone system presents a full calling party number (CPN) to the EGW when an emergency number is dialed, you must indicate the length of your extension numbering plan on the EGW by configuring the **Extension Number Length** setting. The EGW uses this configuration to match the provisioned extension of the phone with the digits that present to the EGW when an emergency number is dialed. If your deployment includes dynamic phone masks, you must indicate the highest extension number length in the deployment. For example, if your deployment includes both 6 and 4 digit extensions, you must configure a value of 6 for **Extension Number Length**.

For more information, see the document “Configuring the Avaya CM for the EGW Appliance.”

7.3.1.4 Understanding the Endpoints Count on System Status

The endpoints are calculated as follows

Endpoints Count:

- The endpoint has a PBX ID
- The endpoint has an extension

Provisioned Endpoints Count:

- The endpoint has a PBX ID
- The endpoint has an extension
- The endpoint has a location ID.
- The endpoint does not have a location ID, but the IP address of the endpoint matches one of the configured subnets. The endpoint will get the location of the subnet.

Billable Endpoints:

- The endpoint has a PBX ID
- The endpoint has an extension.
- The endpoint has a location ID and the location is not set to local trunking or direct call delivery.
- The endpoint does not have a location ID but the IP address of the endpoint matches one of the configured subnets. The endpoint will get the location of the subnet and the location must not be set to local trunking or direct call delivery.

7.3.2 Configuring EGW for the Session Manager

The Avaya Aura infrastructure uses the Session Manager (SM) core to implement a standard protocol (SIP) that enables communications products from a variety of vendors to work together. In Avaya deployments, Communication Manager (CM) PBX systems act as telephony feature servers, while the SM provides SIP-based call processing, dial plan, and endpoint registration services.

To configure the EGW for Session Manager, you need to add Communication Manager IP-PBX systems with their associated Communication Manager domains (eg. CM1.company.com, CM2.company.com). The domains must be unique per IP-PBX system. You must then add the IPs of all the signaling servers in the Aura deployment. The same signaling IP may be added to multiple IP-PBX systems, provided that each IP-PBX system is provisioned with unique domains. The signaling servers are the IP addresses of all the Session Managers in your core SIP infrastructure (SIP servers capable of routing calls to the EGW).

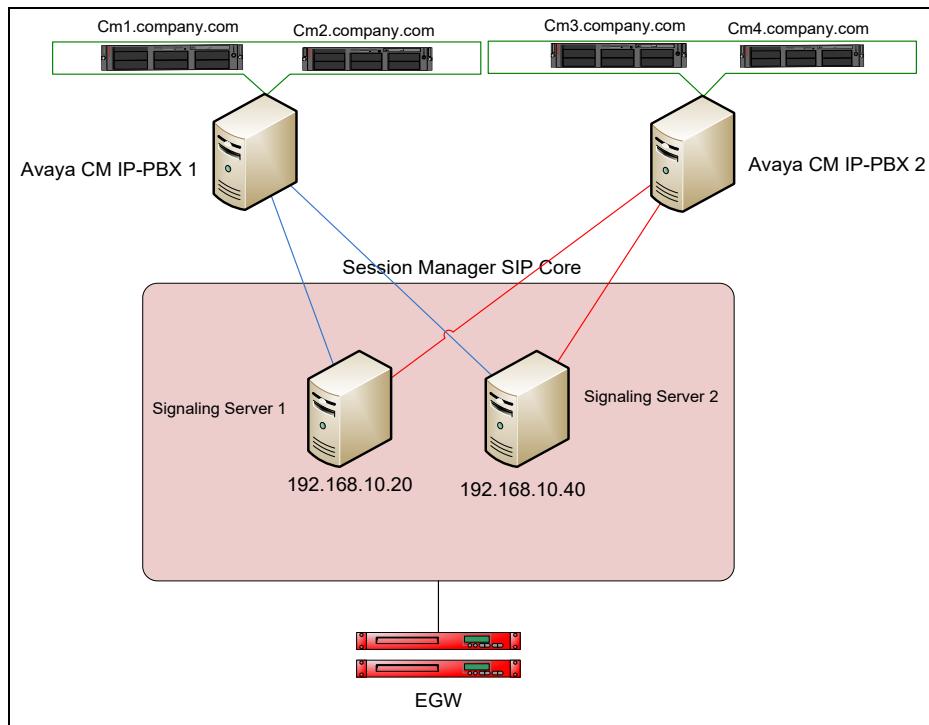


Figure 40: Avaya SM IP-PBX ConfigurationW

The recommended workflow to configure the EGW for Avaya Aura (Session Manager) deployments is as follows:

1. Configure the Communication Manager IP-PBX systems
 - a. Associate the domains of the CM servers to the IP-PBX system
2. Add the SM signaling servers to the CM IP-PBX system(s)

The procedures for this workflow are as follows”

To configure an IP-PBX

1. Click on **Configuration > IP-PBX > Add a New IP-PBX**
2. Enter the appropriate settings as described in the table below

Table 41: Avaya IP-PBX Configuration

Parameter	Description
IP-PBX Name	Name of the IP-PBX. Represents the Communication Manager IP-PBX system(s) in your Aura infrastructure. <i>The IP-PBX Name should not contain any spaces and cannot be empty. It can be a string of alphanumeric characters up to 70 characters in length. Special characters such as (underscore) and – (hyphen) are also accepted.</i>
IP-PBX Type	Avaya Aura.
IP-PBX Version	Version number of the PBX.
Protocol	SIP/TCP or H.323. SIP/TCP must be used for all Session Manager deployments. H.323 is used for Communication Manager deployments without Session Manager.

Advanced Settings:

Table 42: Advanced Settings

Endpoint ID Field	Setting that specifies the field of the SIP Invite which will be used by the EGW to retrieve the users SIP URI information. The SIP URI includes the user info (eg. Station or DID) and PBX IP address, and is used by the EGW to uniquely identify the caller. Choose from FROM or CONTACT .
Domains	The domains which represent the Communication manager servers in your Communication Manager IP-PBX system. Domains must be unique per IP-PBX system.
DNIS Prefix	This setting is used for topologies that proxy calls through a session border controller. The DNIS prefix allows multiple IP-PBX servers to share the same signaling IP address. Consult with Intrado staff before attempting to configure this section.
Local Gateway Prefix	Prefix which is used to deliver a unique ELIN to the IP-PBX for an outgoing 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.
Local Gateway Suffix	Suffix which may be used in conjunction with Prefix, in order to deliver a unique ELIN to the IP-PBX for an outbound 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.
Redirected DNIS (RDNIS)	Setting which enables an ELIN or an ELIN + DNIS to be used as the RDNIS. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. The available values for updating the IP-PBX: <ul style="list-style-type: none"> • None (selected by default) : Not a local trunk • ELIN: Local trunking use case with one Emergency number. One possible Emergency termination. • DNIS+ELIN: Local trunking use case with multiple Emergency numbers. Multiple possible Emergency terminations depending of the DNIS.
Callbacks use VIA Header	In Session Manager deployments, this parameter must be set to Yes. The VIA header is a field in the SIP INVITE sent to the EGW that contains an entry for the Session Manager signaling server IP. This IP is required by the EGW in order to successfully route callbacks to the originating station.
Callbacks use original PAI	Setting which enable the EGW to use the original PAI to obtain the station's callback number. The P-Asserted Identity is a field in the SIP INVITE sent to the EGW that can contain a 10 digit callback number. If this setting is Yes, the EGW will use the PAI as the callback number. If the PAI is non-10 digit, the EGW will use an Extension-Bind number as the callback.* If this parameter is Yes and the PAI field is empty, the EGW will associate an Extension-Bind number to the original SIP URI From or Contact. *if PAI is non-10 digit and Extension Bind is not enabled on the EGW, the EGW will route the Session Manager adaptation as the callback number. This is a misconfiguration of the system.
Security Desk for unprovisioned calls	Setting that enable the EGW to choose which security desk will be reached when an unprovisioned call is made. The dropdown menu will list all the security desks that are available for your organization. These would have been set up when Security Desk Groups were configured.
Use Media IP Address for Layer 3 Discovery	Setting that enables the EGW to obtain the IP address from the incoming SDP body at call time. Set to No by default.

Do not use these media address(es)	Using this section, the user can list all the possible IP addresses that must be excluded when they are present in the SDP body. In other words, if the IP address listed here is found in the SDP body, it may not be the endpoint's IP address. Hence, the call originating from this IP address will be processed as unprovisioned.
Use Home Numbering Plan	Setting which enables the EGW to match station extension with the calling party number (CPN) sent when 911 is dialed. Only applicable if the SM appends digits to the station extension for calls to the EGW. Choosing Yes enables you to specify the extension number length.
Extension Number Length	Setting used to match the station extension with the CPN sent when 911 is dialed. Comparison is made from right to left, using the configured Extension Number Length value. If the values match, the endpoint can be identified and appropriate call routing can be initiated.
IP-PBX Preferences	<p>Uncheck “Use Default Settings” to view and/or change the IP-PBX preferences</p> <p>Endpoint Determination Order that determines how the EGW will retrieve the endpoint information at call time. Default is as follows:</p> <ul style="list-style-type: none"> -extension -mac -ip -devicename <p>Location Determination Preferences that determine the order in which EGW will retrieve the location from the endpoint information at call time. Default is as follows:</p> <ul style="list-style-type: none"> -static -I2_wlan -I3 <p>The order can be changed by picking the parameter and moving it to its preferred place.</p>
Static PBX Preferences	Uncheck “Use Default Settings” to view and/or change preferences. Default is as follows:
SIP Extension-IP Match Preferences	Preferences that determine the order in which the EGW will extract the Extension and the IP of the caller. Each entry corresponds to a predefined REGEX. As soon as a REGEX is matching the SIP URI, we record the Extension and the IP assuming the generic format: <code>sip:[User];ext=[Extension]@[Host]</code> Default is as follows: <ul style="list-style-type: none"> - Extension: User [Ext] ; IP: Host - Extension: User ; IP: Host - Extension: Host[:*] - Extension: Host <p>Explanations of the available REGEX can be found below.</p>

REGEX Definitions:

Table 43: Regex Definitions

REGEX	SIP URI match description
Extension: User [Ext] ; IP: Host	Format detected : sip:[User];ext=[Extension]@[Host] Extension = [User] IP = [Host]
Extension: [User] Ext ; IP: Host	Format detected : sip:[User];ext=[Extension]@[Host] Extension = [Extension] IP = [Host]
Extension: User ; IP: Host	Format detected : sip:[User]@[Host] Extension = [User] IP = [Host]
Extension: Host[.*]	Format detected : sip:[Host]: Extension = [Host]
Extension: Host	Format detected : sip:[Host] Extension = [Host]
IP: Host[.*]	Format detected : sip:[Host]: IP = [Host]
IP: Host	Format detected : sip:[Host] IP = [Host]

To configure a Session Manager signaling server

3. Click on **Configuration > IP-PBX > Add a Server**
4. Configure the server information explained in the following table

Table 44: Avaya SM Server Configuration

Parameter	Description
IP-PBX	Select the IP-PBX system to which you want to associate the server.
Server Name	Name of the server. For more information, on accepted characters for this field, click here.
Signaling IP Address/FQDN	IP address or FQDN of the signaling server.
Callback Port	Default is 5060. Value of 0 will bypass use of callback port.
Connection Timeout	Amount of time in seconds that will elapse before the EGW issues a connection timeout alarm.
Monitoring Enabled	Setting which enables SIP Options monitoring for the SIP signaling server. When monitoring is enabled, the EGW will maintain the peer status as up or down for the server, and send sip options alarms and notifications accordingly. The monitoring enables the EGW to send proactive service unavailable SIP 503 response messages when a sip user agent requests a service from a server that is known to be in a down state.

7.4 Configuring Microsoft Skype for Business Server Deployments

7.4.1 Understanding How the EGW Works with Microsoft Skype for Business Server Deployments

Call Routing Overview

The call flow below illustrates an EGW deployment where the EGW server is responsible for applying specific routing instructions for a call based on a PIDF-LO location document delivered by the client. The call route policy for the call can specify SIP or PSTN termination, either through an SBC/edge device or appropriate PSTN gateway.

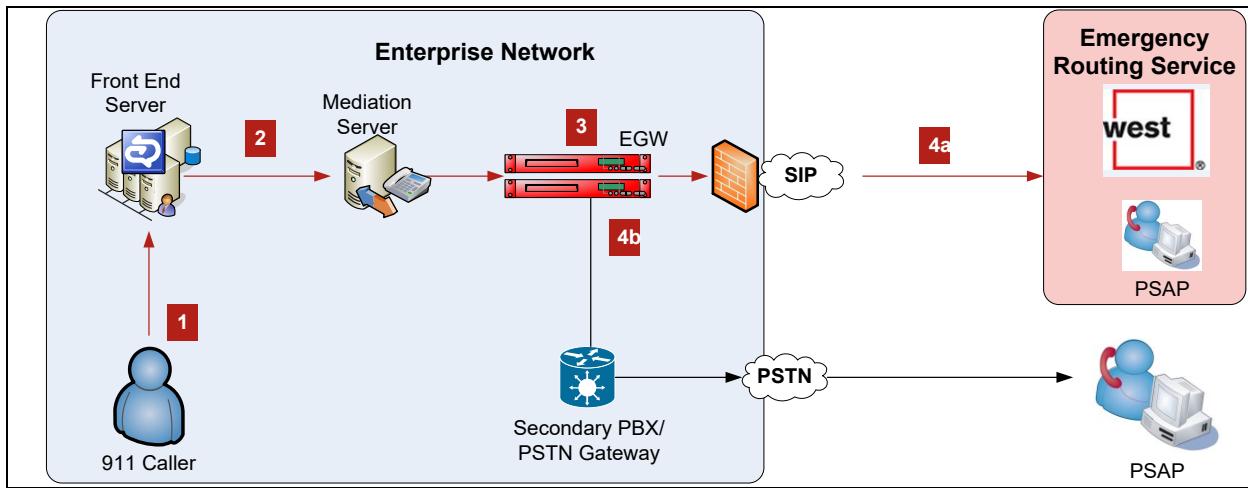


Figure 41: Lync Server Call Routing

1. Client dials 911. PIDF-LO is included in SIP INVITE
2. Microsoft Lync Server analyses the location policy for the client and applies the applicable call routing and notification policies
3. Call is routed by the Mediation Server to the EGW. EGW matches PIDF-LO to the Emergency Response Location (ERL) and specific routing instructions for the call
4. a. The EGW terminates the call to the appropriate PSAP using a SIP Trunk to the ERS
b. In the event of a local trunking call, the EGW routes the call to a secondary PBX or PSTN Gateway, for termination to the local emergency services provider using 911 trunks.

** If local trunking is in use, calling prefixes and/or suffixes may need to be configured on the EGW.

Under various server failure scenarios, 911 calls are directed to a PSTN Gateway for termination to the Intrado Emergency Call Response Center (ECRC). A dial peer is configured on the PSTN gateway that will translate the emergency DNIS (911 + endpoint identifier) to the 10 digit number of the ECRC. Gateway configuration will vary by vendor.

The diagram below depicts the following scenarios:

- In the event of EGW server failure, configured rules will initiate failover either to a secondary EGW or to the PSTN Gateway

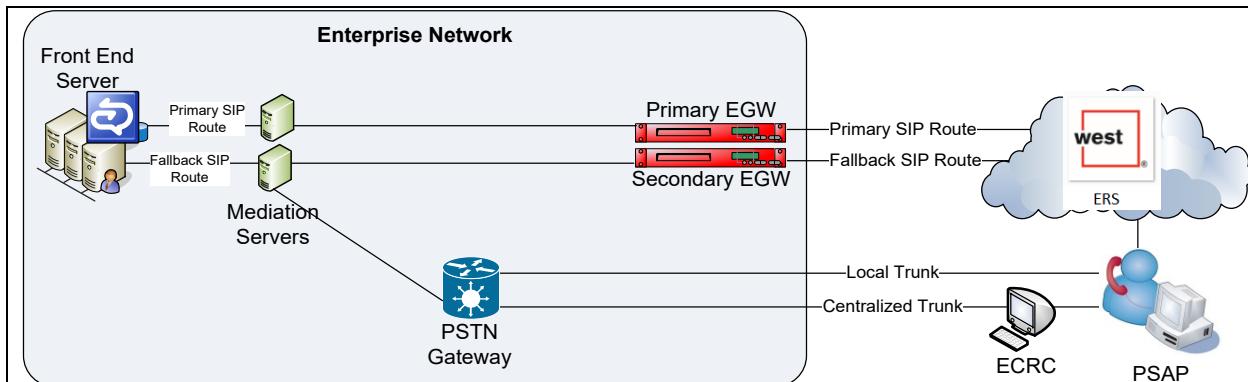


Figure 42: Lync Failover

7.4.2 Device Inventory

This section describes the various ways that the device inventory can be added to the EGW for emergency services.

7.4.2.1 Devices Added to EGW Device Inventory

Automatic Phone Inventory

The EGW provides support for Microsoft Lync Server clients that register with the registrar server and obtain their locations via the Microsoft LIS server. In this case, the LIS sends the HELD requests to the EGW and the EGW adds the clients to the endpoint inventory.

It is also possible to turn off the Automatic Phone Inventory feature. If Automatic Phone Inventory feature is turned-off, all received phone registrations will only update existing endpoints. In this configuration, endpoints need to be added to the EGW using its provisioning interfaces (batch, GUI, SOAP). A script can be used on your Lync Front End server to provision the endpoints in the EGW.

Enterprise Voice Script

This script will query the Front End server for all enterprise voice enabled users and insert them in a text file that will then be pushed to the EGW via a SOAP call to populate the Endpoint inventory.

For more information, see the document “Microsoft Lync Server 2013 EGW Configuration Guide.”

Provisioning/Endpoint Location determination

In the diagram below, the client is enabled with the E911 location policy through registration, before sending a request for location to the LIS interface. The LIS sends load balanced location requests to the redundant EGW servers, via a standard web load balancer.

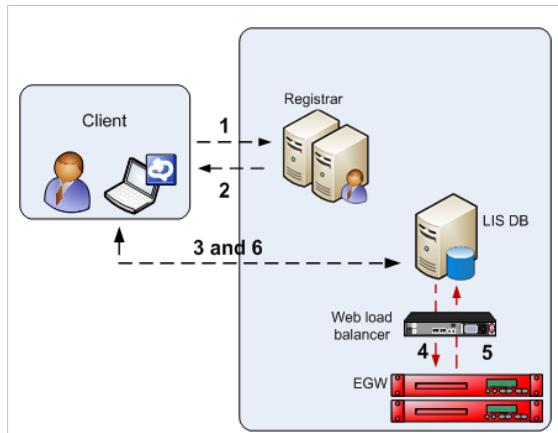


Figure 43: Provisioning and Location Determination

1. Client sends subnet information to registrar
2. Registrar returns LIS URI during registration
3. Client sends networking identifiers to the LIS using Microsoft specified interface
4. LIS forewords request to the EGW via web load balancer
5. EGW does networking identifier/location match to retrieve location in PIDF-LO format
6. EGW returns location in PIDF-LO format to Client

Other endpoints can also be added to the endpoints inventory (devices behind legacy PBX systems etc.).

On-site/Off-site Discovery:

Off-campus users can manually provision a location using the Lync client. If a user dials 911, the PIDF-LO is sent to the EGW and the EGW determines that the location was manually provided by the user. Based on this input, the EGW initiates routing to the 24/7/365 emergency call response center (ECRC) where a trained call taker confirms the caller's location and forewords the call to the appropriate regional public safety answering point (PSAP). The manually provided data is automatically provided at the ECRC for emergency calls from unprovisioned endpoints.

For more information, see the document "EGW/Microsoft Lync Server 2010 Configuration Guide."

7.4.2.2 HELD PBX Preferences

EGW uses the settings in the HELD preferences when it receives Lync calls with incoming PIDF-LO information. In this case, the **Endpoint Determination** and **Location Determination** preferences are not used and the EGW discovers the endpoint and location information based on the settings in the **HELD PBX Preferences**. On the other hand, if incoming Lync calls do not contain the PIDF-LO information, then the settings in the **Endpoint Determination** and **Location Determination** preferences apply.

MAC Address

By default, the MAC address is the first networking parameter that is used to find the endpoint. If the MAC address from the PIDF-LO matches the MAC address in the **Endpoints** page, then the location provided by the static assignment or EGW scan mechanisms are retrieved.

If the location was statically provisioned, this takes precedence over all other mechanisms such as WLAN Scan or Layer 2 scan. However, if both scan mechanisms, i.e. WLAN scan or Layer 2 scan are able to provide the location, they are considered of equal priority but EGW will assign the location that was retrieved by the most recently implemented scan.

IP Address

By default, the IP address is the second networking parameter that is used to find the endpoint, if the MAC address fails to match the endpoint information.

In this case, the endpoint's IP address is used to match one of the already-provisioned subnet location.

Extension

By default, the extension is the third networking parameter that is used to find the endpoint, if the MAC and IP address fail to return a match. When multiple devices use the same extension, the MAC address is used in addition to help determine the endpoint.

BSSID

By default, the BSSID is the fourth networking parameter that is used to find the endpoint. If the MAC address, IP address and the extension number fail to retrieve the matching endpoint, the BSSID is used to find the Access point in the WLAN configuration that matches the BSSID present in the PIDF-LO. Following this, the location information associated to this Access Point is retrieved.

Switchinfo

Lync clients installed in Windows 8 and 10 environments are capable of returning additional switch information such as switch port name, number, etc. in the PIDF-LO. If none of the above parameters are able to return a match, the switch information is used.

7.4.2.3 HELD Request

7.4.2.3.1 HELD Request Filtering

You can filter the ranges of IP subnets that will be enabled for Microsoft Skype for Business server client device inventory population on the EGW.

When a subnet is added to the Lync Subnet Filter, any HELD requests received by the EGW by endpoints within the subnet will be responded to by a SIP 404 message. The HELD request will not result in device inventory population.

Subnet filtering is enabled by configuring the “Lync Subnet Filter” Parameter. For more information see section 7.4.3 “Configuring EGW for Microsoft Lync” .

7.4.2.3.2 HELD Request with LLDP-MED

When users login to their Skype for Business clients, the EGW receives HELD requests containing the following information: MAC address, IP address, BSSID and user name.

Users logging into their Skype for Business clients in a Windows 8 or 10 environments also forward the LLDP-MED data in the HELD request. The LLDP-MED data contains the pertinent switch information such as the switch IP and port name. According to the settings in the the HELD preferences (**Dashboard**→ **Configuration** →**IP-PBX** → **HELD PBX Preferences**), EGW tries to match the parameters (MAC address, IP address, Extension, BSSID, in that order) found in the HELD request to the endpoint information to locate the caller. When LLDP-MED data is present as well in the HELD request and none of the above parameters return a location match, then the switch information (switch IP and port name) is used to find a location match from the Current switch list information.

7.4.2.4 Understanding the Endpoints Count on System Status

The endpoints are calculated as follows

Endpoints Count:

- The endpoint has a PBX ID
- The endpoint has an extension.

Provisioned Endpoints Count:

- The endpoint has a PBX ID.
- The endpoint has an extension
- The endpoint has a location ID
- The endpoint does not have a location ID but the IP address of the endpoint matches one of the configured subnets. The endpoint will get the location of the subnet.

Billable Endpoints:

- The endpoint has a PBX ID
- The endpoint has an extension
- The endpoint has a location ID and the location is not set to local trunking or direct call delivery.
- The endpoint does not have a location ID but the IP address of the endpoint matches one of the configured subnets. The endpoint will get the location of the subnet and the location must not be set to local trunking or direct call delivery.

The endpoints count at **System Status** → **Status** shows the combination of all endpoints in the system, minus any endpoints that have been filtered using HELD request filtering.

Support for Multiple Devices:

For Microsoft Lync, the endpoint count is user-based, and only takes into account the unique Lync usernames, even if they log into multiple devices.

The Last 12 months Endpoints Peak reported. Reports the peak endpoints per month (all endpoints on the system excluding those which have been filtered using HELD request filtering).

For more information see section 18 “System Status.”

7.4.2.5 Callbacks

The EGW routes callbacks from the PSAP back to the original caller that made the emergency call. The EGW stores a mapping between the extension of the caller and the IP-PBX signaling server that can be used to complete the callback. In order for the EGW to properly route the callback to the correct Microsoft Lync server 2013 IP-PBX signaling server, the parameter “Callback Use VIA Header” must be set to Yes. The parameter is defined during IP-PBX configuration at the EGW.

7.4.3 Configuring EGW for Microsoft Lync

To configure a Microsoft Lync IP-PBX

1. Click on **Configuration** → **IP-PBX** → **Add a New IP-PBX**
2. Enter the appropriate settings as described in the table below

Table 45: IP-PBX Configuration

Parameter	Description
IP-PBX Name	Name of the IP-PBX. <i>The IP-PBX Name should not contain any spaces and cannot be empty. It can be a string of alphanumeric characters up to 70 characters in length. Special characters such as (underscore) and – (hyphen) are also accepted.</i>
IP-PBX Type	Microsoft.
IP-PBX Version	Lync. If Lync connection to the ERS must be TCP. For more information, see section 5.1.1 “ERS Account Settings.”
Protocol	SIP/TCP.

Advanced Settings:

Table 46: Advanced Settings

Automatic Endpoint Inventory	Default setting is Yes . When set to Yes , HELD requests will be able to create and update endpoints at the EGW. When set to No , the HELD requests will only be able to update already existing locations. In the second scenario, the EGW’s provisioning interfaces can be used to provision the endpoints at the EGW.
Lync Subnet Filter	Filter(s) which will turn off device inventory capability for HELD requests from certain subnets. For the set of IP subnets defined, any HELD requests will receive a SIP 404 message, and the device will not be provisioned for E911 service. Eg. 192.168.0.0/16 Up to 256 subnets can be configured.
PSTN Gateway	Select a gateway that will be used to manage the dial plan for local trunking call routing. The configuration for the PSTN Gateway PBX system follows the recommended local trunking configuration. For more information, see section 6 “Configuring Local Trunking (LEC Call Routing).”
DNIS Prefix	This setting is used for topologies that proxy calls through a session border controller. The DNIS prefix allows multiple IP-PBX servers to share the same signaling IP address. Consult with Intrado staff before attempting to configure this section.
Local Gateway Prefix	Prefix which is used to deliver a unique ELIN to the IP-PBX for an outgoing 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.

Local Gateway Suffix	Suffix which may be used in conjunction with Prefix, in order to deliver a unique ELIN to the IP-PBX for an outbound 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.
Redirected DNIS (RDNIS)	<p>Setting which enables an ELIN or an ELIN + DNIS to be used as the RDNIS. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX.</p> <p>The available values for updating the IP-PBX:</p> <ul style="list-style-type: none"> • None (selected by default) : Not a local trunk • ELIN: Local trunking use case with one Emergency number. One possible Emergency termination. • DNIS+ELIN: Local trunking use case with multiple Emergency numbers. Multiple possible Emergency terminations depending of the DNIS.
Callback Use VIA Header	<p>If this field is set to Yes, the EGW will look at the VIA Header in the SIP Invite message, in order to obtain the IP address of the signaling server for the call. This may be the preferred setting in deployments where the IP included in the endpoint's SIP URI does not accurately represent the signaling server for the call.</p> <p>Note: For Microsoft Lync 2013 systems it is required to set this parameter to Yes for callbacks to work properly.</p>
Callback Use Original PAI	Setting which enable the EGW to use the PAI to obtain the station's callback number. The P-Asserted Identity is a field in the SIP INVITE sent to the EGW that can contain a 10 digit callback number. If this setting is Yes, the EGW will use the PAI as the callback number, unless an Extension-Bind or ELIN number is applicable for the call. If the parameter is Yes and the PAI field is empty, the EGW will use the original SIP URI From or Contact to obtain the callback number.
Security Desk for Unprovisioned Calls	Setting that enable the EGW to choose which security desk will be reached when an unprovisioned call is made. The dropdown menu will list all the security desks that are available for your organization. These would have been set up when Security Desk Groups were configured.
Use Media IP Address for Layer 3 Discovery	Set to No by default. Setting that enables the EGW to obtain the IP address from the incoming SDP body at call time.
Do not use these media address(es)	Using this section, the user can list all the possible IP addresses that must be excluded when they are present in the SDP body. In other words, if the IP address listed here is found in the SDP body, it may not be the endpoint's IP address. Hence, the call originating from this IP address will be processed as unprovisioned.
Add + on ELIN Callback	Setting which set the + sign in front of the ELIN callback number. In some use cases where ELINs are used as local extensions, the + is not required and can force the callback to fail. For these specific scenarios, the option should be set to No. Otherwise, by default, this value is always set to Yes.
Enhanced Endpoint Identification	Setting which enables the Endpoint information to be returned in the NAM field. Set to Yes by default.

IP-PBX Preferences	<p>Settings that enable the EGW to determine the endpoint and location information. Uncheck “Use Default Settings” to view and/or change the IP-PBX preferences. Change the order by picking the parameter and dropping it to the desired location in the list.</p> <p>Endpoint Determination Order that determines how the EGW will retrieve the endpoint information at call time. Default is as follows:</p> <ul style="list-style-type: none"> -extension -mac -ip -devicename <p>Location Determination Preferences that determine the order in which EGW will retrieve the location from the endpoint information at call time. Default is as follows:</p> <ul style="list-style-type: none"> -static -l2_wlan -l3
HELD PBX Preferences	<p>Settings that govern the order of networking parameters that the EGW will use to determine the client’s location in response to a HELD request.</p> <p>Uncheck “Use Default Settings” to view and/or change the IP-PBX preferences. Change the order by picking the parameter and dropping it to the desired location in the list.</p> <p>Default order is as follows:</p> <ul style="list-style-type: none"> -mac -ip -extension -bssid -switchinfo
Static PBX Preferences	<p>Uncheck “Use Default Settings” to view and/or change preferences. Default is as follows:</p> <ul style="list-style-type: none"> -mac -extension -dn
SIP Extension-IP Match Preferences	<p>Preferences that determine the order in which the EGW will extract the Extension and the IP of the caller. Each entry corresponds to a predefined REGEX. As soon as a REGEX is matching the SIP URI, we record the Extension and the IP assuming the generic format: <code>sip:[User];ext=[Extension]@[Host]</code></p> <p>Default is as follows:</p> <ul style="list-style-type: none"> - Extension: User [Ext] ; IP: Host - Extension: User ; IP: Host - IP: Host[*] - IP: Host <p>Explanations of the available REGEX can be found below.</p>

REGEX Definitions:

Table 47: Regex Definitions

REGEX	SIP URI match description
Extension: User [Ext] ; IP: Host	Format detected : sip:[User];ext=[Extension]@[Host] Extension = [User] IP = [Host]
Extension: [User] Ext ; IP: Host	Format detected : sip:[User];ext=[Extension]@[Host] Extension = [Extension] IP = [Host]
Extension: User ; IP: Host	Format detected : sip:[User]@[Host] Extension = [User] IP = [Host]
Extension: Host[.*]	Format detected : sip:[Host]: Extension = [Host]
Extension: Host	Format detected : sip:[Host] Extension = [Host]
IP: Host[.*]	Format detected : sip:[Host]: IP = [Host]
IP: Host	Format detected : sip:[Host] IP = [Host]

To configure a Microsoft Lync server

1. Click on **Configuration > IP-PBX > Add a Server**
2. Configure the server information explained in the following table

Table 48: Server Configuration

Parameter	Description
IP-PBX	Select the IP-PBX system to which you want to associate the server.
Server name	Name of the server. For more information on the naming strategy for this field, click here .
Signaling IP Address/FQDN	IP address or FQDN of your Mediation server.
Callback Port	Default is 5060. Must match Unified IP port number entered during IP-PBX configuration. Value of 0 will bypass use of callback port.
Connection Timeout	Amount of time in seconds that will elapse before the EGW issues a connection timeout alarm.
Monitoring Enabled	Setting which enables SIP Options monitoring for the SIP signaling server. When monitoring is enabled, the EGW will maintain the peer status as up or down for the server, and send sip options alarms and notifications accordingly. The monitoring enables the EGW to send proactive service unavailable SIP 503 response messages when a sip user agent requests a service from a server that is known to be in a down state.

7.5 Configuring ShoreTel Settings

7.5.1 Understanding How the EGW Works with ShoreTel

Call Routing Overview

When 911 is dialed, the EGW uses the phone information to determine the location of the caller. The location is used to determine the call route to the correct PSAP.

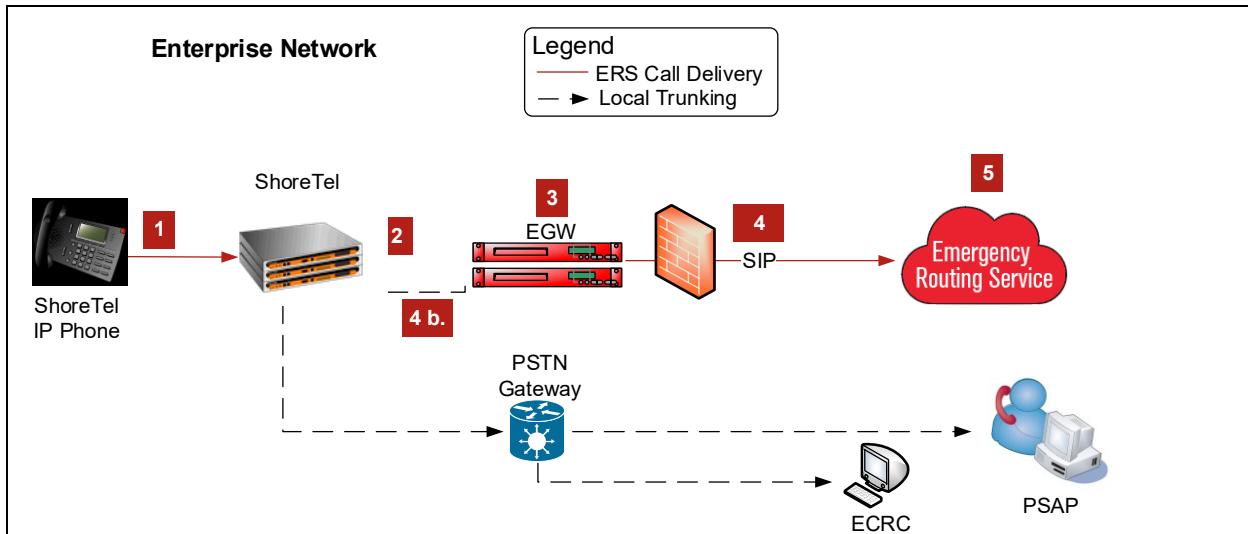


Figure 7-44 ShoreTel Call Flow

1. ShoreTel IP phone initiates a 911 call.
2. ShoreTel voice switch forwards the call and provisioning data (MAC, IP, device name) to the EGW.
3. EGW uses the MAC or IP address or device name (for softphones) to determine the location of the caller.
4. EGW routes the call to ERS:
 - a. EGW forwards the call to the ERS using SIP.
 - b. If SIP is down, EGW returns the call to the ShoreTel switch which relays the call instead to the ECRC over PSTN. In the local trunking scenario, the same call flow is followed: the ShoreTel switch routes the call over PSTN with the ELIN to the appropriate PSAP.
5. The call and location information are delivered from the ERS to the appropriate PSAP.

If the EGW servers are not available, the ShoreTel switch can route to a PSTN gateway for delivery to the ECRC.

7.5.1.1 Provisioning

The endpoints inventory for ShoreTel hardphones are automatically populated on the EGW using the automatic phone inventory feature. Multiple endpoints can also be added using the batch file processing. For more information see section [12.2 Provisioning Endpoints](#).

Layer 3 discovery is used for location provisioning when ShoreTel softphone endpoints that are discovered on a wired device connected to the corporate network are added to the EGW by the ESL process. In this case, ESL adds the device name and the MAC and IP address of the endpoint to the EGW.

WLAN discovery is used for location provisioning when ShoreTel softphone endpoints that are discovered on a wireless device on a corporate network are added to the EGW by the ESL process. ESL obtains the BSSID of the softphone and when this BSSID is matched to the BSSID of the Access Point configured on the EGW, then the location of the wireless controller is assigned to the softphone endpoint.

Automatic Phone Inventory:

The feature is enabled by specifying a MAC address mask (configured using regular expressions) on a per IP-PBX basis. For the group of endpoints discovered within the group during a Layer 2 scan, the EGW adds the endpoints to the inventory, and assigns them to the connected switch/switch port and ERL.

The regular expression will specify the MAC address Organically Unique Identifier (OUI) as the first 3 bytes (octets). The second group of three octets will be used to specify the range that should be included for automatic phone inventory.

Example for Shoretel:

- 001049 – Assigned to Shoretel phones

001049[0-9a-fA-F]{6}

Where 001049 are the three octets of the OUI. The [0-9a-fA-F]{6} means to match any three octets for the non-OUI part of the MAC address.

Remote Location Manager (RLM)

The Remote Location Manager (RLM) is a client for Windows workstations that prompts users to confirm or self-provision their location. The RLM will pop up if a softphone is launched, or if the network settings of the softphone are changed. The RLM then sends the softphone data and self-reported location to the EGW.

For more information, see the document “RLM for Windows Softphone Installation and Configuration Guide.”

IP PBX Preferences

Endpoint Determination directs the EGW on which parameter to acquire the endpoint information. The default settings are as follows:

- extension
- mac
- ip
- devicename

The above settings mean that the extension of the device is first used to acquire the endpoint information.

Location Determination directs EGW on which parameter to acquire the location information. The default settings are as follows:

- static
- l2_wlan
- l3

Even though the default is as above, if the user sets a remote location, this takes precedence over the above preferences.

The “Found By” column in the **Endpoints** page is populated by the entity that was used to determine the location.

Static PBX Preferences

The settings here define the default behavior when you assign a location to the endpoint in a static setting. Use this setting to prioritize the static assignment. The default settings are as follows:

- mac
- extension
- devicename

7.5.1.2 Understanding the Endpoints Count on System Status

The endpoints are calculated as follows

Endpoints Count:

- The endpoint has a PBX ID

Provisioned Endpoints Count:

- The endpoint has a PBX ID

- The endpoint has a location ID
- The endpoint does not have a location ID but the IP address of the endpoint matches one of the configured subnets. The endpoint will get the location of the subnet.

Billable Endpoints:

- The endpoint has a PBX ID.
- The endpoint has a location ID and the location is not set to local trunking or direct call delivery.
- The endpoint does not have a location ID but the IP address of the endpoint matches one of the configured subnets. The endpoint will get the location of the subnet and the location must not be set to local trunking or direct call delivery.

7.5.2 Configuring the EGW for the ShoreTel

In addition to configuring your ShoreTel system and provisioning ERLs and endpoints, you need to configure ShoreTel IP-PBX settings using the EGW Dashboard.

To configure a ShoreTel IP-PBX

1. Click on **Configuration** → **IP-PBX** → **Add a New IP-PBX**
2. Enter the appropriate settings as described in the table below

Table 49: ShoreTel IP-PBX Configuration

Parameter	Description
IP-PBX Name	Name of the IP-PBX. Must not contain any spaces. For more information on the naming strategy for this field, click here .
IP-PBX Type	ShoreTel.
Protocol	Protocol that will be used to communicate between the PBX system and the EGW (SIP or H.323).
IP-PBX Version	Version number of the IP-PBX.

Advanced Settings:

Table 50: Advanced Settings

Endpoint ID Field	Setting that determines which SIP field will be used to deliver the extension number or DID to the EGW. Default for ShoreTel is FROM.
DNIS Prefix	This setting is used for topologies that proxy calls through a session border controller. The DNIS prefix allows multiple IP-PBX servers to share the same signaling IP address. Consult with Intrado staff before attempting to configure this section.
Local Gateway Prefix	Prefix which is used to deliver a unique ELIN to the IP-PBX for an outgoing 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.
Local Gateway Suffix	Suffix which may be used in conjunction with Prefix, in order to deliver a unique ELIN to the IP-PBX for an outbound 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.

Redirected DNIS (RDNIS)	<p>Setting which enables an ELIN or an ELIN + DNIS to be used as the RDNIS. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX.</p> <p>The available values for updating the IP-PBX:</p> <ul style="list-style-type: none"> • None (selected by default) : Not a local trunk • ELIN: Local trunking use case with one Emergency number. One possible Emergency termination. • DNIS+ELIN: Local trunking use case with multiple Emergency numbers. Multiple possible Emergency terminations depending of the DNIS.
Callback Use VIA Header	If this field is set to Yes, the EGW will look at the VIA Header in the SIP Invite message, in order to obtain the IP address of the signaling server for the call. This may be the preferred setting in deployments where the IP included in the endpoint's SIP URI does not accurately represent the signaling server for the call.
Callback Use Original PAI	Setting which enable the EGW to use the PAI to obtain the station's callback number. The P-Asserted Identity is a field in the SIP INVITE sent to the EGW that can contain a 10 digit callback number. If this setting is Yes, the EGW will use the PAI as the callback number, unless an Extension-Bind or ELIN number is applicable for the call. If the parameter is Yes and the PAI field is empty, the EGW will use the original SIP URI From or Contact to obtain the callback number.
Security Desk for Unprovisioned Calls	Setting that enables the EGW to choose which security desk will be reached when an unprovisioned call is made. The dropdown menu will list all the security desks that are available for your organization. These would have been set up when Security Desk Groups were configured.
Use Media IP Address for Layer 3 Discovery	Set to Yes to enable Layer 3 / Subnet discovery.. This enables the EGW to obtain the IP address from the incoming SDP body at call time.
Do not use these media address(es)	Using this section, the user can list all the possible IP addresses that must be excluded when they are present in the SDP body. In other words, if the IP address listed here is found in the SDP body, it may not be the endpoint's IP address. Hence, the call originating from this IP address will be processed as unprovisioned. This is used when a call can be routed via a media gateway (e.g. for transcoding) that inserts its own IP address.

IP-PBX Preferences	<p>Settings that enable the EGW to determine the endpoint and location information. Uncheck “Use Default Settings” to view and/or change the IP-PBX preferences. Change the order by picking the parameter and dropping it to the desired location in the list.</p> <p>Endpoint Determination Order that determines how the EGW will retrieve the endpoint information at call time. Default is as follows:</p> <ul style="list-style-type: none"> -extension -mac -ip -devicename <p>Location Determination Preferences that determine the order in which EGW will retrieve the location from the endpoint information at call time. Default is as follows:</p> <ul style="list-style-type: none"> -static -I2_wlan -I3
Static PBX Preferences	<p>Uncheck “Use Default Settings” to view and/or change preferences. Default is as follows:</p> <ul style="list-style-type: none"> -mac -extension -dn
SIP Extension-IP Match Preferences	<p>Preferences that determine the order in which the EGW will extract the Extension and the IP of the caller. Each entry corresponds to a predefined REGEX. As soon as a REGEX is matching the SIP URI, we record the Extension and the IP assuming the generic format: sip:[User];ext=[Extension]@[Host]</p> <p>Default is as follows:</p> <ul style="list-style-type: none"> - Extension: User [Ext] ; IP: Host - Extension: User ; IP: Host - Extension: Host[*] - Extension: Host <p>Explanations of the available REGEX can be found below.</p>

REGEX Definitions:

Table 51: REGEX Definitions

REGEX	SIP URI match description
Extension: User [Ext] ; IP: Host	Format detected : sip:[User];ext=[Extension]@[Host] Extension = [User] IP = [Host]
Extension: [User] Ext ; IP: Host	Format detected : sip:[User];ext=[Extension]@[Host] Extension = [Extension] IP = [Host]
Extension: User ; IP: Host	Format detected : sip:[User]@[Host] Extension = [User] IP = [Host]
Extension: Host[*]	Format detected : sip:[Host]: Extension = [Host]

REGEX	SIP URI match description
Extension: Host	Format detected : sip:[Host] Extension = [Host]
IP: Host[:*]	Format detected : sip:[Host]: IP = [Host]
IP: Host	Format detected : sip:[Host] IP = [Host]

To configure a ShoreTel server

1. Click on **Configuration** → **IP-PBX** → **Add a Server**
2. Configure the server information explained in the following table

Table 52: Server Configuration

Parameter	Description
IP-PBX	Select the IP-PBX system to which you want to associate the server (site group created in the previous step).
Server Name	Name of the server. For more information on the naming strategy for this field, click here .
Signaling IP Address/FQDN	IP address or FQDN of the signaling server. The TCP/IP address of the ShoreTel switch that contains the SIP trunks.
Callback Port	Default is 5060. Must match Unified IP port number entered during IP-PBX configuration. Value of 0 will bypass use of callback port.
Connection Timeout	Amount of time in seconds that will elapse before the EGW issues a connection timeout alarm.
Monitoring Enabled	Setting which enables SIP Options monitoring for the SIP signaling server. When monitoring is enabled, the EGW will maintain the peer status as up or down for the server, and send sip options alarms and notifications accordingly. The monitoring enables the EGW to send proactive service unavailable SIP 503 response messages when a sip user agent requests a service from a server that is known to be in a down state.

7.6 Configuring Generic IP-PBX Settings

The EGW is capable of supporting basic functionality for any make and model of IP-PBX that supports SIP or H.323 protocols. The basic functionality includes call routing via ERS or local trunks, and IP phone tracking.

To configure a generic IP-PBX:

1. Click on **Configuration** > **IP-PBX** > **Add a New IP-PBX**
2. Enter the appropriate settings as described in the table below

Table 53: Generic IP-PBX Configuration

Parameter	Description
IP-PBX Name	Name of the IP-PBX. <i>The IP-PBX Name should not contain any spaces and cannot be empty. It can be a string of alphanumeric characters up to 70 characters in length. Special characters such as (underscore) and – (hyphen) are also accepted.</i>
IP-PBX Type	Select Other

Parameter	Description
Protocol	Protocol that will be used to communicate between the IP-PBX system and the EGW (SIP or H.323).

Advanced Settings:

Table 54: Advanced Settings

Domains	All the domains associated to the IP-PBX system are added here, in deployments where the endpoint identifier is presented in SIP protocol @domain to the EGW. This enables the EGW to associate the domains to the appropriate IP-PBX system based on the call from the signaling servers.
*Use Outbound Proxy	When the parameter is set to yes, the EGW will use the IP or fqdn of the Routing server as an outbound proxy. This enables the EGW to deliver the call to the originating user@domain. This supports IP-PBX architectures that use domain peering to interoperate with the EGW (eg. Sbc to sbc communication).
*Use from Domain	The Use From Domain parameter (yes/no) sets the EGW to always set the From: field to be the SIP domain of the originating domain. This is a requirement for some IP-PBX architectures, in order to support security desk routing, and callbacks.
PSTN Gateway:	Select a gateway that will be used to manage the dial plan for local trunking call routing. The configuration for the PSTN Gateway PBX system follows the recommended local trunking configuration. For more information, see section 6 “Configuring Local Trunking (LEC Call Routing).”
DNIS Prefix	This setting is used for topologies that proxy calls through a session border controller. The DNIS prefix allows multiple IP-PBX servers to share the same signaling IP address. Consult with Intrado staff before attempting to configure this section.
Local Gateway Prefix	Prefix which is used to deliver a unique ELIN to the IP-PBX for an outgoing 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.
Local Gateway Suffix	Suffix which may be used in conjunction with Prefix, in order to deliver a unique ELIN to the IP-PBX for an outbound 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.
Redirected DNIS (RDNIS)	Setting which enables an ELIN or an ELIN + DNIS to be used as the RDNIS. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. The available values for updating the IP-PBX: <ul style="list-style-type: none"> None (selected by default) : Not a local trunk ELIN: Local trunking use case with one Emergency number. One possible Emergency termination. DNIS+ELIN: Local trunking use case with multiple Emergency numbers. Multiple possible Emergency terminations depending of the DNIS.
Callback Use VIA Header	If this field is set to Yes, the EGW will look at the VIA Header in the SIP Invite message, in order to obtain the IP address of the signaling server for the call. This may be the preferred setting in deployments where the IP included in the endpoint's SIP URI does not accurately represent the signaling server for the call.

Callback Use Original PAI	Setting which enable the EGW to use the PAI to obtain the station's callback number. The P-Asserted Identity is a field in the SIP INVITE sent to the EGW that can contain a 10 digit callback number. If this setting is Yes, the EGW will use the PAI as the callback number, unless an Extension-Bind or ELIN number is applicable for the call. If the parameter is Yes and the PAI field is empty, the EGW will use the original SIP URI From or Contact to obtain the callback number.
Security Desk for Unprovisioned Calls	Setting that enables the EGW to choose which security desk will be reached when an unprovisioned call is made. The dropdown menu will list all the security desks that are available for your organization. These would have been set up when Security Desk Groups were configured.
Use Media IP Address for Layer 3 Discovery	Set to No by default. Setting that enables the EGW to obtain the IP address from the incoming SDP body at call time.
Do not use these media address(es)	Using this section, the user can list all the possible IP addresses that must be excluded when they are present in the SDP body. In other words, if the IP address listed here is found in the SDP body, as it may not be the endpoint's IP address. Hence, the call originating from this IP address will be processed as unprovisioned.
IP-PBX Preferences	<p>Settings that enable the EGW to determine the endpoint and location information. Uncheck "Use Default Settings" to view and/or change the IP-PBX preferences. Change the order by picking the parameter and dropping it to the desired location in the list.</p> <p>Endpoint Determination Order that determines how the EGW will retrieve the endpoint information at call time. Default is as follows:</p> <ul style="list-style-type: none"> -extension -mac -ip -devicename <p>Location Determination Preferences that determine the order in which EGW will retrieve the location from the endpoint information at call time. Default is as follows:</p> <ul style="list-style-type: none"> -static -I2_wlan -I3
Static PBX Preferences	Uncheck "Use Default Settings" to view and/or change preferences. Default is as follows:
SIP Extension-IP Match Preferences	<p>Preferences that determine the order in which the EGW will extract the Extension and the IP of the caller. Each entry corresponds to a predefined REGEX. As soon as a REGEX is matching the SIP URI, we record the Extension and the IP assuming the generic format: <code>sip:[User];ext=[Extension]@[Host]</code></p> <p>Default is as follows:</p> <ul style="list-style-type: none"> - Extension: User [Ext] ; IP: Host - Extension: User ; IP: Host - Extension: Host[:*] - Extension: Host <p>Explanations of the available REGEX can be found below.</p>

*Fields marked with * appear only when the IP-PBX settings are edited. They do not appear when the IP-PBX is created.

REGEX Definitions:

Table 55: REGEX Definitions

REGEX	SIP URI match description
Extension: User [Ext] ; IP: Host	Format detected : sip:[User];ext=[Extension]@[Host] Extension = [User] IP = [Host]
Extension: [User] Ext ; IP: Host	Format detected : sip:[User];ext=[Extension]@[Host] Extension = [Extension] IP = [Host]
Extension: User ; IP: Host	Format detected : sip:[User]@[Host] Extension = [User] IP = [Host]
Extension: Host[:*]	Format detected : sip:[Host]: Extension = [Host]
Extension: Host	Format detected : sip:[Host] Extension = [Host]
IP: Host[:*]	Format detected : sip:[Host]: IP = [Host]
IP: Host	Format detected : sip:[Host] IP = [Host]

To configure a generic IP-PBX server

1. Click on Configuration > IP-PBX > Add a Server
2. Configure the server information explained in the following table

Table 56: Server Configuration

Parameter	Description
IP-PBX	Select the IP-PBX system to which you want to associate the server.
Server Name	Name of the server. For more information on the naming strategy for this field, click here .
Server type	Signaling or routing. Signaling server: IP-PBX signaling component. Provides support of access side protocols such as SIP. Communicates with the carrier SBC and EGW to deliver the calls to their destinations. Routing Server: SIP redirect server. Provides location services, dial plan/digit translation and sets of routing policies. Communicates with the EGW to provide call routing instructions to the signaling server.
Signaling IP Address/FQDN	IP address or FQDN of the signaling server.
Callback Port	Default is 5060. Must match Unified IP port number entered during IP-PBX configuration. Value of 0 will bypass use of callback port.
Connection Timeout	Amount of time in seconds that will elapse before the EGW issues a connection timeout alarm.

Parameter	Description
Monitoring Enabled	Setting which enables SIP Options monitoring for the SIP signaling server. When monitoring is enabled, the EGW will maintain the peer status as up or down for the server, and send sip options alarms and notifications accordingly. The monitoring enables the EGW to send proactive service unavailable SIP 503 response messages when a sip user agent requests a service from a server that is known to be in a down state.

7.6.1 Automatic Phone Inventory

The feature is enabled by specifying a MAC address mask (configured using regular expressions) on a per IP-PBX basis. For the group of endpoints discovered within the group during a Layer 2 scan, the EGW adds the endpoints to the inventory, and assigns them to the connected switch/switch port and ERL.

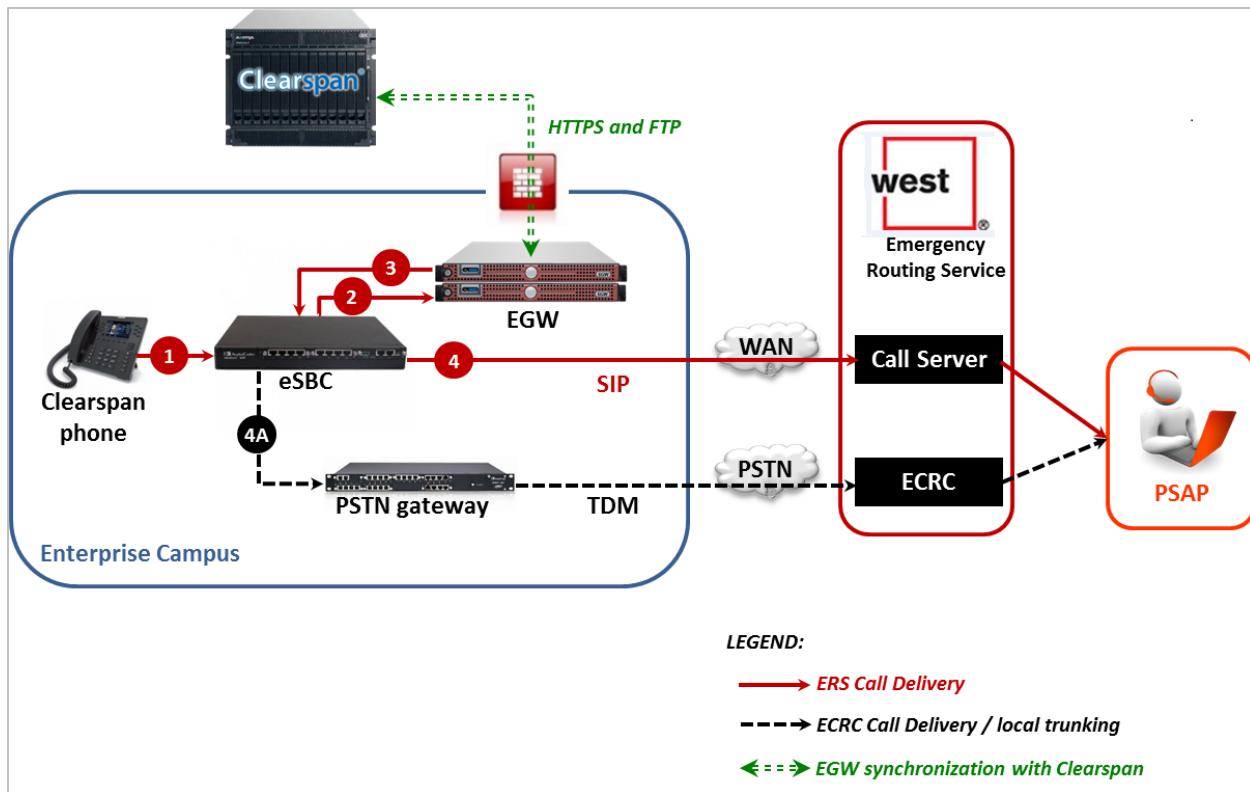
The regular expression will specify the MAC address Organizationally Unique Identifier (OUI) as the first 3 bytes (octets). The second group of three octets will be used to specify the range that should be included for automatic phone inventory.

7.7 Configuring Aastra Clearspan

7.7.1 Understanding how the EGW works with Aastra Clearspan

7.7.1.1 Call Routing Overview

When 911 is dialed, the call is routed through the enterprise Session Border Controller (eSBC) to the EGW. The EGW will modify the FROM field or insert a custom EGW-Location-Key header that will be used to identify the location of the caller. The callback number is populated in the P-Asserted-Identity header. As opposed to ELINs, this allows callbacks to route directly back to users without being re-mapped. The EGW then sends the call back to the eSBC for outbound processing. This approach provides additional alternate outbound call completion options and reuses the VoIP infrastructure, including firewall configurations, via the site's eSBC.



1. The Clearspan station initiates a 911 call by sending the call request to the eSBC.
2. The eSBC forwards the 911 call request to the EGW. The EGW uses the extension to determine the location of the caller.
3. The EGW identifies the location of the caller and forwards the request back to the eSBC with a unique 911 digit string.
4. Based on the unique 911 digit string and associated routing rules, the eSBC will forward the call. The call will be delivered via SIP to the ERS Call Server.
 - (4A) As an alternate connection, the call can be rerouted to the ERS ECRC via a local PSTN gateway.

7.7.1.2 Provisioning

The endpoint records in the EGW are managed by an endpoint record manager (ERM) application. The ERM communicates with the Clearspan user/device database and the EGW to synchronize the endpoint records in the EGW with the users and devices configured in the Clearspan system. The ERM is configured to run on a periodic basis determined by the customer.

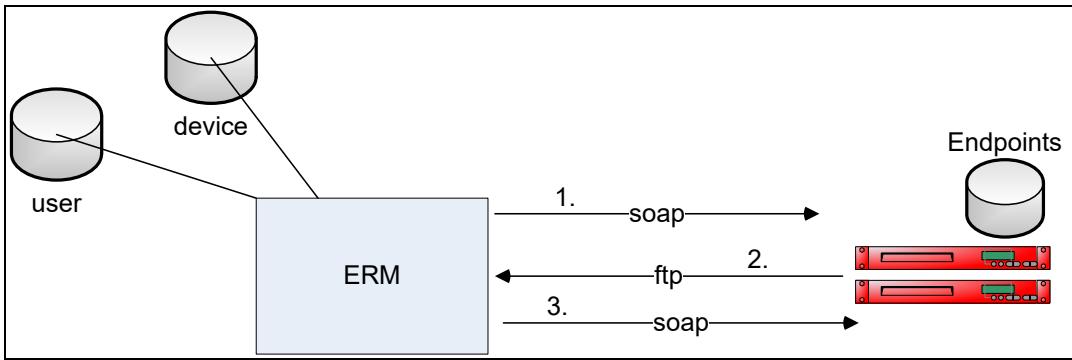


Figure 46: Endpoint Provisioning Logic

1. Aastra Endpoint record manager (ERM) creates endpoint records on EGW
2. ERM downloads ftp report of results from EGW to compare with user and device db from Clearspan system.
3. ERM extracts users and devices from Clearspan for comparison to EGW endpoints

For each device, if the device does not already have an endpoint record in EGW, then it can be created using SOAP. If endpoint record exists, then ERL ID is retrieved through Layer 2 Discovery mechanisms.

For each user:

-if user does not exist in EGW create user via SOAP. User takes ERL ID from device. If user ERL ID is older than device ERL ID, copy device ERL ID to user.

For all records:

-delete endpoint records that do not have a corresponding user or device in Aastra Clearspan.

Automatic Phone Inventory

The feature is enabled by specifying a MAC address mask (configured using regular expressions) on a per IP-PBX basis. For the group of endpoints discovered within the group during a Layer 2 scan, the EGW adds the endpoints to the inventory, and assigns them to the connected switch/switch port and ERL.

The regular expression will specify the MAC address Organizationally Unique Identifier (OUI) as the first 3 bytes (octets). The second group of three octets will be used to specify the range that should be included for automatic phone inventory.

Example for Aastra:

- 0010BC – Assigned to Aastra phones

0010BC[0-9a-fA-F]{6}

Where 0010BC are the three octets of the OUI. The [0-9a-fA-F]{6} means to match any three octets for the non-OUI part of the MAC address.

IP PBX Preferences

Endpoint Determination directs the EGW on which parameter to acquire the endpoint information. The default settings are as follows:

- extension
- mac
- ip
- devicename

The above settings mean that the extension of the device is first used to acquire the endpoint information.

Location Determination directs EGW on which parameter to acquire the location information. The default settings are as follows:

- static
- l2_wlan
- l3

Even though the default is as above, if the user sets a remote location, this takes precedence over the above preferences.

The “Found By” column in the **Endpoints** page is populated by the entity that was used to determine the location.

Static PBX Preferences

The settings here define the default behavior when you assign a location to the endpoint in a static setting. Use this setting to prioritize the static assignment. The default settings are as follows:

- mac
- extension
- devicename

7.7.1.3 Understanding the Endpoints Count on System Status

The endpoints are calculated as follows

Endpoints Count:

- The endpoint has a pbx id
- The endpoint has an extension.

Provisioned Endpoints Count:

- The endpoint has a pbx id
- The endpoint has an extension.
- The endpoint has a location ID
- The endpoint does not have a location ID but the ip address of the endpoint matches one of the configured subnets. The endpoint will get the location of the subnet.

Billable Endpoints:

- The endpoint has a pbx id.
- The endpoint has an extension
- The endpoint has a location ID and the location is not set to local trunking or direct call delivery.
- The endpoint does not have a location ID but the ip address of the endpoint matches one of the configured subnets. The endpoint will get the location of the subnet and the location must not be set to local trunking or direct call delivery.

7.7.2 Configuring the EGW for the Aastra Clearspan

To configure an IP-PBX:

1. Click on Configuration > IP-PBX > Add a New IP-PBX
2. Enter the appropriate settings as described in the table below

Table 57: IP-PBX Configuration

Parameter	Description
IP-PBX Name	Name of the system For more information on the characters accepted in this field, click here .
IP-PBX Type	Aastra
Protocol	Protocol that will be used to communicate between the PBX system and the EGW (SIP/UDP, SIP/TCP or H.323).

Advanced Settings:**Table 58: Advanced Settings**

Endpoint ID Field	Setting that determines which SIP field will be used to deliver the extension number or DID to the EGW. Please use default values or consult with Intrado installation staff prior to making changes.
DNIS Prefix	This setting is used for topologies that proxy calls through a session border controller. The DNIS prefix allows multiple IP-PBX servers to share the same signaling IP address. Consult with Intrado staff before attempting to configure this section.
Local Gateway Prefix	Prefix which is used to deliver a unique ELIN to the IP-PBX for an outgoing 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.
Local Gateway Suffix	Suffix which may be used in conjunction with Prefix, in order to deliver a unique ELIN to the IP-PBX for an outbound 911 call using local trunking. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. This field should be blank if calls are routed to the ERS.
Redirected DNIS (RDNIS)	Setting which enables an ELIN or an ELIN + DNIS to be used as the RDNIS. Only applicable if call routing to the local exchange carrier will be used for the IP-PBX. The available values for updating the IP-PBX: <ul style="list-style-type: none"> • None (selected by default) : Not a local trunk • ELIN: Local trunking use case with one Emergency number. One possible Emergency termination. • DNIS+ELIN: Local trunking use case with multiple Emergency numbers. Multiple possible Emergency terminations depending of the DNIS.
Callback Use VIA Header	If this field is set to Yes, the EGW will look at the VIA Header in the SIP Invite message, in order to obtain the IP address of the signaling server for the call. This may be the preferred setting in deployments where the IP included in the endpoint's SIP URI does not accurately represent the signaling server for the call.
Callback Use Original PAI	Setting which enable the EGW to use the PAI to obtain the station's callback number. The P-Asserted Identity is a field in the SIP INVITE sent to the EGW that can contain a 10 digit callback number. If this setting is Yes, the EGW will use the PAI as the callback number, unless an Extension-Bind or ELIN number is applicable for the call. If the parameter is Yes and the PAI field is empty, the EGW will use the original SIP URI From or Contact to obtain the callback number.
Security Desk for Unprovisioned Calls	Setting that enables the EGW to choose which security desk will be reached when an unprovisioned call is made. The dropdown menu will list all the security desks that are available for your organization. These would have been set up when Security Desk Groups were configured.

Use Media IP Address for Layer 3 Discovery	Set to No by default. Setting that enables the EGW to obtain the IP address from the incoming SDP body at call time.
Do not use these media address(es)	Using this section, the user can list all the possible IP addresses that must be excluded when they are present in the SDP body. In other words, if the IP address listed here is found in the SDP body, it may not be the endpoint's IP address. Hence, the call originating from this IP address will be processed as unprovisioned.
IP-PBX Preferences	<p>Settings that enable the EGW to determine the endpoint and location information.</p> <p>Uncheck “Use Default Settings” to view and/or change the IP-PBX preferences. Change the order by picking the parameter and dropping it to the desired location in the list.</p> <p>Endpoint Determination Order that determines how the EGW will retrieve the endpoint information at call time. Default is as follows:</p> <ul style="list-style-type: none"> -extension -mac -ip -devicename <p>Location Determination Preferences that determine the order in which EGW will retrieve the location from the endpoint information at call time. Default is as follows:</p> <ul style="list-style-type: none"> - static - I2_wlan - I3
Static PBX Preferences	<p>Uncheck “Use Default Settings” to view and/or change preferences. Uncheck “Use Default Settings” to view and/or change the IP-PBX preferences. Change the order by picking the parameter and dropping it to the desired location in the list.</p> <p>Default is as follows:</p> <ul style="list-style-type: none"> - mac - extension - dn
SIP Extension-IP Match Preferences	<p>Preferences that determine the order in which the EGW will extract the Extension and the IP of the caller. Each entry corresponds to a predefined REGEX. As soon as a REGEX is matching the SIP URI, we record the Extension and the IP assuming the generic format:</p> <p>sip:[User];ext=[Extension]@[Host]</p> <p>Default is as follows:</p> <ul style="list-style-type: none"> - Extension: User [Ext] ; IP: Host - Extension: User ; IP: Host - Extension: Host[:*] - Extension: Host <p>Explanations of the available REGEX can be found below.</p>

REGEX Definitions:

Table 59: REGEX Definitions

REGEX	SIP URI match description
Extension: User [Ext] ; IP: Host	Format detected : sip:[User];ext=[Extension]@[Host] Extension = [User] IP = [Host]
Extension: [User] Ext ; IP: Host	Format detected : sip:[User];ext=[Extension]@[Host] Extension = [Extension] IP = [Host]
Extension: User ; IP: Host	Format detected : sip:[User]@[Host] Extension = [User] IP = [Host]
Extension: Host[.*]	Format detected : sip:[Host]: Extension = [Host]
Extension: Host	Format detected : sip:[Host] Extension = [Host]
IP: Host[.*]	Format detected : sip:[Host]: IP = [Host]
IP: Host	Format detected : sip:[Host] IP = [Host]

To configure an IP-PBX server

1. Click on Configuration > IP-PBX > Add a Server
2. Configure the server information explained in the following table

Table 60: Server Configuration

Parameter	Description
IP-PBX	Select the IP-PBX system to which you want to associate the server.
Server Name	<Name of the location/group> i.e. Campus1 For more information on the characters accepted in this field, click here.
Signaling IP Address/FQDN	<Audiocodes edge device's LAN IP address>
Callback Port	<Audiocodes edge device's LAN port>
Connection Timeout	Amount of time in seconds that will elapse before the EGW issues a connection timeout alarm. Default 30 seconds.
Monitoring Enabled	Setting which enables SIP Options monitoring for the SIP signaling server. When monitoring is enabled, the EGW will maintain the peer status as up or down for the server, and send sip options alarms and notifications accordingly. The monitoring enables the EGW to send proactive service unavailable SIP 503 response messages when a sip user agent requests a service from a server that is known to be in a down state.

7.8 Configuring Lync for MSE

If you already have the Microsoft MSE for EGW enabled and configured, and also have Lync softphones in your organization, you can easily integrate them for your emergency call needs.

7.8.1 Call Routing Overview

When 911 is dialed, the IP address of the softphone is retrieved in order to generate a Wireless User Location URL. This is then used to generate the map, which will pinpoint the exact location of the caller.

7.8.2 Dashboard Configuration

To ensure that the Lync Softphone client works with the MSE/ Aruba integration, the following settings need to be configured on the EGW dashboard:

To configure Lync for MSE from the EGW Dashboard:

1. Click on the **Configuration** tab.
2. Go to the IP-PBX tab.
3. Click on the **Add a new IP-PBX** button.
4. In the **IP-PBX Type** section, choose **Microsoft**.
5. Ensure that the **Enhanced Endpoint Identification** is set to **Yes** and press **Save** to retain your settings.

8 Configuring Alerting, Notification

The EGW sends a variety of on-site alerts and notifications, and is capable of performing call routing to on-site answering points and security desks.

The EGW sends a variety of email notifications under different circumstances:

- Crisis Alerts (emergency number is dialed)
- Unprovisioned call alerts (emergency call is made from an unprovisioned endpoint)
- Off-campus alerts (emergency call is made from an off-campus endpoint)
- Alarm notifications (an alarm is raised by the EGW)
- Batch processing notification (reports for batch file processing)
- Grace period reminder notifications

For more information concerning support and maintenance, see the document “West Safety Services Support Policy”.

Alarms and alerts can be sent using email or by SNMP traps. For more information, see section 8.2 “Configuring SNMP Traps Settings.”

Grace period

You will be sent notification emails every 24 hours during the duration of the time that your EGW server is in grace mode. An EGW server will go into grace mode, if it has been de-activated. For more information, please see section 19.2 “Network Settings” and section 2.3 “Licensing.”

Desk Alert

Desk Alert software is installed on security desk workstations. It notifies security desk personnel of 911 calls in progress using pop-up windows and audible alerts.

Security Desk Call Routing

Security desk call routing allows 911 calls to be sent to security desk personnel in order to improve on-site response times. Unique security desk routing rules can be configured per ERL. There are two options: direct call delivery and call monitoring with optional one-way mute. If call monitoring is selected for an ERL, the call is routed to the PSAP and security staff may listen to and participate in the call. If one-way mute is enabled, the security desk staff may only listen, and may not participate in the call.

8.1 Configuring Mail Server Settings

Mail server settings must be configured to send email notifications. The EGW contains its own built-in mail server, and can be configured with two SMTP Hosts for greater redundancy.

To configure mail server settings

1. Click on **Configuration** → **Notification** → **Mail Server**.
2. Configure the appropriate settings as described in the following table:

Table 61: Mail Server Settings

Parameter	Description
SMTP Host 1 (FQDN)	FQDN of SMTP host. Default is localhost.* Must be an FQDN.
SMTP Host 2 (FQDN)	FQDN of the failover email server. Local host or external mail server. Must be an FQDN.
RAC SMTP Host IP	IP address of the mail server for the Remote Access Controller.
Port	Port for relaying outgoing mail to the mail server. Default is 25. **

FROM Name	From name that will be sent with the email. Default is Emergency Gateway.
FROM	Email address that will send the alert emails. Default is EGW@domain.com

*The default values should be used for the EGW's internal mail server. If an external mail server is in use, the **Host** field should be set to the appropriate FQDN of the host.

**An appropriate port must be configured if an external mail server is in use.

Mail Server Tools

The mail connectivity test ensures that the host, port and FROM fields have been configured correctly. If there are problems with the settings, error messages will be raised.

To test connectivity

- Click on **Test Connectivity** or **Test RAC** under **Mail Server Tools**

Once the connection has been verified, a test email may be sent by entering the email in the dialogue box and clicking on **Send**.

8.2 Configuring SNMP Traps Settings

To enable the EGW to send SNMP traps for alarms and alerts to your network management system (NMS), the following is required.

1. Configure SNMP Trap receiver settings at the Dashboard (community string etc.) including the trap selections
2. Configure scheduled task "Queue SNMP Trap"

8.2.1 Configuring the SNMP Trap Receiver Settings

To configure the trap receiver settings

1. Click on **Configuration** → **Notification** → **SNMP Traps**
2. Click on the **Add** button under **SNMP Trap Receivers List**.

The **SNMP Trap Receiver** section is displayed. Here, you can configure the trap receiver settings, as explained below:

3. Under the **SNMP Trap Receiver** section, enter the following information:
 - a. **Name:** Enter a name for the trap receiver.
 - b. **IP Address:** This is the IP address of the trap receiver on the network.
 - c. **Port:** This is the default UDP port 162 for receiving traps
 - d. **SNMP version:** Choose between 2c and 3.
 - e. **Apply to:** Choose from **BOTH, PRIMARY, SECONDARY**

Note: A single trap receiver may be used to receive SNMP traps from both EGW servers. It is also possible to setup separate trap receivers for each EGW server.

4. f. **Enable:** Place a check mark to enable and remove the check mark to disable.

Note: During maintenance windows, SNMP trap notifications can be disabled by checking this box. When the trap receiver is enabled you will have access to the Test trap receiver feature.

4. Under the **Authentication** section, enter the following information:
 - a. **Community String:** Provide a valid community string for authentication between the trap receiver and the EGW. This field is only available when SNMP version 2c is chosen.

- b. **EGW Engine ID:** This is the unique **Engine ID** assigned to your organization's EGW. The Primary and Secondary EGW pair do not share the Engine ID. Use this **Engine ID** to integrate with your organization's network management system to send and receive SNMP traps. This field cannot be edited.
- c. **Security Level:** Choose between **noAuthnopriv**, **authnoPriv** and **authpriv** to set the security level required for the interaction. For more information, please refer to section [SNMP Version 3](#).
- d. **Security Name:** Provide the security name required for SNMP version 3. Up to 50 alphanumeric characters are accepted here.
- e. **Auth Protocol:** Choose from **MD5** or **SHA**. This field is only available when **Security Level** is chosen as **authnoPriv** or **authpriv**.
- f. **Auth Passphrase:** Provide the password required for authentication. A minimum of 8 alphanumeric characters are required and a maximum of 50 alphanumeric characters are accepted in this field.
- g. **Encrypt Protocol:** Choose from **DES** or **AES**. This field is only available when Security Level is chosen as **authPriv**.
- h. **Encrypt Passphrase:** Provide the password required for encryption. A minimum of 8 alphanumeric characters are required here.

5. Under the **Trap Selection** section, you can choose to configure SNMP traps for the following alerts:

- Alarms
- Crisis Alerts
- Unprovisioned Alerts
- Off-Campus alerts

8.2.2 Authentication

SNMP trap receivers use either SNMP version 2c or SNMP version 3 for authentication between the trap receiver and the EGW.

You can select the host and port destination to which the trap messages are sent. When using SNMP version 2c, authentication is done using the community string whereas, when using the SNMP version 3, additional security parameters need to be configured.

8.2.2.1 SNMP Version 3

SNMP version 3 is more secure than SNMP version 2c. If SNMP version 3 is chosen, additional security parameters become available, as defined below:

- When **noAuthNoPriv** is chosen as the **Security Level**, only the **Security Name** is the mandatory field. The **Security Name** is used for authentication and the data packet is passed in clear text.
- When **authNoPriv** is chosen as the **Security Level**, the **Security Name**, **Auth Protocol** and the **Auth Passphrase** need to be configured. MD5 or SHA is used for authentication and the remaining data packet is passed as clear text.
- When **authPriv** is chosen as the **Security Level**, the **Security Name**, **Auth Protocol**, **Auth Passphrase**, **Encrypt Protocol** and **Encrypt Passphrase**. MD5 or SHA is used for authentication and encryption is done with either **DES** (Data Encryption Standard) or **AES** (Advanced Encryption Standard). The entire data packet is encrypted.

8.2.2.2 Sending a Test Trap Notification

To ensure that the SNMP Trap receiver has been properly setup you can send a test trap.

A test trap looks like the following:

```
SNMP : 162|TRAP[requestID=24862, errorStatus=Success(0), errorIndex=0, VBS[1.3.6.1.2.1.1.3.0 = 7 days, 21:33:36.51;
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.38995.1.1.1.0.1; 1.3.6.1.4.1.38995.1.1.1.0.0.1 = 63; 1.3.6.1.4.1.38995.1.1.1.0.0.2 = 3;
1.3.6.1.4.1.38995.1.1.1.0.0.3 = Sending test SNMP trap; 1.3.6.1.4.1.38995.1.1.1.0.0.8 = 1330699859; 1.3.6.1.4.1.38995.1.1.1.0.0.11 =
1]]
```

To send a test trap:

1. Click on **Configuration>Notification>SNMP Traps**.
2. Ensure that there is a checkmark next to **Enable** in the trap receiver settings.
3. Click on Send Trap.
4. Verify in your MIB Browser for the management station that the trap was successfully sent.

8.2.3 Configuring the Scheduled Task

The task Queue SNMP Trap is executed once every minute and runs for 50 seconds. It checks the logs of alarm and alert notifications and sends them as SNMP traps to the configured SNMP trap receivers.

For more information see section 10.1 “Configuring the Task Scheduler Time of Day Settings.”

8.3 Alarms

Alarm notifications are sent to configured distribution lists to report application errors, hardware problems, and connectivity disruptions. There are three severity levels for the alarms: **Warning**, **Critical**, and **Info**. The user can configure the severity level for each alarm using the **Alarms Frequency** page.

Each alarm severity level may be configured with a unique distribution list. You may also configure a distribution list for emails sent via the RAC interface.

To configure a distribution list

1. Click on **Configuration → Notification → Alarms Email List**.

The **Alarm Email List** page will display all the email addresses that are configured to receive emails.

2. Click on the **Add** button.
3. Under the **Email** column, enter the email address where you want to receive the email when an alarm is raised.
4. Choose the severity level: **Critical**, **Warning** or **Info**.
5. Click on the **Save** button.

Using this page, you can also delete or edit email addresses or the severity of the alarms for which you want to receive notifications for.

8.3.1 Alarm Reporting

The **Alarm Status** and the number of **Critical** and **Warning** alarms can be viewed on the EGW dashboard in the top left corner.

Critical alarms are signified by the color red and **Warning** alarms are signified by the color yellow. When you click on the red or yellow boxes, you will be re-directed to the **Alarms** page.

8.3.1.1 Alarm Reporting Mechanism

Various modules in the EGW can experience issues. As soon as these issues are detected, the modules themselves alert the alarm module. The alarm module first raises the alarm. Then, the following things happen, in sequence:

1. The alarm is shown on the dashboard. See section 8.3.1 Alarm Reporting above.
2. The alarm is captured in the alarm logs. See section 18.3.2 Alarms Logs.
3. The alarm is displayed in the Alarms page. See section 18.6 Alarms.
4. The alarm notification module is alerted to the activation of the alarm

The alarm notification module then decides based on the settings in the **Task Scheduler** and the settings in the **Alarm Notification Frequency Settings** whether and when an alarm notification email needs to be sent. For more information on this, please refer to section [8.3.2 Alarms Frequency Settings](#).

The alarm notification module is also responsible for sending SNMP traps. For more information on this, please refer to [8.2 Configuring SNMP Traps Settings](#).

8.3.2 Alarms Frequency Settings

The **Alarms Notification Frequency Settings** page displays all the alarms and their default frequency settings. This page will enable you to edit the **Alarm Level** and the **Alarm Notification Frequency** for every alarm available.

To access **Alarm Notification Frequency Settings**, click on **Configuration** → **Notification** → **Alarms Frequency**.

The **Alarm Level** can even be set to **Disabled** to deactivate the alarm.

To change the alarm frequency settings:

1. Click on **Configuration** → **Notification** → **Alarms Frequency**.

The Alarm Notification Frequency Settings page is displayed. The alarms are listed by these categories: **AXL**, **Configuration**, **CTI**, **Dashboard**, **Discovery**, **Monitoring**, **Nagios**, **Routing**, **Scheduler** and **System**.

The following columns are displayed:

- a. **Alarm ID**:
- b. **Alarm Name**:
- c. **Alarm Level**:
- d. **Alarm Notification Frequency**:
- e. **Actions**
2. Click on the **Edit** button under the **Actions** column.
3. Choose the **Alarm Level** from the dropdown. The choices available are:
 - a. **Critical**
 - b. **Warning**
 - c. **Info**
 - d. **Disabled**
4. Next, choose the **Alarm Notification Frequency** from the dropdown. The choice available are:
 - a. **Never**
 - b. **Always**
 - c. **Once every 5 minutes**
 - d. **Once every 15 minutes**
 - e. **Once every 30 minutes**
 - f. **Once an hour**
 - g. **Once every 12 hours**
 - h. **Once a day**
5. Click on the **Save** button.
6. To restore the EGW alarm default settings, click on the **Restore Default Values** button on the top right corner of the table.

For a complete list of alarms on the EGW see section [20 EGW Alarms](#).

8.3.2.1 Understanding Alarm Notification Frequency Settings

Using the Alarm Notification Frequency settings page, you can manipulate the frequency of notifications sent (emails and/or traps) for the alarms being raised by the EGW.

The following table describes the **Alarm Notification Frequency** that you can set for each alarm on the EGW and what it means and how the alarm reporting will be affected:

Table 62: Alarm Frequency Settings

Alarm Frequency	Description
Never	When you set the Alarm Notification Frequency to Never , this means that an email and/or an SNMP trap will never be sent when this alarm is raised or cleared. <i>Note: Alarms that never trigger email notifications can be seen on the Alarms page (System Status →Alarms)</i>
Always	When you set the Alarm Notification Frequency to Always , this means that an email and/or an SNMP trap will be sent every time this alarm is raised or cleared.
Once every 5 minutes	When you set the Alarm Notification Frequency to Once every 5 minutes , this means that if this alarm is raised more than once in the last 5 minutes, then only one email and/or SNMP trap will be sent every 5 minutes. However, an email and/or trap will be sent when the alarm is cleared.
Once every 15 minutes	When you set the Alarm Notification Frequency to Once every 15 minutes , this means that if this alarm is raised more than once in the last 15 minutes, then only one email and/or SNMP trap will be sent every 15 minutes. However, an email and/or trap will be sent when the alarm is cleared.
Once every 30 minutes	When you set the Alarm Notification Frequency to Once every 30 minutes , this means that if this alarm is raised more than once in the last 30 minutes, then only one email and/or SNMP trap will be sent every 30 minutes. However, an email and/or trap will be sent when the alarm is cleared.
Once an hour	When you set the Alarm Notification Frequency to Once an hour , this means that if this alarm is raised more than once in the last hour, then only one email and/or SNMP trap will be sent every one hour. However, an email and/or trap will be sent when the alarm is cleared.
Once every 12 hours	When you set the Alarm Notification Frequency to Once every 12 hours , this means that if this alarm is raised more than once in the last 12 hours, then only one email and/or SNMP trap will be sent every 12 hours. However, an email and/or trap will be sent when the alarm is cleared.
Once a day	When you set the Alarm Notification Frequency to Once a day , this means that if this alarm is raised more than once in the last 24 hours, then only one email and/or SNMP trap will be sent once a day. However, an email and/or trap will be sent when the alarm is cleared.

*Please note that when an alarm is raised and cleared within the time interval specified in the **Alarm Notification Frequency**, and then raised again within the same interval, the alarm notification email and/ or trap will be sent again.*

Example: Consider the alarm **AXL-01**.

The pre-conditions are defined as follows:

- The **Alarm Notification Frequency** of **AXL-01** is set to **Once an hour**.
- The AXL task is scheduled to perform the scan every **30 minutes**.

If the AXL scheduled task was unable to complete, the EGW will raise an alarm and an email notification (and/ or trap) will be sent. If you fail to clear the alarm, when the AXL task performs the scan after 30 minutes, the same issue will be detected and the same alarm will be raised again. However, in this case, a second email notification (and/or trap) will not be sent.

If the alarm is not cleared, every time the AXL scheduled task runs (every 30 minutes), the alarm will be raised. However, the alarm notification email will only be sent once an hour.

When the alarm is cleared, the email notification (and/or trap) will be sent to notify that the alarm has been cleared.

*Please note that the time interval in the **Alarm Notification Frequency** only applies to sending email notifications (and/or traps) when the alarm is raised. Every time an alarm is cleared, an email notification will be sent, irrespective of the time interval specified in the **Alarm Notification Frequency**.*

8.4 Configuring Crisis Alerts

Crisis Alert notifications are created when a user makes an emergency call. The notification events can be sent as emails or as SNMP traps.

The content of the email is configurable using the administrative Dashboard interface. You may configure the Crisis Alert feature to best communicate critical information to your staff, using the terminology with which they are most familiar.

The notification objects that will be sent for Crisis Alert SNMP traps are described in the document “schedu”.

You can also configure a url that can be used by your emergency responders to better respond to alert notifications. You can configure and test the url variables using the Dashboard. You can provision the url and its variables using the EGW provisioning interfaces: Dashboard, batch, or SOAP.

For more information, see section 11.2.2.3 “URL Template Editor”

8.4.1 Crisis Alert Email Settings

By configuring Crisis Alert email settings you can:

- Specify the **FROM Name**, **FROM field**, **Subject** and **Email Header**.
- Change the naming of the fields that are included in the email.
- Change what fields are displayed and the order in which they appear.

You can also customize the address fields (PIDF-LO) which will comprise the location information which is included in crisis alert emails. The address fields are customized using the Multiline address template. To configure the multiline address template, see section 8.7 “Customize Address.”

Please note that the number of email recipients that can receive crisis email alerts is limited to 12. This is configurable in the “Add ERL” page. For more information, please refer to section Add ERL Page.

To configure Crisis Alert

1. Click on **Configuration > Notification > Crisis Email Alert**
2. Enter the content of the **FROM Name**, **FROM field**, **Subject** and **Email Header**
3. Modify the naming of fields as required
4. Change the order of fields so that the most relevant fields are displayed first

The following field titles may be changed using the **Crisis Email Alert Settings**

Table 63: Crisis Email Settings

Field Title	Description
FROM Name	Name that will appear in the FROM Name.
FROM Field	Email that will appear in the FROM Field.

Field Title	Description
FROM Name	Name that will appear in the FROM Name.
Subject	Subject of the email.
Email Header	Text that will appear in the body header of the email.
Endpoint	Identifier of the phone. Could be modified to display “Extension Number” or “Telephone Number” depending on the terminology with which your employees are most familiar.
Timestamp	Time when the 911 call was made. Could be changed to “Time of Call,” for example.
Callback	10-digit number that can be dialed to reach the 911 caller in the event that the 911 call is dropped.
URL Data	A web link that references a campus map or database query. Could be changed to “Extra,” for example.
IP-PBX System	IP-PBX system from which the 911 call was made. Could be changed to “PBX System” or “Phone System,” for example.
Calling Party Name	Name of the employee that dialed 911. Could be changed to “Employee Name,” for example.
Location	Emergency location record that is stored in EGW. Could be changed to “ALI Data,” for example.

To modify the fields in the email and change their order:

1. From the **Crisis Email Alert** screen, select the fields you want to include in the email and click **Set**.
2. Using the **Up** and **Down** buttons, position the fields in the required order.

8.5 Configuring Unprovisioned Call Alerts

Unprovisioned Alert notifications are created when a user makes an emergency call and the user is not already defined in the EGW endpoints inventory. The notification events can be sent as emails or as SNMP traps.

The content of the email is configurable using the administrative Dashboard interface. You may configure the feature to best communicate critical information to your staff, using the terminology with which they are most familiar.

The notification objects that will be sent for Alert SNMP traps are described in the document “West EGW Proprietary MIB.”

8.5.1 Unprovisioned Alert Email Settings

By configuring Unprovisioned Email Alert you can:

- Specify the **FROM Name**, **FROM Field**, **TO Email**, and **Subject** of the email.
- Change the naming of the fields that are included in the email.
- Change what fields are displayed and the order in which they appear.

To configure Unprovisioned Email Alert

1. Click on **Configuration** → **Notification** → **Unprovisioned Email Alert**
2. Enter the content of **FROM Name**, **FROM Field**, **TO Email**, and **Subject**
3. Modify the naming of fields as required
4. Change the order of fields so that the most relevant fields are displayed first

The following field titles may be changed using the **Crisis Email Alert Settings**.

Table 64: Unprovisioned Email Alert Settings

Field Title	Description
FROM Name	Name that will appear in the FROM Name.
FROM Field	Email that will appear in the FROM Field.
TO Email	Email address that will receive the Unprovisioned Email Alerts.

Field Title	Description
Subject	Subject of the email.
Email Header	Text that will appear in the body header of the email.
Endpoint	Identifier of the phone. Could be modified to display “Extension Number” or “Telephone Number” depending on the terminology with which your employees are most familiar.
Timestamp	Time when the 911 call was made. Could be changed to “Time of Call,” for example.
Callback	10-digit number that can be dialed to reach the 911 caller in the event that the 911 call is dropped.
IP-PBX System	IP-PBX system from which the 911 call was made. Could be changed to “PBX System” or “Phone System,” for example.
Calling Party Name	Name of the employee that dialed 911. Could be changed to “Employee Name,” for example.

To modify the fields in the email and change their order:

1. From the **Unprovisioned Email Alert** screen, select the fields you want to include in the email and click **Set**.
2. Using the **Up** and **Down** buttons, position the fields in the required order.

8.6 Configuring Off-Campus Call Alerts

Off-campus Alert notifications are created when a user makes an emergency call and the user is located off-site. The notification events can be sent as emails or as SNMP traps.

The content of the email is configurable using the administrative Dashboard interface. You may configure the feature to best communicate critical information to your staff, using the terminology with which they are most familiar.

The notification objects that will be sent for Alert SNMP traps are described in the document “EGW Proprietary MIB Reference.”

8.6.1 Off-campus alert email settings

By configuring off-campus email alerts you can:

- Specify the **FROM Name**, **FROM Field**, **TO Email**, and **Subject** of the email.
- Change the naming of the fields that are included in the email.
- Change what fields are displayed and the order in which they appear.

You can also customize the address fields (PIDF-LO) which will comprise the location information which is included in off-campus alert emails. The address fields are customized using the Multiline address template. To configure the multiline address template, see section 8.7 “Customize Address.”

To configure off-campus email alerts

1. Click on **Configuration** → **Notification** → **Off-Campus Email Alerts**
2. Enter the content of **FROM Name**, **FROM Field**, **TO Email**, and **Subject**
3. Modify the naming of fields as required
4. Change the order of fields so that the most relevant fields are displayed first

The following field titles may be changed using the crisis email alert settings.

Table 65: Off Campus Email Alert Settings

Field Title	Description
FROM Name	Name that will appear in the FROM Name Field.
FROM Field	Email that will appear in the FROM Field.
TO Email	Email address that will receive the off-campus email alerts.

Field Title	Description
Subject	Subject of the email.
Email Header	Text that will appear in the body header of the email.
Endpoint	Identifier of the phone. Could be modified to display "Extension Number" or "Telephone Number" depending on the terminology with which your employees are most familiar.
Callback	10-digit number that can be dialed to reach the 911 caller in the event that the 911 call is dropped.
IP-PBX System	Phone system from which the 911 call was made.
Location	Emergency location record that is stored in EGW. Could be changed to "ALI Data," for example.
Timestamp	Time when the 911 call was made. Could be changed to "Time of Call," for example.
Calling Party Name	Name of the employee that dialed 911. Could be changed to "Employee Name," for example.

To modify the fields in the email and change their order

1. From the **Off-Campus Email Alerts** screen, select the fields you want to include in the email and click **Set**.
2. Using the **Up** and **Down** buttons, position the fields in the required order.
3. Click on **Save** to retain these settings.

8.7 Customize Address

The **Customize Address Form** can be used to customize both the single line and multi line address templates.

The **Single Line Address Template** controls the display of provisioned address information at the following outputs:

- Search ERLs
- Search Endpoints
- ERL and endpoint summary reports

The **Multiline Address Template** controls the display of provisioned address information at the following outputs:

- Crisis Alerts
- Test mode notifications
- Off-campus alerts

8.7.1 Multiline Address Template

The address information displayed in alert emails includes the values of the PIDF-LO fields and any PIDF-LO field labels that you decide to include.

From the customize address form you can perform the following

- Add labels to describe the PIDF-LO field values that will be included in the emails (eg. House number, house number suffix)
- Remove an address field
- Change the order of the address fields

To add an address label

1. Click on **Configuration** → **Notification** → **Customize address**
2. Enter the label text next to the PIDF-LO address field of choice in the **Multiline address Template** selection box (eg. House Number, House suffix etc.)

To remove an address field:

- Highlight the field and click back or delete (ensure line break is also deleted)

To change the order of the fields

- Copy the field that you would like to move
- Delete the field
- Move the field to its new location and paste.

8.7.1.1 Multiline Address Template Example:

This example shows the content of the Location information presented in a crisis alert email, based on address field customization.

Information Entered into Multiline Address Template:

Street number: {HNO}

Street: {RD}

Street Suffix: {STS}

Suite: {LOC}

Room: {ROOM}

City: {A3}

Country: {country}

Postal Code: {PC}

Crisis Alert Email:

Endpoint: 801

Callback: 1234567891

IP-PBX System: ccm6

Location

Street number: 888

Street: MAIN

Street Suffix: ST

Suite: 6B3

Room: 312

City: NEW YORK

Country: USA

Postal Code: 10044

Timestamp: 2010-04-29 17:44:03

URL Data

8.7.2 Single Line address template

The address information outputted by the single line address template includes the values of the PIDF-LO fields and any additional text or characters that are added in the template (eg. If you want to add separators such as commas and parentheses, or to add field labels to the address display).

From the customize address form you can perform the following:

- Add punctuation (commas, parentheses etc.) or additional text (eg. field labels) to the address information output
- Remove an address field
- Change the order of the address fields

To add punctuation or additional text

1. Click on **Configuration>Notification>Customize address**
2. Enter the characters at the location of your choosing in the Single Line Address template selection box

To remove an address field:

- Highlight the field and click back or delete

To change the order of the fields

- Copy the field that you would like to move
- Delete the field
- Move the field to its new location and Paste.

8.7.2.1 Single Line Address Template Example

Information Entered into Single line Address Template:

{HNO}, {RD}, {LOC},{A3},{A1},{country},{PC},

Output at Search ERLs:

911, Main, Suite 203, New York, NY, USA, 10044

8.8 Configuring Desk Alert

To configure Desk Alert, see the “Desk Alert Administrator User Guide”.

9 Advanced Settings

Advanced settings allow you to enable/disable services, and to configure the timer settings and scheduled tasks that control when certain tasks are executed (SNMP, AXL, etc.).

9.1 Global Settings Screen

You can enable/disable a variety of services from the global settings screen. The applicability of these services to your deployment will vary, based on adopted features.

To view the global settings screen

- Click on **Configuration > Advanced > Global**.

This screen is only available to users with Full access.

Table 66: Global Settings Configuration

Field	Description	Notes
CTI Enabled	Enables the connection between the EGW and CTI Manager servers.	When 911 is dialed, the EGW uses a CTI route point to obtain a phone's MAC, IP address, and extension. These parameters are used to make routing decisions. Requires additional IP-PBX and EGW configuration. See the document "Configuring the CUCM for the EGW Appliance," for more information.
Avaya Push Admin Enabled	Enables the Avaya Push feature. The EGW communicates with ACM using the Avaya Push interface, in order to automatically obtain the inventory of Avaya IP phones (16xx, 46xx, 96xx).	Requires additional IP-PBX configuration. For more information, see the document "Configuring Avaya Communication Manager for the EGW Appliance."
AXL Enabled	An AXL interface to a CUCM server enables the EGW to obtain the Cisco IP phone inventory.	Requires IP-PBX integration and EGW configuration.
NENA 2 US Enabled	Setting that enables the NENA 2 file generation feature in the US.	If multiple ERLs are assigned to the same ELIN in the EGW, this option will not be available. The NENA 2 file generation feature can only be used when each ELIN represents a unique location. The purpose of a NENA 2 file is to populate a Private ALI or LEC PS-ALI.
NENA 2 CAN Enabled	Setting that enables the NENA 2 file generation feature in Canada.	If multiple ERLs are assigned to the same ELIN in the EGW, this option will not be available. The NENA 2 file generation feature can only be used when each ELIN represents a unique location. The purpose of a NENA 2 file is to populate a Private ALI or LEC PS-ALI.
EGW Version Number	Displays the current version of the EGW. This field cannot be modified.	

Field	Description	Notes
EGW License Key	License key which identifies your EGW appliance.	
Canadian Addresses Enabled	Enables the Canadian 911 service.	Requires that the province be specified during ERL provisioning. All Canadian ERLs are associated to ELINs. To upload a Canadian address, see section 11.3 "ERL Batch File Format."
Maximum Permitted Administrators	Maximum amount of administrators for the EGW.	Each administrator can be assigned an access level by the default account (Limited, Provisioning, Full).
Maximum Permitted Desk Alert Licenses	Maximum amount of Desk Alert clients that can be active at any one time.	When this feature is enabled the Desk Alert tab will be available to configure the Desk Alert server. The Desk Alert client software must be installed on each PC workstation that will count as a Desk Alert license. For more information see the document "Desk Alert Administrator User Guide."
Call Recording	Enables the call recording feature.	
Crisis Email Alert Language	Specifies the language of the crisis email alert messages.	English or French. French is the default used for the Canadian service.
Server Time Zone	Specifies the time zone where the primary EGW is located.	The time zone is set based on the city where your data center is located.
Local CPM	Yes/No. Specifies if the CPM is located locally or remotely. If set to yes, the cpm url is hardcoded to localhost location.	For more information about the Central LIS deployment scenario, see section 3.3.3 "Centralized LIS Deployment."
CPM Primary URL	Specifies the location of the primary EGW for the CPM module. Default should be in the following form: http://EGW1IP/CPM/cpm.php	Networking environments that use NAT can set the CPM URLs to the NAT IP. In a central LIS environment, the URL can be the network location of the central LIS.
CPM Secondary URL	Specifies the location of the secondary EGW for the CPM module. Default should be in the following form: http://EGW2IP/CPM/cpm.php	Networking environments that use NAT can set the CPM URLs to the NAT IP. In a central LIS environment, the URL can be the network location of the central LIS.
Default Signaling Port	Default SIP signaling port.	Default is 5060 (UDP).
Default Analog Phone Prefix	Parameter that enables the EGW to identify Cisco analog phones behind VG gateways and Cisco ATAs. Default is VGC, ATA, AAL, AN2.	The setting specifies the MAC address prefix that the EGW will use when matching CTI data against the data in the endpoints inventory at call time.

Field	Description	Notes
Default CTI Redirect DNIS	Default DNIS which is used when the 911 call is redirected from the EGW back to the CUCM (Cisco only).	Default is *913. A corresponding route pattern must be programmed into the IP-PBX which will recognize this DNIS. To configure the CUCM, see the document "Configuring the CUCM for the EGW Hardware Appliance."
Fallback DNIS	DNIS which is used to route the 911 call to Intrado in the event of an internal EGW error. Note: If 10 digit number is used as fallback DNIS, the egw will deliver the call from the originating IP-PBX server. Eg.1234567890 It is also possible to specify a specific IP-PBX server or gateway for use with the fallback DNIS Eg. 5145551234@192.168.0.251:5060	The fallback DNIS typically points to the route pattern of the ECRC configured on the IP-PBX server or gateway. The route pattern is configured to send the call to the Intrado emergency call response center (ECRC).
Fallback Protocol	Fallback protocol between the EGW and the IP-PBX which will be used if the SIP connection is unavailable.	Default is SIP.
Send PAI as Custom Header	Setting that enables the callback number to be delivered to the ERS in a custom SIP header. This can be applicable to deployments that deliver calls from the EGW to the ERS via an SBC. Some SBCs will overwrite the SIP FROM field with the PAI, unless this parameter is set to Yes.	
DNIS for 911 calls	DNIS that will be sent to the EGW when 911 is dialed.	Default is 911.
Endpoint Batch Processing Format Type	Determines the format of the endpoint batch processing file.	Incremental
CDR Export Format Type	Determines the format that will be used to export CDRs to FTP. All, CSV, or text	There are two folders: "/home/cdr/csv/" and/or "/home/cdr/txt/" If setting is All, then both folders are populated with CDR data when the report runs.

Field	Description	Notes
CDR Export Address Template	<p>Determines the address format that will be included in the CDRs exported to FTP.</p> <p>Single Line or Multi Line.</p>	
Delete Layer 2 Logs Older than	<p>Settings that determine the length of time the Layer 2 Logs can exist on the EGW before it is deleted.</p> <p>Default is 1 day.</p>	
Archive Logs Older Than	<p>Setting which determines the length of time that a log can exist on the EGW before it is archived.</p> <p>Default is 180 days.</p>	
Delete Archived Logs Older Than	<p>Setting which controls the length of time that a log can be archived on the EGW before it is deleted.</p> <p>Default is 180 days.</p>	
Delete Endpoint and Location Log Records Older Than	<p>Setting that determines how long endpoint and erl batch logs can exist on the EGW before they are deleted.</p> <p>Default is 180 days.</p>	
Lync Endpoints Validity Period	<p>Setting that determines the period for which the location information associated to the Lync endpoint is valid.</p> <p>The default period is 30 days.</p> <p>When the time period specified in the Lync Endpoints Validity Period has passed:</p> <ul style="list-style-type: none"> Any Lync endpoint that does not have a defined extension will be deleted. Duplicate Lync endpoints that have the same extension but different location information will be deleted. <p><i>Note: With regards to the deletion of duplicate endpoints, the last instance of a provisioned Lync extension will not be deleted.</i></p>	It does not determine the removal of unused provisioned Lync extensions. It only removes outdated duplicate information associated to the extension.

Field	Description	Notes
Device and Extension Validity Period	Setting that determines the period after which all devices and extensions that are not referenced to or by any endpoints are deleted. Default is 30 days.	

Note: When you change the time zone using the Global Settings screen, you will need to manually restart the EGW for this change to take place. This must also be repeated on the Secondary EGW.

Note: In Worldwide mode, the Extension Bind duration parameter is available from the Global settings screen, and determines the amount of time that ELIN numbers remain bound to the stations that dialed 911.

9.1.1 Changing the Time Zone

The time zone on the EGW dashboard can be changed by performing the following steps:

1. Click on **Configuration** → **Advanced** → **Global**.
2. Click on **Edit**.
3. Scroll down to the **Server Time zone** field and choose the time zone of your preference from the drop-down list provided.
4. Click on **Save** to retain your change.
5. Manually restart your EGW pair to apply the time zone change.

Note: It is very important that the EGW pair be restarted to apply the time zone changes.

9.1.2 Configuring Timer Settings

You can view timer settings by clicking on **Configuration** > **Advanced** > **Timer Settings**. The following fields in the table below are displayed.

This screen is only available to users with Full access.

Table 67: Timer Settings

Field	Description	Notes
Session Timeout(s)	Specifies the amount of inactive time in seconds that will elapse before the Dashboard session expires.	Default is 28800 seconds.
Layer 2 Port Discovery Interval	Specifies amount of layer 2 scan jobs that will complete before the EGW performs the next full port discovery cycle. Numerical value between 0 and 1488.	For more information, see section 13.2 “Understanding How Layer 2 Discovery Works.”
CPM Timeout	Setting that determines how long the EGW waits for a response from the CPM to return the routing instructions for the call.	When the timer has been exceeded the Primary CPM Request Timeout alarm is generated.

Field	Description	Notes
CPM Default Connection Timeout	Specifies the amount of time in seconds that the EGW will wait for the ERS to answer an emergency call. If the ERS SBC is unable to answer the call before this timer has expired, the current call to the ERS SBC will be terminated and placed to the next available destination.	Default is 120 seconds.

9.1.3 Batch Settings

You can view the batch settings by clicking on **Configuration > Advanced > Batch Settings**.

The batch settings are used to configure email distribution lists for batch email error reports and summary reports.

Summary Reports

The summary reports include the name of the batch file and other basic information, as illustrated in the following example:

Filename: myBatchFile.txt
 Successful records: 0
 Failed records: 1
 Result filename: log_myBatchFile_1205960355.txt
 Date/Time: 2008-03-19 16:59:15

Error Reports

Error reports include the batch lines that failed to pass with the appropriate error code:

02:LOC_X;211;MAIN ST;;NEW YORK;NY;USA;10044;0;0;;;;

Table 68: Batch Settings

Parameter	Description
Batch Tries	Setting that governs the amount of retries that the EGW will make when sending SOAP queries to the ERS when connectivity is interrupted. Applicable to ERL validation requests.
Location Summary Reports	Email that will receive summary reports.
Location Error Reports	Email that will receive error reports.
Endpoint Summary Reports	Email that will receive summary reports.
Endpoint Error Reports	Email that will receive error reports.
Switch Summary Reports	Email that will receive summary reports.
Switch Error Reports	Email that will receive error reports.
Subnet Summary Reports	Email that will receive summary reports.
Subnet Error Reports	Email that will receive error reports.
WLAN Summary Reports	Email that will receive summary reports for WLAN scanning.
WLAN Error Reports	Email that will receive error reports for WLAN scanning.

9.1.4 Redundancy Settings

The redundancy settings screen provides status information for some critical services and tasks running on the EGW servers. The status information indicates the server (primary or secondary) where the tasks are set to run. For critical services, the status information reports the up/down status.

Redundancy status information can be modified for the following tasks:

- Avaya
- AXL
- CDR Export
- Generate NENA 2 File
- Layer 2 Discovery
- Lync Endpoints
- Queue Email
- Queue SNMP Trap
- Statistics
- WLAN Discovery

For more information, see section 10.1 “Configuring the Task Scheduler Time of Day Settings.”

You can edit the redundancy settings to change which EGW server will be active per task. You can also set if there are any task dependencies.

9.1.4.1 Modifying Task Redundancy Status

For either server (primary/secondary) it is possible to set a task to active or standby

To set active/standby status

1. Click on **Configuration>Advanced>Redundancy**.
2. Click on **Edit**.
3. For the task of choice set to active or standby.

9.1.4.2 Setting Task Dependencies

For either server (primary/secondary) it is possible to indicate if there are any dependencies on a per task basis.

The recommended configuration is to set the tasks as Active on the primary EGW. With this configuration, the dependency setting on the primary would be None. On the secondary, scheduled tasks would be set to Standby. The dependency setting should be set to Primary.

Warning: *In the recommended configuration, do not set Dependency on the secondary as None or Secondary. This is an unsupported configuration.*

To set task dependencies

1. Click on **Configuration → Advanced → Redundancy**.
2. Click on **Edit**.
3. Modify the task dependency status as required.

9.1.5 SOAP Server

The EGW’s SOAP server can be used to provision ERLs and endpoints. The EGW comes pre-configured with default SOAP usernames and passwords, as indicated in the table below.

You can view SOAP server settings by clicking on **Configuration → Advanced → SOAP Server**. The following fields are displayed.

Table 69: SOAP Server Configuration

Field	Description	Notes
SOAP Server Locations Enabled	Enables SOAP server for ERLs on the EGW. Enabled by default.	Uses SOAP/XML interface to EGW SOAP server. Development work is required to develop the webpage based on the needs of your deployment.

SOAP Locations Username	Username that is sent with each SOAP locations call. DEFAULT_SOAP_USER	Encrypted using SSL.
SOAP Locations Password	Password that is sent with each SOAP locations call. DEFAULT_SOAP_PWD	Encrypted using SSL.
SOAP Server Endpoints Enabled	Enables SOAP server for endpoints on the EGW. Enabled by default.	
SOAP Endpoints Username	Username that is sent with each SOAP endpoints call. DEFAULT_SOAP_USER	Encrypted using SSL.
SOAP Endpoints Password	Password that is sent with each SOAP endpoints call. DEFAULT_SOAP_PWD	Encrypted using SSL.
3 rd Party Layer 2 SOAP Server Enabled	Enable the SOAP server on the EGW for third party SNMP data.	
3 rd Party Layer 2 SOAP Server Username	Username for SOAP calls to SNMP SOAP3 rd Party Layer 2 SOAP Server.	
3 rd Party Layer 2 SOAP Server Password	Password sent with SOAP calls to 3 rd Party Layer 2 SOAP Server.	

10 Task Scheduler

Scheduled tasks dictate the daily schedule by which a variety of jobs are executed.

The Task Scheduler **Time of Day** settings can be edited to determine the frequency at which the task scripts will run.

Table 70: List of Scheduled Tasks

Task	Description	Note
Archive logs	<p>The task will archive all of the log files (batch etc.) on the EGW periodically as zip files. The archive files are stored in the location of the original log files (eg. ERL, endpoint batch files).</p> <p>Note: Default setting is on the 1st and 14th of the month. The schedule for Archive logs should be setup to clear past logs in accordance with your system's log growth rate. This will ensure smooth EGW operation and that log files do not grow to unmanageable sizes.</p>	
Avaya	Task that processes the endpoints data, received from the Avaya push interface subscription service. The task adds the data to the endpoints inventory.	
AXL	Task that processes the endpoints data, obtained from the AXL connection to the Cisco UCM.	
Backup	Backs up the data on the EGW periodically. The database and config files are sent to the egwbackup ftp folder, for access by the egwbackup user.	/home/egwbackup/egw_backup-(today's date).tar.gz
Batch Endpoints	Task that connects to the batch folder on the EGW to periodically process the batch files for endpoints.	
Batch 3 rd Party Layer 2	Task that periodically imports 3rd party SNMP batch data into the database.	
Batch locations	Task that connects to the batch folder on the EGW to periodically process the batch files for locations.	
Batch subnets	Task that connects to the batch folder on the EGW to periodically process the batch files for subnets.	
Batch switches	Task that connects to the batch folder on the EGW to periodically process the batch files for switches.	
Batch WLAN	Task that connects to the batch folder on the EGW to periodically process the batch files for WLAN data.	
CDR Export	Backs up the CDRs on the EGW periodically. The CDRs are sent to the cdr ftp folder, for access by the cdruser.	/home/cdr/csv
Delete archive	Task that periodically deletes archived items on the EGW: batch files, batch logs, call recordings, upgrade logs.	Default setting is 180 days for batch provisioning and 365 days for recordings and upgrade logs)

Delete Layer 2 Logs	Task that periodically deletes logs generated by the Layer 2 scan.	Default setting is 1 day.
Device and Extension Cleanup	Task removes all devices and extensions that are not referenced to or by any endpoints and have been in the EGW records for longer than the Device and Extension Validity Period .	Default setting is 30 days.
EGW Peer Check	Task that runs to check connectivity to the Peer EGW.	The EGWs are self-monitoring and issue alerts warnings based on peer connectivity.
Generate NENA 2 file	Task that periodically generates NENA 2 files and stores them at ftp of EGW.	The task uses the ELIN inventory to generate the NENA 2 files.
IP display	Task that periodically refreshes the IP of EGW displayed at the EGW Console screen.	
Layer 2 Scheduled 3 rd Party	Task that processes 3 rd party data in the database and updates the endpoints inventory accordingly. For example, if the MAC address of an endpoint moves to a new switch port, this task associates the correct ERL to the endpoint.	
Layer 2 Scheduled Scan	Task that scans the LAN switches with SNMP and discovers the MAC addresses behind the switch ports. The task associates the discovered MAC addresses to the ERLs.	
Lync Endpoints	Microsoft Lync push task that enters endpoint data for the Lync client HELD requests.	
Lync Endpoints Cleanup	Cleanup task to remove outdated Lync endpoints that have exceeded the validity period and are not attached to an extension anymore.	This task is disabled by default and when enabled set to run at 12:00 AM everyday.
Peer Monitoring	Task that periodically updates the status of the peers in the SIP peers table. Enables the EGW to proactively send SIP 503 service unavailable error messages, in response to user agent requests to peers that are in a known down state. When sip servers (peers) are detected as being down alarms are generated (email and SNMP). For more information see section 20 "EGW Alarms."	Eg. IP-PBX server peers and ERS peers.
Queue email	Task that periodically checks the queue mail database for accumulated messages and delivers the messages asynchronously.	
Resolve domains	Task that periodically resolves the domains of internal destinations in a Microsoft Lync deployment with their IP addresses.	Reduces delays in call processing time related to the resolving of domain names.

Scheduled reports	Task that is used to periodically export provisioning parameters.	The task script can be altered to specify the parameter for the report: ERLs, endpoints, switches, subnets etc.
Statistics	Task that sends heartbeat to the ERS, along with endpoint statistics.	
Synchronization	Task that periodically checks that synchronization is maintained between the primary and secondary EGWs	
Wireless Map Cleanup	Task that periodically clears the maps that are stored through WLAN discovery according to the Map Retention Period specified in Auto Discovery → WLAN Discovery → Global.	Default setting is that the task will run every hour at the 27 th minute.
WLAN Discovery	Task that scans the wireless LAN access points to automatically track the wireless endpoints.	If controllers are not configured, then the WLAN Discovery task will not function.
Queue SNMP trap	The task executes every minute and Sends SNMP traps to the configured management station(s), if SNMP traps notification is enabled.	

10.1 Configuring the Task Scheduler Time of Day Settings

Scheduled tasks are configured in the same manner for each service listed above. To configure a scheduled task

1. Click on **Configuration → Task Scheduler**
2. Click on **Edit** under the **Actions** column for the scheduled task that you would like to configure
3. Alter the time of day settings as required.

Settings for Minutes

Table 71: Task Scheduler Configuration - Minutes

Setting Example	Description
*	The star indicates that the job is to be executed at the beginning of every minute within the hour.
0, 5, 10, 15...	The minutes at which the job is to be executed within each hour, separated by commas. e.g. Run at the beginning of the hour and every 5 minutes thereafter.
0-10	The slash (-) indicates a range of minutes delimited by the numbers to either side of the slash symbol. The job is executed for each minute of the indicated range. e.g. Run every minute for the first 10 minutes of the hour.
0,5,10, 10-20...	The comma and the slash symbol may be used together. e.g. Run at the beginning of the hour and every 5 minutes thereafter until the end of the tenth minute. At the beginning of the eleventh minute, run the job every minute until the end of the twentieth minute.

Settings for Hours

Table 72: Task Scheduler Configuration - Hours

Setting Example	Description
*	The star indicates that the job is to be executed every hour within the day.
0, 5, 10, 15...	The hours at which the job is to be executed within each day, separated by commas. e.g. Run every 5 hours until the fifteenth hour.
0-10	The slash (-) indicates a range of hours delimited by the numbers to either side of the slash symbol. The job is executed for each hour of the indicated range. e.g. Run every hour for the first 10 hours of the day.
0,5,10, 10-20...	The comma and the slash symbol may be used together. e.g. Run at the beginning of the first hour in the day and then every 5 hours until the end of the tenth hour. Thereafter, run every hour until the twentieth hour.

10.1.1.1 Run Now

The **Run Now** button can be used to immediately run any scheduled job from the Dashboard interface. The feature is useful for administrators that would like to verify provisioning results immediately, without the delay normally imposed by job scheduling.

The **Run Now** button is only available to users with Full access privileges.

To use **Run Now**:

1. Click on **Configuration>Task Scheduler**
2. Locate the task of your choice and click **Run Now**
3. When the task is complete, you can verify the results by viewing the batch results log file. The log files are available from several Dashboard screens, and can also be sent to configured email distribution lists.

For more information concerning batch results log files, see sections 11 “Emergency Response Locations (ERLs),” 12 “Endpoints,” 14 “Layer 3 Discovery,” 15 “WLAN Discovery.”

10.1.2 Scheduled Reporting

The Scheduled Reporting task can be used to periodically generate a report of provisioning data which is stored in a folder at ftp of EGW. For example, the scheduled report can be used to generate a report of endpoints: Export batch reports or on-site/off-site summary reports.

Using the EGW SOAP Server to Create a Report

You can automatically generate an endpoints report using the EGW SOAP Server. The SOAP client sends the *generateReportRequest* operation to the EGW when a report is required. In response, the endpoint report is generated and stored in the ftp folder.

For more information see “EGW SOAP Server Interface Description.”

11 Emergency Response Locations (ERLs)

11.1 Understanding Emergency Response Locations (ERLs)

An Emergency Response Location (ERL) is a location record that is provisioned into the EGW's configuration. When 911 is dialed, the EGW processes the call and retrieves the correct ERL, in order to obtain routing instructions and other policies. The ERL record is sent to the emergency responders, and appears on the call taker's screen as the location for the call. When 911 is dialed, the ERL record is sent in crisis alert emails and is displayed at security desk workstations using Desk Alert software. In order to send crisis alert email notifications, email addresses are configured per ERL during ERL provisioning.

11.1.1 Establishing Enterprise ERLs

The National Emergency Number Association (NENA) defines an ERL as "a location to which a 9-1-1 emergency response team may be dispatched. The location should be specific enough to provide a reasonable opportunity for the emergency response team to quickly locate a caller anywhere within it."

Due to the generality of the above definition, there is disagreement concerning the requirements that should apply to the size of ERLs. NENA indicates that it is generally agreed that a single ERL should be no larger than 7,000 square feet and that no more than 48 phones should be assigned per ERL. However, NENA does not go so far as to make strict recommendations.

Regulations pertaining to ERLs are administered at the state level, and vary widely from state to state. Some ordinances establish minimum square footage requirements for ERLs, while others stipulate that accurate location information should be provided for each and every telephone station.

You should develop a strategy for ERL creation which adheres to local regulations and accords with the specifics of your enterprise's deployment. In many cases, you can work with your LEC to learn about these regulations, especially in the case where you are terminating 911 calls to the local emergency network (local trunking).

11.1.2 EGW ERL Settings

ERL records in the EGW may specify location information, specific call route policies, and other settings. The following may be configured during ERL provisioning:

- Local trunking settings
- Security desk routing and emergency conferencing settings
- ELINs
- Crisis alert settings

To effectively prepare an ERL record for the EGW, Intrado recommends using the following checklist:

1. Find out the local regulations that apply to ERLs in your particular state(s).
2. Collaborate with your service provider.
3. Determine ERL-specific call route policies that will apply (e.g. local trunking, ERS, security desk call routing).
4. If local trunking is selected, procure the necessary DIDs (ELINs) that will be used to route 911 calls to the LEC's emergency network.
5. If security desk call routing is selected, determine what type of routing will be used (Direct Delivery or Call Monitor, Security Desk Dial Plan Only), and specify the name of the security desk to which the 911 calls will be routed. You should also work with your security desk personnel to determine the ERL naming strategy that will be used. The ERL information must display at security desk workstations in a format that security staff can easily understand.
6. For the Crisis Alert feature, specify the distribution list to which emails will be sent when 911 is dialed. If you include a URL link with the email, determine the additional information that will be provided for the ERL.

7. If WLAN Discovery will be enabled, determine if the APs are organized so that ERLs can be logically assigned (eg. On a floor by floor basis).

For more information concerning local trunking, see section 6 “Configuring Local Trunking (LEC Call Routing).”

For more information concerning security desk call routing, see section 5.4 “Configuring Emergency Conferencing and Security Desk Routing.”

For more information concerning crisis alert, see section 8.4 “Configuring Crisis Alerts.”

For more information concerning WLAN Discovery, see section 15.3 “Provisioning WLAN Discovery.”

11.1.3 Assigning ERLs to the Network

The first step in programming the EGW is to upload the ERL inventory and perform address error correction and resolution if necessary. Once the ERLs are provisioned, you may assign ERLs to layer 2 switches and switch ports (if you use layer 2 discovery) or WLAN Controllers. ERLs are assigned to the network using the Dashboard interface, or by batch file upload (Dashboard only). The default ERL on the switch specifies the ERL that will be assigned to all the ports on the switch, unless individual switch port ERL mappings are otherwise specified. The default ERL on the wireless controller specifies the ERL that will be assigned to all access points on the Controller, unless individual access point to ERL mapping are otherwise specified.

Note: *The Default ERL is not used if the EGW cannot retrieve the appropriate ERL for a phone when 911 is dialed. In this case, the EGW considers the phone to be unprovisioned, and sets the phone’s status to Call Center. 911 calls placed from a phone in Call Center mode will route to the ECRC.*

For more information concerning provisioning switches/switch ports and ERLs, see section 13 Layer 2 Discovery.

11.1.4 Assigning ERLs to IP subnets

Layer 3 ERLs are provisioned for enterprises that will perform automatic discovery using IP subnets. In these deployments, the EGW uses the IP address of a phone to determine the ERL when 911 is dialed. The ERL is retrieved by matching the phone’s IP address to a provisioned IP subnet and its assigned ERL.

An ERL is assigned to the layer 3 feature after it has been provisioned into the EGW configuration. The ERL can be associated to an IP subnet manually using the Dashboard interface. The Dashboard can also be used to bulk upload a file of subnet ERLs.

For more information, see section 14 “Layer 3 Discovery.”

11.1.5 ERL Maintenance

You must configure the EGW with ERL data for every area at the enterprise where employees can use their phones. For deployments where employees move their phones, the ERL configuration should include locations where phones could likely move in the future.

System administrators (telephony, network, etc.) should work together to maintain the ERL configuration and respond to problems.

For a complete list of system maintenance tasks pertaining to ERLs, see the document “EGW Appliance Standard Operating Procedures.”

11.2 Provisioning ERLs

The following list describes all of the methods that may be used to add, edit or delete ERL records to the EGW configuration:

- Dashboard GUI: add, edit, delete ERL records.
- Batch file (Dashboard or FTP): A batch file is prepared and uploaded via the Dashboard interface or to the FTP of EGW.* The file must be prepared in accordance with the batch file format. For more information, see section 11.3 “ERL Batch File Format.”

- SOAP: A web services interface may be established to upload data to the EGW following the SOAP interface specifications. SOAP interface specifications are included in the document “EGW SOAP Server Interface Specifications.”
- Remote Location Manager (RLM): An off-site user can provision an ERL using the Remote Location Manager (RLM) software (for more information about RLM, see section 17 “Provisioning Off-Campus Users.”

*The processing of ERL batch files is handled by the Task Scheduler. The scheduled tasks are set to periodically process batch files on a daily basis. You can configure the precise daily settings (hours, minutes) using the Dashboard interface.

11.2.1 Deletion Restrictions

The methods above may be used to add, delete and update ERL records. It should be noted that it is not possible to delete an ERL, if the ERL is associated to any of the following entities:

- Endpoint
- Switch
- Switch port
- Wireless controller
- Access point
- Subnet

Note: ELINs, and crisis email alerts are automatically deleted when an ERL is removed.

11.2.2 Dashboard Interface

11.2.2.1 ERL Page

The ERL page appears when you choose **Provisioning>ERLs**

Authorization Requirements:

You must have Provisioning access level privileges to access this page.

Description:

Use the ERL page to define the emergency response locations (ERLs) for your company.

Field	Description	Notes
Search bar	Enter the search terms to filter the ERLs displayed on the search page.	
Add ERL	Click Add to create a new ERL	
More Details	Click more details to see the more details screen	Same information fields are displayed when clicking on add or edit
Edit	Click edit to see the Edit screen	Same information fields are displayed when clicking on more details or Add
Delete	Click delete to delete the ERL	
ERL ID	ERL ID for the location.	
Address	Provisioned address.	
Call Delivery Type	ERS, Local Trunking, Direct Call Delivery, Security Desk Dial Plan Only.	
Is remote	Identifies the location as on-site or off-site (remote).	

	Yes/No	
--	--------	--

11.2.2.2 Add ERL Page

The Add New ERL page appears when you select **Add** on the ERLs page:

Authorization Requirements:

You must have Provisioning access level privileges to access this page.

Description:

Use the Add ERL page to create a new emergency response location (ERL). Alternatively, you can create or update many ERLs at once by importing predefined ERL information using a batch file

For more information, see section 11.2.3 “Batch File Processing.”

Table 73: ERLs Page Field Descriptions

Field	Description	Notes
ERL ID	The name of the ERL. The naming strategy you use is critical. The ERL name is one of the primary pieces of information your security team sees when alerted to an emergency call. If the name is easy to understand and very descriptive, it can help your team respond quickly to a call. For example, if you are creating an ERL for each floor in a three story building called Building J, your ERL names might be BldgJ-Floor1, BldgJ-Floor2, BldgJ-Floor3. Work with your security team to develop an ERL naming strategy.	You cannot change the name of an existing ERL. To change an ERL name delete the old ERL and create a new ERL. Any leading and trailing spaces are trimmed.
PIDF-LO location fields	Fields that are used to validate the location	<p>The fields are defined in the following locations</p> <p>US/Canada:</p> <p>See section 11.3.1 “US/Canada ERL Batch File Format.”</p> <p>Worldwide mode:</p> <p>See section 11.3.3 “Worldwide Mode Batch File Format.”</p> <p>Also, see the following document</p> <p>“EGW SOAP Interface Description.”</p>

Field	Description	Notes
Validate ERL	See section 11.2.2.2.1 “Validating ERLs.”	
Location Settings	<p>Call Delivery Type:</p> <p>ERS, Local Trunking</p> <p>Note: ERS call delivery is only available in US/Canada mode.</p>	<p>Corresponds to the following fields in batch and SOAP interfaces:</p> <p>Local gateway enabled, direct call delivery</p> <p>For more information see section US/Canada:</p> <p>See section 11.3.1 “US/Canada ERL Batch File Format.”</p> <p>Worldwide mode:</p> <p>See section 11.3.3 “Worldwide Mode Batch File Format.”</p>
	<p>Security Desk Mode</p> <p>Specifies the security desk routing setting.</p> <p>Call Monitoring:</p> <p>PSAP entirely. When call monitoring is enabled, a three-way call is routed between the security desk and the PSAP. An optional one-way mute can be configured to restrict security desk personnel from participating in the call.</p> <p>Direct Call Delivery:</p> <p>In direct call delivery, the call is sent directly to the security desk or private answering point, bypassing the PSAP entirely.</p> <p>Security Desk Dial Plan Only:</p> <p>A call to the ERL will route as an emergency call (e.g. 911) unless the dialed number is a security desk dial plan number. In this case, the call routes to an on-site security desk.</p> <p>Security Desk:</p> <p>Specifies the security desk group that will be used to route the call for the ERL.</p>	

Field	Description	Notes
	Wireless User Locator Enabled	<p>Yes/No</p> <p>Field which enables wireless location enablement services for the ERL. When enabled, the EGW will query a location server at call time, in order to build a url link to a wireless map depicting the user's location. When this field is enabled, the URL Data field below is no longer viewable, due to the dynamic nature of url link creation.</p>
	<p>URL data:</p> <p>Specify url that will link to additional information to assist emergency responders</p>	<p>The url link can contain static and dynamic variables that will point to ERL data that you would like to deliver with Desk Alert or Crisis Alert notifications. This ERL data provided in the url link can be used to integrate with other systems.</p> <p>The URL Variables can be used with this form: <code> \${variable_name}</code></p> <p>Accepted characters:</p> <p>all alphanumeric (a-z, A-Z, 0-9) and these characters: -._~:/?#@=%&+{}[]!\$'()*;,`</p> <p>To configure the url variables see section 11.2.2.3 "URL Template Editor"</p>
	<p>ELINS:</p> <p>Specify ELIN numbers. Use either static or dynamic ELIN provisioning methods.</p> <p>Note: Dynamic ELIN management not applicable to worldwide mode.</p>	<p>For more information concerning ELINS see the following sections</p> <p>US/Canada:</p> <p>See section 11.3.1 "US/Canada ERL Batch File Format."</p> <p>Worldwide mode:</p> <p>See section 11.3.3 "Worldwide Mode Batch File Format."</p>
	<p>Crisis Email Alert:</p> <p>Specify the distribution list for the people that will be notified during an emergency call.</p>	<p><i>Please note that the number of email recipients that can receive crisis alert notifications is limited to 12.</i></p>

Field	Description	Notes
Create another	Use this checkbox to create multiple ERL records one after the other.	

11.2.2.2.1 Validating ERLs

You can use the Add ERL screen to both validate and add your ERL records

To validate an ERL:

1. Enter the address information, described in the table below
2. Click **Validate ERL**.

Table 74: Location Information Fields

Field	Description
Street number (HNO) Street name (RD) Additional location information (LOC) City/Township (A3) State/Province (A1) Country ZIP/Postal Code (PC) Customer Name (NAM)	The fields are defined in the following locations US/Canada: See section 11.3.1 "US/Canada ERL Batch File Format." Also, see the following document "EGW SOAP Interface Description."

When the Validate ERL button is pressed, a request to validate the ERL is sent to the ERS. The Validation Results and Validation Details are displayed on the right side of the form.

The possible results of a validation can be:

- Success
- Success (Auto-Corrected Address)
- Success (Referred for additional MSAG validation)
- Failure (with Alternatives Addresses)
- Failure

ERS Validation Details:

The validation details are used to display additional information about the location after it has been successfully validated.

The following table provides a summary of each of the Response fields.

Table 75: Response Field Descriptions

Parameter	Description
-----------	-------------

Position Status	Indicates how much of the address was used to determine the latitude and longitude for the purposes of call routing. It will be set to either Full Address .
Civic Status	Indicates how much of the address passed civic address validation. Preferred Full Address: The full address passed validation. Full: The full address is used but some of the fields were not in the preferred form.
MSAG Status	Determines whether an MSAG-valid form of the address entered is available. An address is considered MSAG-valid if it exists in the MSAG database. The MSAG database is created by the Addressing Authority for a region. It contains the valid Address Ranges for the Streets (within the Communities, Counties, and States) in which the Addressing Authority is responsible. Found: A valid form is available. Not found: The MSAG valid form is not currently available. Referred: If an address has been geocoded using MSAG referral, the MSAG status is set to "Referred." When an address is referred for MSAG validation, it is submitted to Intrado technicians who will work to complete the MSAG validation. During this time, any emergency calls will still route the PSAP using geocoding. The PSAP displays equipment displays the address, callback number and name for the caller.
Routing Status	None: A routing strategy cannot currently be generated for a 911 call. Ten Digit (i1): The call is routed to a ten-digit PSAP administrative line. No location is automatically displayed at the PSAP. Caller will be asked to verbally confirm their location. Selective Router (i2): The call is routed via a selective router to the PSAP. The subscriber's address is automatically displayed on the PSAP dispatcher's display terminal.
Responder Type	Indicates the type of response that would first answer the 911 call. Unknown: The Responder Type cannot be currently determined. PSAP: Responder is a PSAP. Response Center: The responder is a call taker at the ECRC.

SUCCESS - Corrected Address:

It is possible that the ERS will return the following response message:
"Success - Automatically corrected address to MSAG format using GPS mapping"

In this case, the ERS corrected the address to the MSAG validation, and verified its accuracy by ensuring the GPS co-ordinates for both addresses match.

Furthermore, any fields that were auto-corrected are highlighted in green to enable easy verification of what was changed.

After verification, you can click on **Save**, to accept the auto-corrected results.

MSAG Referral Process:

If an address has been geocoded using MSAG referral, the MSAG status is set to "Referred."

When an address is referred for MSAG validation, it is submitted to Intrado technicians who will work to complete the MSAG validation. During this time, any emergency calls will still route the the PSAP using geocoding. The PSAP display equipment displays the address, callback number and name for the caller.

Note: Some PSAPs will not display the address until the MSAG process is complete.

In some scenarios, a Intrado technician may need to contact you to obtain additional information or corrections for a submitted address.

Address Alternatives:

When validating a location in the ERS, it is possible for alternatives to be returned on the EGW Dashboard.

Click **Select** for the alternative that most accurately reflects the inputted address, and the address fields are updated with the alternatives selected. Then you can click **Validate** to attempt another validation.

Note: In the case where the house number is a range (i.e. 100-122), and the value that you have entered is within that range, that value will be kept in the form after you click Select. If the house number originally entered is not within the range of the returned alternatives, the field will be cleared, prompting you for user action.

11.2.2.2.2 Adding the ERL

Once the ERL has been validated, it can be added to the ERS. The ERL must be valid before the Save button becomes available, enabling you to save the ERL in the ERS.

For more information concerning Saving ERLs and Validation, see section 11.2.2.2.1: Validating ERLs.

11.2.2.3 URL Template Editor

11.2.2.3.1 About URL Template Editor and Additional Parameters:

You can use the URL template editor to ensure that the variables that you add are correctly formatted and that the correct variable name is used. You can also use the url template editor to test that your url links are valid.

The URL template editor allows you to include both static and dynamic variables.

Static Variables:

Static parameters are derived from the data that is added to the EGW at ERL provisioning. Depending on how you configure the URL data, the parameters can be included in the url link.

Table 76: Static Variables - URL Template Editor

Parameter	Description	Variable name*
ERL ID	Erl_id	erl_id
Building number	HNO	building_number
Street name	HNO	street_name
Location	LOC	location
City	A3	city
State	A1	state
zip	PC	zip

Customer name	NAM	customer_name
Local gateway enabled	Setting made at the ERL	local_gateway_enabled
Direct call delivery	Setting made at the ERL	direct_call_delivery
Security desk id	Unique numerical value assigned to the security desk in the database.	security_desk_id
Security desk name	Setting made at the ERL	security_desk_name
Security desk extension	The security desk number that is configured at the dashboard for the security desk. Corresponds to the parameter security desk number at the dashboard.	security_desk_extension

*the variables in the urls must use the variable name exactly

Dynamic Variables:

Dynamic parameters are derived at call time. You can configure the url link with these variables so that the corresponding data value is available by clicking on the url link in the notification.

Table 77: Dynamic Variables - URL Template Editor

Parameter	Description	Variable name*
Extension	This will be the CLID received at EGW with Mask applied if configured eg. 5147454000	extension
Unmasked extension	Extension with Mask removed if (External Phone Mask is enabled. Eg. 4000)	unmasked_extension
Calling party name	Name of the caller associated to the extension.	calling_party_name
Pai	SIP URI in P-Asserted identity field that is sent to EGW at call time.	pai
Elin	ELIN number associated to the call at call time.	elin
Extension bind	Extension bind number associated to the call at call time.	extension_bind
Ip-pbx id	IP-PBX ID of the IP-PBX configured on the dashboard	ip_pbx_id
Ip-pbx name	IP-PBX ID of the IP-PBX configured on the dashboard	ip_pbx_name
Call type	Emergency, Security Desk, local trunking, test mode)	call_type
dnis	The dialed digits for the call.	dnis
Pani device ip	IP address of device that is sent to the EGW in the P-Access-Network-Info (P-ANI) SIP header at call time.	pani_device_ip

Pani tenant ip	IP address of the tenant that is sent to the EGW in the P-Access-Network-Info (P-ANI) SIP header at call time.	pani_tenant_ip
Sip entity	SIP URI in the SIP INVITE message which is delivered at call time.	sip_entity

*the variables in the urls must use the variable name exactly

Escape Strings:

It should be noted that for any data in the EGW called by a url variable, which includes any of the following characters, the resulting output will contain the applicable escape code.

For example,

`http://mysite.com?street_name=${street_name}`

would translate to:

`http://mysite.com?street_name=De%20La%20Savane`

Table 78: Characters and Their Respective Escape Codes

Character	Escape Code
SPACE	%20
<	%3C
>	%3E
#	%23
%	%25
{	%7B
}	%7D
	%7C
\	%5C
^	%5E
~	%7E
[%5B
]	%5D
`	%60
;	%3B
/	%2F
?	%3F
:	%3A
@	%40
=	%3D
&	%26
\$	%24
'	%27

11.2.2.3.2 Using the URL Template Editor

You can use the URL template to help you create valid urls

Urls should obey the following rules

Always use \${variable_name} to indicate a variable

Where *variable name* represents the exact name of the variable name that you would like to include in the Url.

Note: the variable name must be spelled exactly as documented. For more information see section 11.2.2.3.1 “About URL Template Editor and Additional Parameters.”

You can proceed the variable name with descriptive text to describe the variable. For example,

`http://mysite.com?erl_id=${erl_id}`

The accepted characters for the descriptive information can be found in the documentation of the EGW provisioning interfaces.

To create a url using the template editor

1. Navigate to the Add/Edit ERL screen on the Dashboard
2. In the parameter URL Data, provide the required address (eg.`http://abc.com`)
3. Click on Edit next to the provided address
4. Enter the descriptive text for the variable. For Static Variables and Dynamic Variables click on the variables of choice. The variable is appended directly to the url. Repeat for each required variable.
5. Click on Ok.

Testing the URL Template Editor:

You can use the test feature to verify that the information that is returned by the configured url is what was intended. The test feature also indicates if a url is invalid.

To test a url:

1. Navigate to the **Add/Edit ERL** screen
2. Enter a url and the intended variables as described above
3. Click on the Test tab. Manually enter the values for any required dynamic variables
4. Click on Test.

If the url is valid you will see the result. You can check the result to ensure that it reports the data that was intended. If the url is invalid, an error message is displayed.

11.2.3 Batch File Processing

To upload a batch file via the Dashboard interface:

1. Prepare the batch file in accordance with the batch file format (see section 11.3 “ERL Batch File Format”).
2. Click on **Provisioning > ERLs>Batch**
3. Click on the **Choose File** button to browse and upload the file.
4. Click on the **Upload** button.
5. Click **Batch Process**.

The file will start to be processed and the **Status** column will indicate *Processing*.

11.2.3.1 ERL Batch File Processing Mechanism

The batch file that was uploaded undergoes file format validation to ensure that the format is valid and can be processed by the EGW. If the file format is invalid, the EGW informs the user in the form of a Log Error File and the batch operation is terminated. For more information on this, please go to section **Error Log File**.

After ensuring the file format is valid, the batch processing mechanism proceeds to process the batch file. The file is processed one row at a time and the operation specified in the batch file is executed.

If there is an issue validating an address, only that specific address is not provisioned. The remaining ERLs found in the batch file are added to the EGW.

The ERL(s) that could not be provisioned (or updated/ deleted), will be recorded, along with the reason for the failure in the error log file.

11.2.4 FTP

To batch upload via FTP

1. Open an FTP connection to the EGW using the IP of the EGW, username: batcher1, password: 911batch.
2. Go to **batch** directory.
3. Upload the file to the EGW.

Batch files uploaded to the EGW using FTP are governed by scheduled tasks settings. The scheduled tasks dictate precise daily intervals at which batch processing will occur. To configure scheduled tasks, see section 10 Task Scheduler



Note: After a batch file uploaded to the EGW via FTP is processed, it is automatically removed from the FTP directory. These files can be viewed using the Dashboard interface.

FTP Batch Results

The batch logs summary and error reports are sent to the email addresses configured at **Configuration>Advanced>Batch Settings**. Logs can also be viewed from the Dashboard.

11.2.5 SOAP interface

To provision ERLs using the SOAP interface

1. Click on **Configuration > Advanced > SOAP Server**.
2. Enable SOAP server locations.
3. Enter your SOAP username and password.
4. Send function calls to the IP of your EGW in accordance with the SOAP server documentation.

To send SOAP provisioning requests to the EGW SOAP server in the correct format, see the document “EGW SOAP Server Interface Description.”

11.3 ERL Batch File Format

The batch file format is used to process multiple ERL records using the Dashboard or ftp. Each line in the file describes an ERL with its provisioning parameters. The ERL batch file format uses CSV files.

The ERL batch file format has been designed to support the PIDF-LO location format. PIDF-LO is a standards-based format for storing location data, which provides support for international character set encodings, variable length dialing plans, and various emergency numbers.



Note: The CSV batch file format applies to both US/Canada, and Worldwide modes of operation. The EGW legacy batch file format (.txt) may still be used by customers in US/Canada. For more information, see Appendix A.

11.3.1 US/Canada ERL Batch File Format

In US/Canada operation, the batch file format uses CSV files.

The first record in the CSV file is a header record containing column (field) names. This header record specifies which fields will be included in the file and the order in which they occur.



Note: Only the required fields are mandatory, and you can use the header record to specify the order in which the fields will occur in the batch file.

Note: The dash symbol (-) is not permitted. However, the underscore symbol (_) is permitted.

- 1 character min
- 31 characters max
- a-z,A-Z,0-9,_(commas not part of the list)

Table 79: Batch File Format

Header Name	Description and possible values (if the same for all countries)	Format Supported	Req?
operation	Value: 1 = Add or update 2 = Delete		Y
erl_id	Unique identifier of the location. Alphanumeric between 1 and 31 characters in length.	<ul style="list-style-type: none"> • 1 character min • 31 characters max • a-z,A-Z,0-9,_(commas not part of the list) 	Y
HNO	House number, numeric part only. Street number or Building number. Example 800, 600, 3891	<ul style="list-style-type: none"> • 10 characters. max. • ([a-zA-Z]\s\d\.\\'\(\'),\V#-\]{1,10}) 	Y
HNS	House number suffix. Example: 12, a, 2134	<ul style="list-style-type: none"> • 5 characters. max • ([a-zA-Z]\d]{1,5}) 	N
PRD	Prefix Directional. Leading street direction. Example: W, SE, N, NE	<ul style="list-style-type: none"> • 2 characters max. • ((ne) (nw) (se) (sw) (n) (e) (s) (w) (NE) (NW)) 	N

Header Name	Description and possible values (if the same for all countries)	Format Supported	Req?
) (SE) (SW) (N) (E) (S) (W))	
RD	Primary road or street. Street name. Example: Sunset, Magnolias, 44	<ul style="list-style-type: none"> • 48 characters max. • (\x{a1}-\x{01ff}\w\s\d\.\'(\'),\V#-]{1,48}) 	Y
STS	Street suffix. Example: ST, BLVD, HWY	<ul style="list-style-type: none"> • 10 characters max. • ([a-zA-Z]{1,10}) 	N
POD	Post Directional. Trailing street suffix. Example: W, SE, N, NE.	<ul style="list-style-type: none"> • 2 characters max. • ((ne) (nw) (se) (sw) (n) (e) (s) (w) (NE) (NW) (SE) (SW) (N) (E) (S) (W)) 	N
LOC	More precise information about the location. Alphanumeric between 1 and 20 characters. Ex.: Suite 200, Floor 2, Unit 341.	<ul style="list-style-type: none"> • 20 characters max. • /^(\x{a1}-\x{01ff}\w\s\d\.\'(\'),\V#-]{1,20})\$/u 	N
A3	City, township, shi (JP) Example: New York, Los Angeles, Chicago.	<ul style="list-style-type: none"> • 32 characters max. • ([a-zA-Z\s\d\.\'(\'),\V#-]{1,32}) 	Y
A1	The state or province or county of the location. Some countries require it to be the Abbreviated state name (2 letters) while others require it to be the full name. The validation is Country specific.	<ul style="list-style-type: none"> • 2 characters max • ([A-Z]{2,2}) 	Y
Country	The ISO 3166 alpha-2. Ex.: US, CA. United States, Canada.	<ul style="list-style-type: none"> • 2 characters min • 3 characters max • ([A-Z]{2,3}) 	Y
PC	Postal Code for most countries and the zip code for the United States. Validation is based on the Country specifications. Example: 10044, H4P 2R9	US <ul style="list-style-type: none"> • (((0-9){5,5}) ([0-9]{5,5}-[0-9]{4,4})) CA <ul style="list-style-type: none"> • ([ABCEGHJ-NPRSTVXY][0-9][ABCEGHJ-NPRSTV-Z]()[0-9][ABCEGHJ-NPRSTV-Z][0-9]\$) 	Y
NAM	The name of the customer. This field will appear on the PSAP screen as the "Name". Between 1 and 60 characters.	<ul style="list-style-type: none"> • 60 character max. 	N*

Header Name	Description and possible values (if the same for all countries)	Format Supported	Req?
	Note: Due to PSAP display limitations, an error may be returned for any values submitted that are longer than 32 characters. It is a best practice to provision the NAM field between 1-32 characters.	<ul style="list-style-type: none"> /^([x{a1}-x{01ff}\w\s\d\.\\"(\()\.\#\-\]{1,60})\$/u 	For ERS 3.x this field is mandatory
Local_trunking	Defines if the location will be going through a local trunk or not. Values: 1 = Yes 0 = No If not defined, default is 0.		N
direct_call_delivery (security desk call route setting)	Setting which determines call routing for the security desk route. 0 = Call Monitoring 1 = Direct Call Delivery 2 = Security Desk Dial Plan Only When set to 0, default setting of Call Monitoring will be used, if a security desk is configured at the Dashboard. The security desk is referenced by the Security Desk Name (Position 14) specified for the ERL record. When set to 1, security desk call routing feature will use Direct Delivery. If 2 is set, the security desk feature will only apply to calls made to a security desk dial plan number (e.g. 511, 888). If the ERL setting is 2, and a security desk number is dialed, the call will route as a direct delivery call to the on-site security desk. With this configuration, a call from the same ERL to the emergency number (e.g. 911) will not route to the security desk.		N
Elin	ELINs. Must be 10 digit numbers for US and CA. ELINs may be defined statically or dynamically. Static assignment To statically assign ELINs (one or multiple), enter the ELIN numbers (must be 10 digit numbers and comma delimited). e.g. 1000000000,333333333,2323232323.		N

Header Name	Description and possible values (if the same for all countries)	Format Supported	Req?
	<p>Dynamic assignment (ERS call delivery only) Add the amount of ELINs, enclosed in parentheses, which you would like the EGW to assign to this ERL. The EGW will select available ELINs from the ELIN pool based on this number. For example, [1],[2],[3] An error will be generated if the ELIN pool has been exhausted.</p> <p> Note: Dynamic ELIN management should be reserved for enterprises with on-site security P-ALI databases, or for enterprises that use local trunking to route all 911 calls within a single PSAP jurisdiction.</p> <p>Multiple ERLs per ELIN It is possible to assign multiple ERLs to the same ELIN number. However, you are not able to assign a dynamic ELIN from the ELIN pool to more than one ERL. A dynamic ELIN can only be assigned to one ERL at a time.</p>		
security_desk	The name identifier of the security desk (if applicable). Letters and underscores.		N
crisis_email	Distribution list which will receive an email when 911 is dialed from the ERL. Comma delimited for multiple entries. e.g. john@enterpriseabc.com, jane@enterpriseabc.com. Hanging commas at the end of the crisis email alert list are not accepted.		N
url_data	<p>The url link can contain static and dynamic variables that will point to ERL data that you would like to deliver with Desk Alert or Crisis Alert notifications. This ERL data provided in the url link can be used to integrate with other systems.</p> <p>The URL Variables can be used with this form: \${variable_name}</p> <p>Accepted characters: all alphanumeric (a-z, A-Z, 0-9) and these characters: .~/?#@=%+&</p>		N

Header Name	Description and possible values (if the same for all countries)	Format Supported	Req?

Note: For the delete operation, it is only mandatory to specify the ERL ID. All other fields may be left empty.

Batch file Examples

The first row in the CSV file is a header record containing column (field) names. This header record specifies which fields will be included in the file and the order in which they occur.

```
OPERATION,ERL_ID,HNO,RD,STS,LOC,A3,A1,COUNTRY,PC,NAM,DIRECT_CALL_DELIVERY,SECURITY_DESK,URL_DATA
```

```
1,LOC123,123,Main,ST,Empire State Building,New
York,NY,US,10044,West,1,Main,http://maps.google.com?ERLID=${erl_id}
```

```
"OPERATION","ERL_ID","HNO","RD","STS","LOC","A3","A1","COUNTRY","PC","NAM","DIRECT_CALL_DELIVERY","SECURITY_DESK","URL_DATA"
```

```
"1","LOC123","123","Main","ST","Empire State Building","New
York","NY","US","10044","West","1","Main","http://maps.google.com?ERLID=${erl_id}&BuildingNumber=${building_number}"
```

```
"OPERATION","ERL_ID","HNO","RD","STS","LOC","A3","A1","COUNTRY","PC","NAM","DIRECT_CALL_DELIVERY","SECURITY_DESK","URL_DATA"
```

```
"1","LOC123","123","Main","ST","Empire State Building","New
York","NY","US","10044","West","1","Main","http://my-site-
datafeed.google.com/feed.php?extension=${extension}&cpn=${calling_party_name}"
```

11.3.2 Dynamic ELIN Management

The ERL batch file format can be used to dynamically assign ELINs to ERL records. There are a variety of operations that can be performed to add and remove ELINs from the ERL configuration. For example, the entry below would dynamically assign one ELIN to the ERL record.

```
"Operation","ERL_ID", "HNO", "RD", "LOC", "A3", "Country", "PC", "NAM", "Local_Trunking", "Direct_Call_Delivery",
"ELIN"
"1", "LOC123", "123", "Main", "New York", "US", "10044", "Company X", "1", "1", [1]
```



Note: Dynamic ELIN management should be reserved for enterprises with on-site security P-ALI databases, or for enterprises that use local trunking to route all 911 calls within a single PSAP jurisdiction. This feature is not applicable for call delivery via the ERS. You are not permitted to provision a dynamic ELIN pool number to more than one ERL at a time.

11.3.2.1 Dynamic ELIN Management Example

The following sequence illustrates all possible ELIN management operations. It describes the outcome for the indicated values of the ELIN field:

[1]

- The EGW dynamically assigns one free ELIN to the ERL record.

[2]

- One ELIN is already assigned to this ERL. An additional ELIN is assigned, for a total of two ELINS.

[1]

- Two ELINs were previously assigned to the ERL. This operation releases one ELIN.

5146661111

- The dynamic ELIN is released from the ERL. The specified ELIN is statically assigned to the ERL.

0

- All ELINs are removed from the ERL record.

3333333333

- The number specified is a dynamic ELIN. It is bound to the ERL record, but remains dynamic.

11.3.3 Worldwide Mode Batch File Format

In Worldwide operation, the batch file format uses CSV files.

The first record in the CSV file should be a header record containing column (field) names. This header record specifies which fields will be included in the file and the order in which they occur.



Note: All column (field) names containing non-ASCII characters must be enclosed by double quotes (eg. "Zürich"). Preferable, all fields are enclosed by double quotes.



Important: The required fields indicate what fields are required for all Worldwide Mode countries. Country-specific field validation requirements are provided in Appendix B for each worldwide mode country supported by the EGW. Consult the appendix for your specific country. For more information, see section 23.2 "Country Specific Validation Requirements."

Table 80: Batch File Format - World Wide Mode

Header Name	Description and possible values (if the same for all countries)	Req?
operation	Value: 1 = Add or update 2 = Delete	Y
erl_id	Unique identifier of the location. Alphanumeric between 1 and 31 characters in length.	Y
HNO	House number, numeric part only.	N
HNS	House number suffix	N
BLD	Building (structure)	N
PRD	Leading street direction	N
RD	Primary road or street	N
STS	Street suffix	N
POD	Trailing street suffix	N
RDSEC	Road section	N
RDBR	Road branch	N
RDSUBBR	Road sub-branch	N
PRM	Road pre-modifier	N
POM	Road post-modifier	N
LMK	Landmark or vanity address	N
LOC	More precise information about the location. Alphanumeric between 1 and 60 characters. Ex.: Suite 200, Floor 2, Unit 341.	N
FLR	Floor	N
UNIT	Unit (apartment, suite)	N
ROOM	Room	N
PLC	Place-type	N
ADDCODE	Additional code	N
SEAT	Seat (desk, cubicle, workstation)	N
A2	County, parish, gun (JP), district (IN)	N
A3	City, township, shi (JP)	N
A4	City division, borough, city district, ward, chou (JP)	N
A5	Neighborhood, block	N
PCN	Postal community name	N
A1	The state or province or county of the location. Some countries require it to be the Abbreviated state name (2 letters) while others require it to be the full name. The validation is Country specific.	N
country	The ISO 3166 alpha-2. Ex.: US, CA, FR, GB or GBR	Y
PC	Postal Code for most countries and the zip code for the United States. Validation is based on the Country specifications.	N
POBOX	Post office box	N
NAM	The name of the customer. This field will appear on the PSAP screen as the "Name". Between 1 and 60 characters.	N
local_gateway_enabled	Defines if the location will be going through a local trunk or not. Values: 1 = Yes 0 = No If not defined, default is 0.	N
	 Note: For Worldwide mode, either local trunking or direct delivery must be enabled.	

direct_call_delivery	Determines if a call made using this location will be directed to a security desk or not. Setting this field to 1 removes data from 911enable. 1 = Yes. 0 = No. If not defined, default is 0.  Note: For Worldwide mode, either local trunking or direct delivery setting must be enabled.	N
elin	ELINs for the ERL. Can be between 3 and 15 digits for other countries. Ex.: 1000000000,3333333333,2323232323.  Note: Dynamic ELIN feature is not applicable to Worldwide mode.	N
security_desk	The name identifier of the security desk (if any). Letters and underscores.	N
crisis_email	Distribution list which will receive an email when 911 is dialed from the ERL. Comma delimited for multiple entries. e.g. john@enterpriseabc.com, jane@enterpriseabc.com.	N
url_data	Information that will appear in the Crisis Alert Email. e.g. URL or database query. The url link can contain static and dynamic variables that will point to ERL data that you would like to deliver with Desk Alert or Crisis Alert notifications. This ERL data provided in the url link can be used to integrate with other systems. The URL Variables can be used with this form: \${variable_name} Accepted characters: all alphanumeric (a-z, A-Z, 0-9) and these characters: .~/?#@=%+&	N

Batch file Examples

The first record in the CSV file should be a header record containing column (field) names. This header record specifies which fields will be included in the file and the order in which they occur.

“Operation”,“ERL ID”,“HNO”,“RD”,“A4”,“A3”,“PC”,“Local_Trunking”
“1”,“Loc1”,“1”,“Upper Littleton”,“Winford”,“Bristol”,“BS188HF”.

- The batch file is adding the ERL LOC1
- Local Trunking is enabled

11.3.4 ERL Batch Logs

Batch log files report on the success or failure of each entry in a submitted batch file. The batch logs are generated in response to the following actions:

- Batch Process

To view the batch logs

- Click on **Provisioning > ERLs > Batch Logs**

The columns of the log display the following information:

- Original File Name
- Log file
- Error Log File
- Log date
- Status
- Batch Process or Delete

*These actions apply to uploading an ERL batch file using the Dashboard interface. For more information, see section 11.2.2 “Dashboard Interface.”

11.3.4.1 Log File

To view a log file, click on **View Log File** under **Log File**.

The log file provides a status report for each line of the processed batch file. A line will contain an error code followed by a description, and then the original line in the batch file. If the operation was executed successfully, the error code will be set to 00. If the operation failed to complete successfully, the error code will be larger than 00.

11.3.4.2 Error Log File

To view a log file, click on **View Log File** under **Log File**.

This log file will only be generated when there is an error processing the batch file. It provides the result of the file format validation as well as the results of the address validation.

When the batch file format is invalid, the **Output** and the **Message** column will populate to indicate that the CSV file format was invalid and the batch file has not been processed.

When ERL(s) could not be validated, the list of the ERLs that did not pass address validation will be recorded in this file with the appropriate code and the description.

11.3.5 ERL Batch Results

The following table details each possible outcome resulting from a single operation.

Table 81: Batch Log Response Codes

Response Code #	Description	Add / Update	Delete
00	SUCCESS_ Entry is successful.	X	X
01	INVALID_ROW_NUMBER_ Entry does not include the correct number of row.	X	X
02	INVALID_OPERATION_ Operation entered is invalid.	X	X
03	INVALID_ERL_ID_ Format of the ERL ID is invalid.	X	X
04	INVALID_BUILDING_NUMBER_ Format of the building number is invalid.	X	
05	INVALID_STREET_NAME_ Format of the street name is invalid.	X	
06	INVALID_ADDRESS_TYPE_		
07	INVALID_CITY_NAME_ Format of the city is invalid.	X	
8	INVALID_STATE_ABBR_		
09	INVALID_COUNTRY_ Format of the country is invalid.	X	
10	INVALID_ZIP_CODE_ Format of the zip code/postal code is invalid.	X	
11	INVALID_LCL_GW a) Local gateway enabled setting is invalid. b) An ELIN must be present in order to use this setting.	X	
12	INVALID_CALL_DELI_ a) Direct call delivery setting is invalid. b) A valid security desk name is required in order to use this setting.	X	

Response Code #	Description	Add / Update	Delete
13	INVALID_CUST_NAME_ Format of the customer name is invalid.	X	
14	INVALID_ELIN_NUMS_ One of the ELIN numbers entered is invalid.	X	
15	INVALID_SEC_DESK_ Security desk name entered does not exist.	X	
17	INVALID_CRISIS_EMAIL_ One of the crisis emails is invalid.	X	
18	ADDRESS_ALREADY_EXISTS_ Address entered already exists.	X	
19	INVALID_LOCATION_ ERL ID entered is invalid.		X
21	ADDRESS_FAILED_ Address failed validation.	X	
22	SUBNET_ALREADY_EXISTS One of the subnets entered is already assigned to another ERL ID.	X	
23	ENDPOINT_ALREADY_EXIST Endpoints assigned to the ERL ID entered.		X
24	ELIN_ALREADY_EXISTS_ One of the ELIN numbers is already set to another ERL ID, or is an existing Extension-Bind number.	X	
25	CONFLICT_DD_LCL_GW Direct call delivery and local gateway cannot be enabled at the same time.	X	
26	SOAP_FAULT_ An error occurred during the SOAP call.	X	X

Response Code #	Description	Add / Update	Delete
27	ACC_TYPE_LCL_NO_ALLOWED License key is invalid for local trunking.	X	
28	ACC_TYPE_LCL_ONLY License key is only valid for local trunking.	X	
29	SWITCH_USING_ERL_ Cannot delete ERL because a switch is assigned.		X
30	SWITCH_PORT_USING_ERL_ Cannot delete ERL because a switch port is assigned.		X
31	INVALID_URL_DATA_ "URL data contains invalid characters."	X	
32	CAN_NOT_ALLOWED_ You do not have support for Canadian addresses enabled.	X	
33	CAN_REQ_ELINS_ At least one ELIN must be assigned to each Canadian address.	X	
34	INVALID_LICENSE_KEY_ Invalid license key. Either the license key is not defined or it is in the wrong format.	X	
35	ELIN_POOL_EXHAUSTED_ ELIN pool is exhausted or dynamic ELIN pool is empty.	X	
36	DYNAMIC_ELIN_ALREADY_EXISTS One of the ELINs that you tried to assign to the ERL is in the dynamic ELIN pool. Dynamic ELINs cannot be assigned to more than one ERL at a time.		
	Dynamic_elin_not_allowed The EGW is currently not configured for use with the dynamic ELIN feature.		

Response Code #	Description	Add / Update	Delete
37	WLAN_USING_ERL_ Cannot delete ERL because a WLAN controller is assigned.		X
38	ACCESS_POINT_USING_ERL_ Cannot delete ERL because an access point is assigned.		X
39	INVALID_FILE_TYPE_ Supported file extension for worldwide mode is only .csv (PIDF-LO)		
40	INVALID_CSV_HEADER_ Invalid CSV Header. The following CSV header is not valid:		
41	MISSING_CSV_HEADER_ Missing CSV Header. The following CSV header is missing:		
42	No batch has been processed, check your csv file format		
43	INVALID_ACC_WW_ Invalid account for this server. The current mode of EGW Operation (International) only supports local trunking or direct call delivery.		
44	UNSUPPORTED_FIELD_USED_ Unsupported Field Used. The following field does not support the Country of operation.		
45	SECURITY_DESK_SET_DESK_ALERT_ONLY Direct call delivery setting not applicable. The specified security desk is set to Desk Alert Only.		
46	DUPLICATE_CSV_HEADER_ Duplicate CSV header. The following CSV header is a duplicate of another CSV header:		
49	Invalid url variable		

Response Code #	Description	Add / Update	Delete
51	The specified civic address already exists in location <ERL ID>		

Batch File Example

The batch file results returned in the log file are displayed in CSV format. The results include an error code and description followed by the original line in the batch file entry:

“error_code”, “error_description”, “Operation”, “ERL ID”, “HNO”,
“RD”, “LOC”, “A3”, “Country”, “PC”, “NAM”, “Security_Desk”, “Local_Trunking”, “Direct_Call_Delivery”, “ELIN”

“Error code”, “error description”, “Operation”, “ERL ID”, “HNO”, “RD”, “A4”, “A3”, “PC”, “Local Trunking”

“00”, “success”, “1”, “Loc1”, “1”, “Upper Littleton”, “Winford”, “Bristol”, “BS188HF”.

“03”, “Format of the ERL ID is invalid”, “1”, “Loc1”, “1”, “Upper Littleton”, “Winford”, “Bristol”, “BS188HF”.

View Peer

If **Log File** displays **View Peer**, you must login to the Peer in order to view the log file. This scenario occurs when a batch file is processed by the Peer machine.

11.4 Exporting/Backing Up ERLs

Use the Export ERL page to create ERL export files for your own use, for example, to back up or move an ERL configuration. ERLs are exported from the EGW by generating an ERL report. The report is a semicolon delimited batch file that can be re-imported using the Dashboard.

To generate an ERL report

- Click on **System Status > Reports** and select ERLs as report type.

For more information see section 18.4 “Reports.”

12 Endpoints

12.1 Understanding Endpoints

The EGW supports automatic discovery and tracking for a variety of IP phones and softphones using different methods:

12.1.1 Phone Discovery

Vendor Proprietary Methods (eg. Cisco, Avaya):

The EGW interoperates with vendor technologies to discover the inventory of IP endpoints.

Automatic Phone Inventory:

For deployments using Layer 2 Discovery, the EGW supports automatic phone inventory discovery using the layer 2 networking identifiers of the endpoints (eg. MAC address). On a per IP-PBX basis, endpoint MAC address phone masks are configured at the EGW. If an endpoint is found in a layer 2 scan falling within the mask range it is added to the endpoints inventory at the EGW and assigned to the corresponding switch port and ERL.

For more information see section 12 Endpoints.

E911 Softphone Locator (ESL):

Certain IP softphones (e.g. Microsoft Office Communicator, Avaya) are supported by the E911 Softphone Locator (ESL), a Windows-based service. This enables these softphones to be automatically tracked using layer 2/3 Discovery and/or WLAN Discovery.

Manually Configured Phones:

The EGW can be manually configured with various analog and digital phones using the Dashboard interface. It is also possible to bulk load manually configured phones in a batch file or using the SOAP interface.

It is also possible to automate how these phones are added by using existing enterprise databases, such as a telephone directory or an on-site asset management tool (network management software).

For more information, see section 2.2 “Emergency Gateway Specifications.”

12.1.2 Phone Tracking

Once the phone inventory has been discovered, the EGW tries to associate the phones to emergency response locations (ERLs). If Layer 2 Discovery is used, the EGW tries to associate the phones to their attached switch ports. By discovering the phones and their attached layer 2 switch ports, the EGW can track a phone when it moves, and assign an ERL to a phone when an emergency call is made.

If a phone is tracked using layer 3 discovery, the EGW uses the ERL assigned to the phone’s IP subnet to identify its location.

In wireless deployments, endpoints can be discovered using WLAN scanning (SNMP), or by using the E911 Softphone Locator (ESL). Regardless of what method is employed, the EGW will attempt to use the wireless phone’s current BSSID in order to determine the location. When WLAN Discovery is enabled, the EGW can seamlessly track phones that move between wired and wireless modes of operation: If a phone is in wireless mode, it can be picked up by the next WLAN scan, or ESL push. If it is in wired mode, it can be tracked using layer 2/3 discovery.

In addition, a combination of Layer 2 and Layer 3 can also be used

For more information about WLAN scanning, see section 15 “WLAN Discovery.”

12.1.3 Unprovisioned Phones (Call Center Mode)

Phones in the EGW configuration can have a status of Provisioned or Unprovisioned. A provisioned phone is assigned to a valid ERL. An unprovisioned phone, on the other hand, is not assigned to an ERL in the EGW. Unprovisioned phones display a status of Call Center Mode. When an unprovisioned phone dials 911, the call is routed to the 24/7/365 Emergency Call Response Center (ECRC).

A phone is put into unprovisioned mode under the following circumstances:

- The phone could not be assigned to an ERL by layer 2 or layer 3 discovery
- A phone was not added to the configuration manually (batch, soap, on-site/off-site RLM)
- A phone was intentionally set to unprovisioned mode using manual methods (eg. Off-site user sets their phone to Response Center)



Note: For Cisco deployments that use layer 3 discovery, endpoints will display as unprovisioned in the web Dashboard. However, the phones are provisioned when 911 is dialed: the EGW uses the IP address of the phone to obtain routing instructions.

12.2 Provisioning Endpoints

Multiple endpoint records may be uploaded to the EGW simultaneously using one of three methods:

- **Dashboard interface:** Add, edit and delete endpoint records.
- **Batch files:** A batch file is uploaded using the EGW web interface. The file may be validated and processed in real-time.
- **FTP:** The batch file is uploaded to the EGW FTP server. The file is validated/processed during the next scheduled task interval.
- **SOAP interface:** A web services interface can be established to upload data to the EGW following the WSDL specifications. The data is validated in real-time.

12.2.1 Dashboard

12.2.1.1 Endpoints Page

The Endpoints page appears when you choose **Provisioning>Endpoints**.

Authorization Requirements:

You must have Provisioning access level privileges to access this page.

Description:

Use the Endpoints page to locate and view phones that you would like to modify or delete. You can also navigate to add new phones from this page.

Table 82: Endpoints Screen Field Descriptions

Field	Description
Search endpoints	Enter search criteria to select the manually configured phones you want to find. To find all manually configured phones, click Find without entering any criteria.
Endpoints Search results	Displays the search results. For each phone found, the system displays the extension, device name, MAC address, PBX name, IP address, ERL ID. Click the Edit icon to view and modify the information for that phone. You can change any of the fields.

Extension	Extension associated to the endpoint.
Device Name	Device name associated to the endpoint.
MAC Address	MAC address associated to the endpoint.
PBX Name	PBX name associated to the endpoint.
IP Address	IP Address associated to the endpoint.
ERL ID	ERL ID associated to the endpoint.
Found By	Mechanism or parameter used to assign the ERL ID to the endpoint. Possible values: Remote, Static parameter (MAC, Device name, etc), Layer 3, etc
IsRemote	Indicates whether the endpoint is remote.
Last Modified	Date and time the endpoint was last modified.
Actions	<p>The options are available:</p> <ul style="list-style-type: none"> • ERL Details: Click here to view the ERL Information associated to the endpoint. • Edit**: Click here to change the IP Address and/or the ERL ID associated to the endpoint. <i>(Note: If the ERL ID was assigned by Layer 3 Discovery, it will be greyed out and will be displayed with <ERL ID>**)</i> • Delete: Click here to delete the endpoint.
Edit**	<p>Click edit to change the following parameters for the endpoint:</p> <ul style="list-style-type: none"> • IP Address • ERL ID <p>If the ERL ID was assigned by Layer 3 Discovery, it will be greyed out and will be displayed with <ERL ID>**</p>
Delete	Click to delete the endpoint.

**Editing the endpoint

To edit the endpoint:

1. Choose the endpoint row you want to edit.
2. Click on the **Edit** button.

If the IP address was discovered by Layer 3 discovery, then the ERL ID will be displayed as <ERLID> (grayed out).

When you hover upon the ERL ID, the tooltip displays “Layer 3 Discovery returned an ERL ID. Edit this field to statically assign a different ERL ID”.

When this ERL ID is changed manually, a dialog box is displayed with the following message:

“This operation will statically assign an ERL_ID to this endpoint if it conflicts with Layer 3 Discovery. Are you sure you want to update this endpoint?”

Please note that changing the ERL ID using the above mentioned method will make the endpoint to become statically provisioned and Layer 3 discovery process will no longer detect this endpoint.

Add New Manual Endpoint

To manually add an endpoint, choose **Endpoints>Endpoints>Add**. Click the **Add** link. A new row appears in the **Endpoints Search Results** and the fields are available for editing.

Table 83: Endpoints Screen Field Descriptions

Field	Description
Extension	Extension of the phone
Device name	Device name of the phone, if applicable
MAC address	MAC address of the phone, if it is an IP phone.
PBX name	Name of the associated PBX system.
IP address	IP address of the phone, if it is an IP phone.
ERL ID	Emergency response location to associate with the phone.

12.2.2 Batch Files

To upload a batch file via the Dashboard interface

1. Prepare the batch file in accordance with the batch file format (see section 12.2.5 “Endpoint Batch File Format”).
2. Click on **Provisioning > Endpoints.>Batch**.
3. Click on the **Choose File** button and locate the batch file for upload.
4. Click on the **Upload** button to upload the batch file.

Now the **Actions** columns under the Batch Logs section become populated with the following action buttons:

- **Batch Process:** Clicking on this button will proceed to provision the endpoint batch file.
- **Delete:** Clicking on this button will delete the endpoint batch file that you just uploaded.

12.2.2.1 Endpoint Batch File Processing Mechanism

The batch process mechanism processes the endpoint batch file one line at a time and executes the operation as specified in the batch file. The batch file is read and processed completely even if an error is detected.

If any errors are detected, the erroneous line is detected and captured in the **Log Error File**. For more information on the **Log Error File**, please go to section 12.2.6.2Log Error File.

Automatic Batch Logs

Endpoint batch log file generation is customizable using the Dashboard interface. Endpoint batch log files are generated under the following circumstances:

- A batch file is processed via the Dashboard interface
- A batch file in the ftp folder is processed
- A scheduled task generates a batch file automatically (e.g. Layer 2 discovery, Avaya Push, Cisco AXL)

By default, batch logs that are automatically generated by certain scheduled tasks (layer 2 Discovery, Avaya Push, and Cisco AXL) are disabled. However, it is possible to enable these logs using the Dashboard

To enable automatic Endpoint batch logs

1. Click on **Provisioning > Endpoints**
2. Check the **Display Automatic** checkbox under **Batch Logs**

Once this configuration is made, any future scheduled tasks that generate Endpoint batch files will result in log files being populated in the Endpoints batch logs screen.

12.2.3 FTP

To batch upload via ftp

1. Open an ftp connection to the EGW using the IP of the EGW, username: batchendpoint, password: 911batch.
2. Go to **batch** directory.
3. Upload the file to the EGW.

Batch files uploaded to the EGW using FTP are governed by the scheduled tasks settings. The scheduled tasks dictate precise intervals at which batch processing will occur.



Note: After a batch file uploaded to the EGW via FTP is processed, it is automatically removed from the FTP directory. These files can be viewed using the Dashboard interface.

FTP Batch results

The batch logs summary and error reports are sent to the email addresses configured at **Configuration > Advanced > Batch Settings**. Logs can also be viewed from the Dashboard.

12.2.4 SOAP

To provision endpoints using the SOAP interface

1. Click on **Configuration > Advanced > SOAP Server**.
2. Enable SOAP server endpoints.
3. Enter your SOAP username and password.
4. Send function calls to the IP of your EGW in accordance with the SOAP server documentation.

To send SOAP provisioning requests to the EGW SOAP server in the correct format, see the document “SOAP Server Interface Description.”

12.2.5 Endpoint Batch File Format

Each line in the batch file describes an endpoint with its provisioning parameters. The parameters are entered as fields in a semicolon delimited file format.

Full or Incremental Discovery Cycle

The endpoint batch processing module can use a Full or Incremental discovery cycle. Using the incremental setting, the batch file will only add/overwrite data to the EGW for the specific endpoints in the batch file. When using the full discovery cycle, the status of endpoints not included in the batch file is changed to Call Center Mode (Unprovisioned). To delete these endpoints from the database, it is necessary to upload a batch file that performs the Delete operation, or to delete the endpoint using the Dashboard interface.



Note: The full batch processing discovery cycle is preferred for enterprises that have on-site asset management tools (network management software).

The following table describes each of these fields in detail.

Table 84: Fields for Batch Provisioning Endpoints

Position	Field Name	Description	Req?
1	Operation	<p>In Incremental Mode</p> <p>Value:</p> <ul style="list-style-type: none"> • 1 = Add or update* • 2 = Delete* <p>For automatic FTP provisioning, value must be 1.</p> <p>For the delete operation, send the Operation, IP-PBX ID, Extension, or MAC address fields. For ShoreTel and Cisco endpoints, Device Name is also accepted. **</p>	Y
2	IP-PBX name	The name of the PBX to which the endpoints will be assigned.	Y
3	Extension	<p>The extension of the phone.</p> <p>Alphanumeric up to 50 characters.</p> <p>(a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), , pound(#), dash(-), underscore(_), at sign (@).</p> <p>Note: The extension provisioned in the EGW must be the extension that will be output by the phone system post PBX digit manipulation (eg. Digits appended/deleted, prefixes etc.).</p>	<p>Conditional (either extension, MAC or device name must be present)</p> <p>Extension can also now accept Lync username for users of Microsoft Lync Server 2013.</p>
4	MAC address	<p>The MAC address of the phone.</p> <p>Hexadecimal and must be 12 characters in length e.g. AB02FC91AC0F</p>	<p>Conditional (either extension, MAC or device name must be present)</p>

Position	Field Name	Description	Req?
5	ERL ID	The ERL ID to which the endpoints are assigned. If left blank, the Endpoint's Status will not change. If set to <ECRC>, the endpoint is assigned to Call Center mode.	N
6	IP address	The current IP address of the phone (if available). Must be IPv4.	N
7	Display name	The display name of the phone (if available).	N
8	Timestamp	The UNIX timestamp representing the time at which the endpoint values were discovered. The timestamp is a recommended field for enterprises that have deployed automated asset management tools in conjunction with the Remote Location Manager (real-time interface for remote users). In this scenario, the time at which the batch file is processed may be later than the last user generated real-time update. To account for this, the timestamp ensures that the RLM file will not be overwritten. Time must be in UNIX format e.g. 1208791332 represents April 21 2008 15:22:12.	N
9	Device Name	The device name of the phone. eg. CSFJohnDoe. Alphanumeric up to 50 characters and supports underscore (_), dash (-), or dot (.)	Conditional (either extension, MAC or device name must be present)

***It is not possible to update and delete the same endpoint record in a single batch file.**

Example of Add Operation

The following is an example of an add operation in the batch file:

1;PBX1;300;00DC45AC1021;ERL_RG5;192.168.1.2;JOHN SMITH;1245785451;

- The operation is set to Add or Update.
- The IP-PBX to which the phone is assigned is provided.
- The phone's extension number and MAC address are provided.
- The number 1245785451 is the UNIX timestamp and represents the time: Tue, 23 Jun 2009 19:30:51 GMT.

Example of Delete Operation

The following is an example of a delete operation in the batch file:

2;PBX2;;509A4C5262CC

- The operation is set to delete
- The IP-PBX to which the phone is assigned is provided
- The MAC address is provided.



** Note: For the delete operation, it is important to send only the **Operation**, **IP-PBX name**, **Extension** or **MAC address** fields. But for Cisco and ShoreTel endpoints, the **Device Name** is also accepted. Sending other fields will cause the validation to fail.

12.2.6 Endpoint Batch Logs

Batch log files report on the success or failure of each entry in a submitted batch file. The batch logs are generated in response to the following actions:

- Batch Process

To view the batch logs

- Click on **Provisioning > Endpoints > Batch**

The columns of the log display the following information:

- Original File Name
- Log File
- Error Log File
- Log Date
- Status
- Actions (Batch Process and Delete*)

*These actions apply to uploading an endpoint batch file using the Dashboard interface, or for endpoints added using the automatic endpoint inventory feature. To display endpoints added using the automated endpoint inventory feature, it is necessary to place a checkmark in the box "Display Automatic."

12.2.6.1 Log File

To view a log file, click on **View Log File** under **Log File**.

The log file provides a status report for each line of the processed batch file. A line will contain an error code followed by the original line in the batch file. If the operation was executed successfully, the response code will be set to 00. If the operation failed to complete successfully, the error code will be larger than 00. For more information on these codes, please refer to section 12.2.6.2.1 Response Codes.

12.2.6.2 Log Error File

To view the log error file, click on **View Log File** under **Error Log File**.

The **Error Log File** is only generated when an error was detected in the log file and an entry could not be processed. The lines in this file will contain a response code followed by the original entry that could not be processed. For more information on response codes, please refer to section 12.2.6.2.1 Response Codes.

12.2.6.2.1 Response Codes

The following table details each possible outcome resulting from a single operation.

Table 85: Endpoint Batch Log Response Codes

Response Code #	Description	Add / Update	Delete
00	SUCCESS	X	X

Response Code #	Description	Add / Update	Delete
	The entry is successful.		
01	INVALID_ROW_NUMBER_ The entry does not have the right number of fields.	X	X
02	INVALID_OPERATION_ The operation entered is invalid.	X	X
03	INVALID_PBX_NAME_ The IP-PBX name entered is invalid.	X	X
04	INVALID_ENDPOINT_ The endpoint format is invalid.	X	X
05	INVALID_MAC_ADDRESS_ The MAC address format is invalid.	X	X
06	INVALID_MAC_ENDPOINT_ The Endpoint ID was not specified. Either extension or MAC must be present in the batch file.	X	X
07	INVALID_ERL_ID_ The ERL ID entered is invalid.	X	
08	INVALID_IP_ADDRESS_ The IP address entered is invalid.	X	
09	INVALID_DISPLAY_NAME_ The display name entered is invalid.	X	
10	INVALID_TIMESTAMP_ The timestamp entered is invalid.	X	
11	TIMESTAMP_TOO_OLD_ The timestamp entered is too old.	X	
12	ENDPOINT_CONFLICT_		
13	CANNOT_DELETE_FULL_LIST_MODE_ The entry cannot be deleted because the EGW is set to perform automatic batch provisioning.	X	
14	ENDPOINT_DOESNT_EXISTS_		X

Response Code #	Description	Add / Update	Delete
	The endpoint does not exist.		
15	ENDPOINT_ALREADY_INSERT_ Endpoint_already_exists The endpoint was previously added within this batch file. Row ignored. Only applies if Endpoint record not previously provisioned in the database.	X	
17	ENDPOINTS_LICENSE_EXCEEDED_ Endpoints License Exceeded. The limit of allowed endpoints has been exceeded. Please check the endpoints license.	X	
18	INVALID_DEVICE_NAME_ Invalid Device name. The device name is not valid. Only alphanumerical characters are accepted.	X	
19	ENDPOINT_EXISTS_CROSS_CLUSTER_ Endpoint exists cross cluster. The endpoint row exists in another PBX ID belonging to the same group.	X	
20	MISSING_EXT_FOR_STATIC_ASSIGNMENT_ Extension must be provided when statically assigning a location to an endpoint. This error code is returned only for Avaya, Skype for Business, Generic and Aastra PBX types.	X	
21	MISSING_MAC_OR_EXT_ Extension or MAC address must be provided. Providing only the Device Name is not supported for this PBX Type. This error code is returned only for Aastra, Skype for Business, Generic and Avaya PBX types.	X	
22	MISSING_DN_FOR_STATIC_ASSIGNMENT_ Device name must be provided when statically assigning a location to an endpoint. This error code is only returned for Cisco IP-PBX.	X	
200	SKIPPED_ This code is returned when less information is provided than what is currently already present in the endpoint records.	X	X

The following is an example batch log:

00;1;PBX1;300;00DC45AC1021;ERL_RG5;192.168.1.2;JOHN SMITH;5552224141;1245785451

- The 00 at the beginning of the batch log indicates that the endpoint entry was successful.

View Peer

If **Log File** displays **View Peer**, you must login to the Peer to view the log file. This scenario occurs when a batch file is processed by the Peer machine.

12.3 Exporting/Backing Up Endpoints

Use the Reports screen to create endpoint export files for your own use, for example, to back up or move an endpoint configuration. Endpoints are exported from the EGW by generating an Endpoint report. The report is a semicolon delimited batch file that may be re-imported using the Dashboard.

To generate an Endpoint report

- Click on **System Status > Reports** and select the endpoints file type.

For more information see section 18.4 "Reports."

12.4 Call History (CDRs)

You may view the emergency call history of the endpoints on the network using the Call Detail Records (CDRs) on the Dashboard. On the CDRs screen of the web Dashboard, it is possible to search for a specific endpoint by entering its MAC address or other unique parameter. This allows you to quickly review the call history for a specific endpoint.

The CDRs include the following fields:

- Start time
- Duration
- Endpoint caller ID
- ERL ID
- Callback number
- Call destination
- Wave file
- Call status
- url data

CDRs allow you to:

- Click on the wave file to listen to the recording of the call.
- Filter the logs by month using the search feature to quickly retrieve a specific record.
- Review parameters per call under a variety of troubleshooting scenarios.
- Determine the destination IP and Call Destination of each 911 call

Note: A call minute is approximately 1024Kb. On a 30 GB partition, the recorded call minutes could go up to 31,000 minutes.

13 Layer 2 Discovery

The EGW uses layer 2 discovery to determine the location of a phone based on its attached switch or switch port. This capability can provide highly granular location discovery down to the floor or cubicle level.

Enterprises can either assign ERLs to switches, or to individual switch ports. In a common use scenario, an enterprise with a switch on each floor can assign an ERL per switch. For a greater level of granularity, ERLs may be assigned on a switch port basis (eg. 1 ERL per cubicle). In deployments where switches span multiple floors, ERLs are assigned on a per port basis, in order to provide floor level granularity.

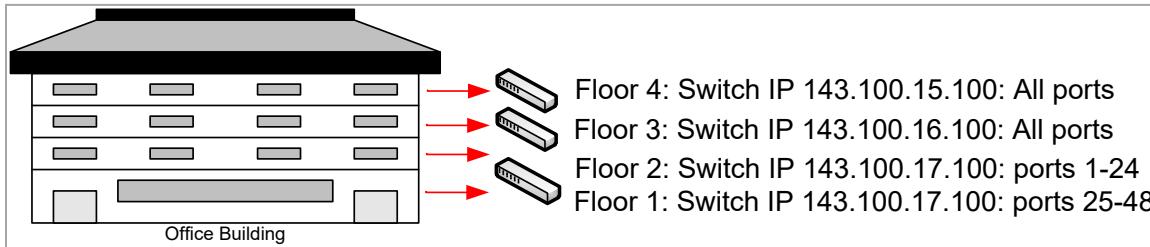


Figure 47: Layer 2 Discovery

13.1 Switch Requirements for EGW

The EGW Layer 2 Discovery uses different discovery models depending on the MIB supported by the switches being scanned. The EGW supports the following Switch Types:

- Auto Detect
- 3Com Bridge MIB
- 3Com Q-Bridge MIB
- Bridge-MIB
- Q-Bridge-MIB
- Phybridge-PoLRE-MIB
- Phybridge-Uniphyer-MIB
- Cisco
- Juniper

Cisco:

Supports the following

- VLAN-based discovery
- Trunk port detection
- Auto detect

Juniper:

Supports the following

- VLAN-based discovery
- Trunk port detection
- Auto detect

Phybridge:

Supported Models:

- Phybridge-PoLRE-MIB
- Phybridge-Uniphyer-MIB

Supported features:

- Auto detect

Note: Because of Phybridge's unique "central convergence" topology, trunk port detection and VLAN-based discovery are not required.

Bridge-MIB:

The Bridge-MIB only provides basic Layer 2 Discovery.

All Models:

The EGW uses SNMP to track your phones and supports the following versions of SNMP:

- 1
- 2c
- 3

Ensure that the phones you are using are supported by EGW.

The Network hardware and Software Requirements lists the supported devices and software versions, on a per vendor basis. For more information, see section 2.2 "Emergency Gateway Specifications."

13.2 Understanding How Layer 2 Discovery Works

Layer 2 Discovery depends on a layer 2 map that associates your layer 2 switches and ports to Emergency Response Locations (ERLs). Once the layer 2 map has been loaded into the EGW configuration, the EGW scans the switches to discover the MAC addresses of the devices behind the switch ports. Scanning the switches enables the EGW to track the locations of the devices.

It is also extremely important that the endpoints be provisioned for them to be scanned successfully.



Note: Before provisioning layer 2 discovery information, it is necessary to have previously added ERLs to the EGW configuration. ERLs cannot be assigned to switches, unless they are already present in the configuration. It is also necessary to populate the endpoints inventory, before the phones can be tracked.

13.2.1 EGW Scans

The EGW can perform manual or scheduled scan jobs. When the Layer 2 Discovery feature is enabled, a daily scheduled scan is enabled, which will run based on the default settings of the task scheduler.

The Layer 2 Discovery Scan Manager is responsible for running both the manually created and scheduled jobs. The scan jobs are comprised of scan tasks per switch that use SNMP to discover the MAC addresses behind the switch ports.

13.2.2 3rd Party Scanning

Scanning can be enabled or disabled on a per switch basis. If scanning is disabled, a third party scanning tool can be used to scan the switches and deliver the results to the EGW.

The third party external scan data can be manually added to the EGW from the Dashboard, or the data can be uploaded to the EGW FTP for processing. The EGW also has a SOAP interface for third party scanning data.

The Layer 2 Discovery Manager is responsible for processing the third party external scan data using a scan job. The third party scans can be manually run by uploading a batch file from the Dashboard.

A daily scan job called "Layer 2 Scheduled 3rd Party" will process the data from the FTP or SOAP interface.

For information about the SOAP interface, see the document "EGW SOAP Server API Interface Description."

13.2.3 The Layer 2 Discovery Scan Manager

The EGW Layer 2 Discovery Scan Manager is responsible for managing both the EGW scans and processing of 3rd party scanning data.

The results of the scans and data processing are available at **Auto Discovery>Layer 2 Discovery>Scan**.

It is also possible to see all of the discovered switch ports and MACs by going to **Auto Discovery>Layer 2 Discovery>Discovered Ports**.

13.2.4 Automatic Phone Inventory

You can setup your EGW to automatically discover the endpoint inventory that will be used for Layer 2 Discovery. This capability can work independent of, or in conjunction with, vendor-proprietary methods of endpoint discovery. The feature is enabled by specifying a MAC address mask (configured using regular expressions) on a per IP-PBX basis. For the group of endpoints discovered within the group during a Layer 2 scan, the EGW adds the endpoints to the inventory, and assigns them to the connected switch/switch port and ERL.

For more information see section 12 “Endpoints.”

13.2.5 How Does the EGW assign ERLs to Endpoints Using Layer 2 Discovery

The endpoints can be manually added using the **Endpoints** tab or they can be provisioned automatically using **Auto Discovery**. Once the endpoints are provisioned, they can be tracked. The EGW Layer 2 Discovery feature will only process endpoint tracking information for endpoints that are provisioned.

The tracking process uses SNMP to associate the provisioned MAC address of a phone with a switch, switch port and ERL. Phone is assigned to an ERL when the next layer 2 discovery scheduled task runs.

Once the endpoints exist in the inventory, and have been assigned to an ERL, the EGW updates the device’s ERL if the phones move. After the phone moves, it is assigned to a new ERL when the next layer 2 discovery scheduled task runs.

13.2.5.1 Unprovisioned/Call Center

If a phone is not found on the network during a subsequent scan it is set to call center mode. In this mode emergency calls route to the ECRC. The MAC ageing time of your layer two switches is applicable, and the MACs must be aged out of the switch tables before the EGW will fail to discover a MAC in a subsequent scan. The **Layer 2 Discovery Failure Count** parameter setting at the EGW is also applicable. This setting controls the amount of times that the layer 2 task will fail to discover a previously discovered endpoint, before the status of the endpoint is changed to call center mode (Unprovisioned).

The following scenarios are applicable

- Endpoint keep alive/IP-PBX re-registration setting is longer than the MAC address age-out time on switches.

In this case, endpoints will fail to exist on the switches for a period of time and could go undiscovered by the EGW. It is important to always set the endpoint keep alive/IP-PBX re-registration timer to be of shorter duration than the MAC address age out time of your switches. This will help to ensure that the EGW properly discovers the endpoints.

13.3 Interconnected/Cascaded Switches

The EGW is capable of supporting large deployments of interconnected switches. The switches may be managed and/or unmanaged and they may be deployed with either single or redundant links.

13.3.1 Understanding How the EGW Supports Interconnected Switches

When the EGW scans the switches it can determine the trunking ports which are uplink ports. A port is determined to be an uplink port if its MAC address exists on another port’s forwarding MAC table.

For certain switch vendors, it is also possible for the EGW to use Trunk Port Detection (enabled on a per switch basis) to detect trunk ports. When automatic trunk port detection is enabled, the EGW will determine the trunking ports by querying the information found in the switch MIB. It is also possible to modify the switch inventory using the Dashboard to manually indicate the trunking ports.

By accurately identifying all trunk ports (including uplink ports) the EGW is able to appropriately handle instances of duplicate MACs that can be discovered on the network. The EGW ensures that only MAC addresses that represent real phones are tracked and assigned ERLs.

If an instance of a duplicate MAC is detected that requires investigation, the EGW will generate an alarm.

For example, for longer scanning intervals, a MAC address could move which would result in a duplicate MAC being detected. The EGW would then issue an alarm.

13.3.1.1 Port Types

For each port the EGW discovers on the switches, the following port types are possible.

Trunk Port: Port specifically identified by the switch as a trunk port by information found in one of its MIBs.

Uplink Port: Port determined to be a trunk port by the EGW because it's MAC address is found on another port's forwarding MAC table.

Manual Trunk: User has configured this port as a trunk port.

Not Trunk: Assumed to be an access port and is eligible to determine an endpoint's location.

Note: There are some cases wherein a phone can be connected to a Trunk Port. Cisco switches assume that any port that performs VLAN tagging is a trunk port but some phones do support VLAN tagging. However, EGW will not detect this phone's MAC address on any access port. To solve this discrepancy, EGW will try to detect the port that only has the Trunk Port status.

For more information, see section 13.6.3 "Discovered Ports."

13.3.2 Provisioning the EGW with Interconnected Switches

In large deployments of interconnected switches, it is often necessary to distinguish between different switch layer designations: Access, Distribution, and Core. In EGW deployments, it is only necessary to provision the Access and Distribution layers. It is not necessary to provision your Core switches.

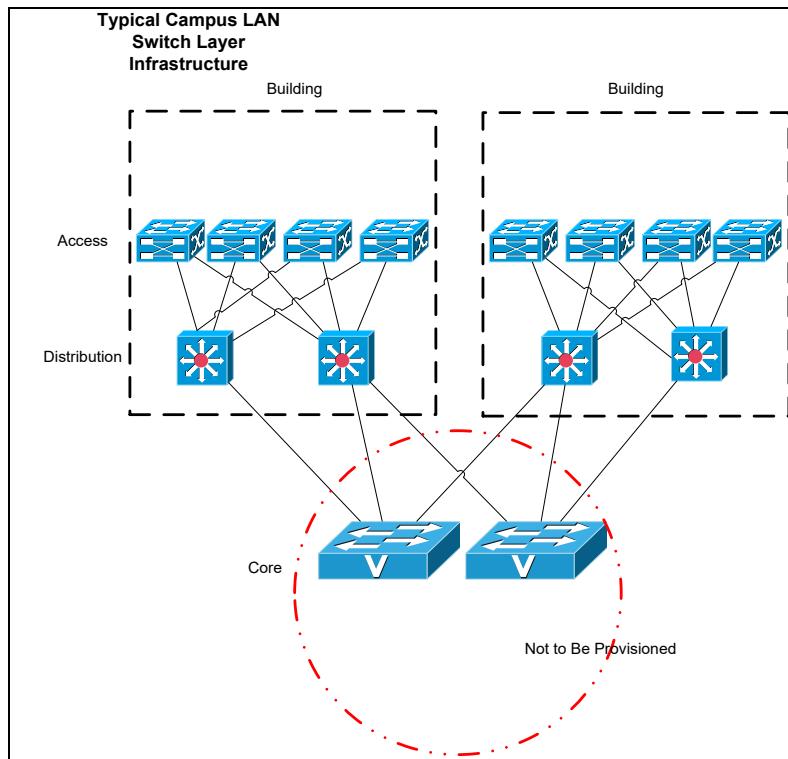


Figure 48: Provisioning of Interconnected Switches

In regards to a common campus LAN infrastructure, standard switch layers may be defined as follows:

- **Access switches:** The access layer of the Campus LAN includes the portion of the network from the desktop port(s) to the wiring closet switch. For the EGW's purposes, your Access switches are any switches attached to endpoints capable of making emergency calls.*

*In a common campus LAN infrastructure, Access switches may be either managed or unmanaged devices. For the EGW's purposes, an unmanaged switch is any switch that does not support the required SNMP MIBS. For unmanaged switches, the EGW can only assign one ERL per switch. For managed switches, ERLs may be provisioned down to the switch port level.

- **Distribution switches:** The distribution layer of the Campus LAN includes the portion of the network from the wiring closet switches to the next-hop switch, and it may be the first layer-2-to-layer-3 traversal in the LAN.

Access and Distribution Switch Provisioning

The EGW supports two common layer 2 discovery scenarios for deployments with interconnected switches

1. ERL assignment to the port level.
 2. ERL assignment to the switch level.
1. Port-level ERL provisioning

If you will be provisioning ERLs to the port level, you must provision both your Access and Distribution switches. In this scenario, port ERLs are provisioned for the Access switches. Default ERLs are provided for the Distribution switches.

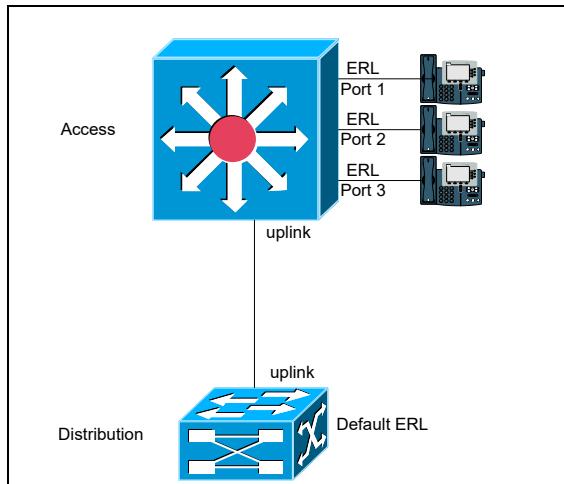


Figure 49: Port-Level ERL Provisioning

2. Switch-level ERL provisioning

In this scenario, only the Distribution switches are provisioned. Each Access switch is assigned an ERL based on the port to which it is connected on the Distribution switch. When a phone connects to an Access switch, it takes the ERL from the connected Distribution switch port.*

***Trunk Port Detection** should be set to **No** in this scenario.

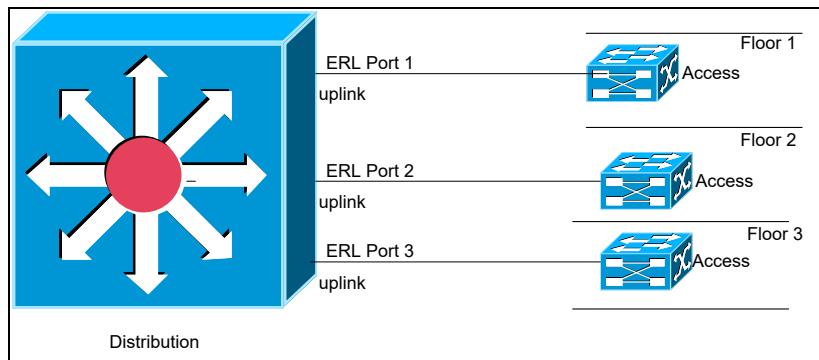


Figure 50: Switch-Level ERL Provisioning



Note: This is the recommended topology for enterprises with unmanaged switches as part of the LAN infrastructure. An unmanaged switch is assigned an ERL based on the Distribution switch port to which it is connected. The ERL of the unmanaged switch is the same as the ERL which is assigned to the Distribution switch port.

13.3.3 Voice VLAN Options

Voice VLAN Options can be used to limit SNMP scanning to specific voice VLANs. The feature can be used to limit EGW Layer 2 Discovery to the specific VLANs to which the endpoints are attached.

For more information, see section 13.4.2 “Switch Identification.”

13.4 Configuring Layer 2 Discovery

To enable layer 2 discovery, you must provision the EGW with the details of the switches. Switches may be configured one at a time, or multiple switches may be configured simultaneously in a batch.



Note: Before provisioning layer 2 discovery information, it is necessary to have previously added ERLs to the EGW configuration.

13.4.1 Global

Layer 2 Discovery behavior is controlled by the Global settings, defined in the table below.

Table 86: Layer 2 Discovery - Global Settings

Parameter	Description
Layer 2 Discovery Disabled	Parameter that enables/disables the layer 2 Discovery module. When Layer 2 Discovery is disabled, the Scan Manager will not process any new scan jobs.
Layer 2 Discovery Failure Count	Parameter that controls the amount of failed attempts that must occur, before the EGW puts a previously discovered endpoint into call center mode (Unprovisioned). For more information, see section 13.2.5 “How Does the EGW assign ERLs to Endpoints Using Layer 2 Discovery.”
Job Log Level	Parameter that controls log verbosity of scan job logs. For a list of log verbosity levels applicable, click here .
Task Job Level	Parameter that controls the log verbosity of the tasks in any given job. For a list of log verbosity levels applicable, click here .
Batch 3 rd Party Processing Format Type	Setting which controls batch processing for 3 rd party scans: Full or Incremental Using the incremental setting, the batch file will only add/overwrite data to the EGW for the specific MACs in the batch file. When using the Full discovery cycle, the EGW will expect the entire inventory of MACs to be provided for each scan. The setting is only applicable to deployments that use 3 rd party scanning tools, and depends on how the tool is setup to work with EGW.
Number of Concurrent SNMP Connections	Parameter that controls the number of parallel SNMP connections that the Scan Manager can run at the same time. The parameter controls the number of switches that can be scanned in parallel.
Submit Endpoint File	Global parameter that controls how the EGW will process MACs that are discovered on the switches. The parameter is also available on a per scan basis. If set to Yes, the EGW will process the MAC addresses discovered on the switches by updating the endpoints inventory. If set to No, the EGW will not update the endpoints inventory, based on the results of the scan. The results of the scan are stored on the EGW, pending manual intervention. This parameter can be used if processing of partial results to the endpoint table is determined to be problematic. To insure reliable endpoint location information, Layer 2 Discovery errors should be investigated and corrected promptly. Repeated failure to scan one or more switches will prevent the EGW from accurately associating ERLs to endpoints.

Submit Endpoint File On Failure	<p>Global Parameter that controls how the EGW will process MACs that are discovered on the switches. The parameter is also available on a per scan basis.</p> <p>If set to Yes, the EGW will process the MAC addresses discovered on the switches, even if there were some scanning errors during the scan (eg. A switch was unreachable).</p> <p>If set to No, the EGW will not update the endpoints inventory, based on the results of the scan. The results of the scan are stored on the EGW, pending user intervention.</p> <p>This is useful for troubleshooting purposes, when you want to review the discovered MACs before committing to making changes to the endpoints inventory.*</p>
Automatic Phone Inventory	Parameter settings which control the Automatic Phone Inventory feature.

**Note: This is especially useful when processing of partial results to the endpoint table is determined to be problematic. Normally, Layer 2 Discovery results will provide enough information to update endpoints found on the switches that were successfully scanned while preserving existing information. To ensure reliable endpoint information, Layer 2 discovery errors must be investigated and corrected promptly.*

Log Verbosity Levels

The following log verbosity levels are applicable. The selected verbosity level is inclusive with any higher level. For example, when debug is set, Debug, Info, Warning and Error events are output to the scan log.

The following table describes the log verbosity levels:

Table 87: Log Verbosity Levels

Log Verbosity Level	Description
Off	No messages will be outputted to the logs
Error	Error events will be output to the scan logs
Warning	Warning and error events will be output to the scan log
Info	Info, warning, error events will be output to the scan log
Debug	Debug, info, warning and error events will output to the scan log
All	All events will be output to the scan logs

Note: Log verbosity settings should be made in accordance with your system's log growth rate. This will ensure smooth EGW operation and that log files do not grow to unmanageable sizes.

13.4.1.1 Configuring Automatic Phone Inventory

To configure automatic phone inventory you need to indicate the endpoints for the IP-PBX that will be enabled for the feature. You will specify the Organizationally Unique Identifier and range of MAC addresses using regular expressions.

To configure automatic phone inventory

1. Click on **Auto Discovery>Layer 2 Discovery>Global**
2. Click on **Edit**.

3. For **Automatic Inventory** select the appropriate IP-PBX from the dropdown.
4. Add the regular expression pattern(s) that establishes the range of MAC addresses that will be enabled for Automatic Phone Discovery. Any MAC addresses discovered on the network within the range are added to the endpoints database and associated to the ERL of the attached switch port(s).

To see examples specific to your IP-PBX system, and to obtain the correct OUI, see section 7 “Configuring IP-PBX Settings.”

For more information concerning endpoint provisioning, see section 12 “Endpoints.”

13.4.2 Switch Identification

Switches can be added one at a time, or multiple switches can be added using a batch file.

To add a switch on the Dashboard

1. Click on **Auto Discovery > Layer 2 Discovery > Switch > Add a Switch**.
2. Configure the appropriate settings as described in the following table.

Table 88: Adding a Switch - Field Descriptions

Parameter	Description
IP Address	IP address of the switch. Required.
SNMP Port	Standard SNMP port. Numerical value. Default value is port 161. Must be a numeric value within the valid port range: between 1-65535.
Switch Type	<p>The EGW provides support for several Layer 2 Discovery models. This provides support for managed switches from most switch vendors on the market.</p> <p>Auto Detect: If no specific Switch Type is specified, the EGW will attempt to auto-detect the MIB supported by the switch on the next scan.</p> <p>Bridge-MIB: Layer 2 Discovery model that provides support for switches that use the Bridge MIB.</p> <p>Cisco: Layer 2 Discovery model that provides support for Cisco switches.</p> <p>Juniper: Layer 2 Discovery model that provides support for Juniper.</p> <p>Phybridge-PoLRE-MIB: Layer 2 Discovery model that provides support for Phybridge.</p> <p>Phybridge-Uniphyer-MIB: Layer 2 Discovery model that provides support for Phybridge.</p> <p>Q-Bridge-MIB: Layer 2 Discovery model that provides support for switches that use the Q-Bridge MIB.</p>
Scan Enabled	Parameter that enables or disables scanning for a switch. Switch scanning can be disabled for deployments that use 3 rd party scanning tools to scan the switches.
SNMP Version	1, 2c or 3.
SNMP Timeout	Time in seconds that the EGW will attempt to scan a switch before a switch timeout occurs.
SNMP Retry Count	Number of attempts the EGW will initiate before declaring that the switch is unreachable.
Description	Short note describing or identifying the switch. This field is optional.
Vendor	Switch vendor (optional).
Default ERL ID	ERL ID representing the physical location of the switch in the enterprise deployment. Required.

Parameter	Description
Log Level	Parameter that controls log verbosity of scan tasks. For more information, see section 13.4.1 "Global."
Trunk Port Detection	Parameter that enables/disables trunk port detection for the switch. When trunk port detection is enabled, the EGW will determine which ports are trunk ports to properly manage instances of duplicate MAC addresses found on the network. This option is only available for switches that provide trunk port identification in their MIB. At present, this is implemented for Cisco and Juniper switches.
Only Scan Voice VLANs	Yes/No. Parameter that enables scanning of specific VLANs on the network. If enabled, you can specify the specific Voice VLANs that you would like the EGW to scan. Scanning will be limited to only these specific VLANs.
SNMP Community String	String that acts as a password to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). Special characters are accepted and must be 25 characters or less. Default value is "public."

13.4.2.1 SNMP Version 3

If SNMP version 3 is selected as the SNMP version, additional security parameters become available, as defined below.

Table 89: SNMP Version 3 Security Levels

Security level	Authentication	Encryption	Function and accepted characters
V3 (noAuthNoPriv)	Username/Security Name. Up to 50 alphanumeric and special characters accepted.	None	Uses username for authentication. Packet is passed in clear text.
V3 (authNoPriv)	MD5 or SHA. Requires Username and Auth passphrase. Up to 50 alphanumeric and special characters accepted.	None	Uses HMAC-MD5 or HMAC-SHA for authentication. Remaining packet is passed in clear text.
V3 (authPriv)	MD5 or SHA. Requires Username, Auth passphrase and Encrypt Passphrase. Up to 50 alphanumeric and special characters accepted.	DES (data encryption standard), or AES (advanced encryption standard). Requires encrypt passphrase.	Uses HMAC-MD5 or HMAC-SHA for authentication. Entire packet is encrypted.

13.4.2.2 Assigning ERLs to Specific Ports on a Switch

It is possible to assign ERLs to specific ports on a switch, when those ports are wired to devices in a different ERL. It may also be necessary to assign ERLs to specific ports on a switch in the event that a switch is rewired.

A common scenario occurs for unmanaged switch ports that will take the ERL from the port of the Distribution switch to which they are connected. In this case, it is necessary to assign an ERL to this port which reflects the physical location of the unmanaged switch.

To manually assign ERLs to specific ports on a switch

1. For the switch that you want to edit, expand the switch by clicking on the plus sign next to the IP address.
2. To add a port prior to a scan, click on **Add a port**. To import ports from a previously scanned switch, click on **Import Ports**.
3. Configure the parameters in the table below.

Table 90: Adding a Port- Assigning ERLs to a Specific Port

Parameter	Description
Switch Port Name	Name of the port on the switch. Eg. Fa0/1
Default ERL ID	ERL that will be applied to the port on the switch.
Trunk Port	Parameter that indicates if a port is a trunk port.

4. Once you have entered the applicable data click on Create or Save.

13.4.3 Provisioning Switches in a Batch

To upload multiple switches simultaneously, it is possible to upload switches in a batch. You may upload batch switches using the Dashboard or FTP:

- **Administrative Dashboard:** A batch file is uploaded using the EGW web interface. The file may be validated and processed in real-time.
- **FTP:** The file is uploaded via FTP. It is validated and processed based on the settings of the Scheduled Task.

13.4.3.1 Dashboard

To upload a batch file via the Dashboard interface

1. Prepare the batch file in accordance with the batch file format, as mentioned in section 13.4.4 Batch File Format.
2. Click on **Auto Discovery > Layer 2 Discovery > Switch**
3. Click on **Import**.
4. Add the file and click on **Start Upload**.
5. Click **Validate***
6. The Log File is displayed in the Import Switches Dialog Window
 - a. If the batch log file does not include any errors you may move ahead to the processing stage by clicking **Import**. Then click on **Finish**.
 - b. If the batch log file contains errors, you may correct them before attempting another validation.

*When you click **Validate**, the batch file is validated and a log file is generated. The log file reports the success or failure of each entry in the batch file. If there are errors you must correct them before moving ahead to the processing stage.



Note: The batch switches feature functions incrementally: the batch file will only add/overwrite data to the EGW for the specific switches in the batch file. The batch file will not overwrite data for switches that are not specified in the batch file. However, any errors generated during the batch upload process necessitate the re-upload of the **entire** batch file.

13.4.3.2 FTP

To batch upload via FTP:

1. Open an FTP connection to the EGW using the IP of the EGW, username: batchswitch, password: 911batch.

2. Go to **batch** directory.
3. Upload the file to the EGW.

Batch files uploaded to the EGW using FTP are governed by scheduled tasks settings. The scheduled task **Batch Switches** dictates precise daily intervals at which batch processing will occur.



Note: After a batch file uploaded to the EGW via FTP is processed, it is automatically removed from the FTP directory. These files can be viewed using the Dashboard interface.

FTP Batch Results

The batch logs summary and error reports are sent to the email addresses configured at **Configuration > Advanced > Batch Settings**. Logs can also be viewed from the Dashboard.

13.4.4 Batch File Format

Switches can be uploaded to the EGW using CSV or text batch file formats.

The CSV format supports switches using SNMP versions 1, 2c or 3.

The text-based batch file format does not support SNMP v3.

Also, for text-based batch files, the Scan Enabled parameter is not present and all switches default to Scan Enabled: Y.

13.4.4.1 CSV batch file format

The supported CSV format uses the following headers.

Table 91: Batch Provisioning of Switches

CSV Header	Description	Required
SWITCH_IP	Unique IP Address among the switch.	Y
SNMP_VERSION	SNMP Version of the switch. 1, 2c, or 3. Default is 2c	N
SNMP_COMMUNITY	SNMP Community String. Special characters are accepted and must be 25 characters or less. Default value is "public."	Y (V2c)
SNMP_SECURITY_NAME	Security name required for SNMP Version 3. Up to 50 alphanumeric and special characters accepted.	Y(V3)
SNMP_SECURITY_LEVEL	V3 (noAuthNoPriv), V3 (authNoPriv), V3 (authPriv)	Y(V3)
SNMP_AUTH_PROTOCOL	MD5 or SHA	Y(V3-Auth)
SNMP_AUTH_PASSPHRASE	Up to 50 alphanumeric and special characters accepted.	Y(V3-Auth)
SNMP_ENCRYPT_PROTOCOL	DES or AES	Y(V3-Priv)
SNMP_ENCRYPT_PASSPHRASE	Minimum 8 and maximum 50 alphanumeric and special characters accepted.	Y(V3-Priv)
SNMP_PORT	SNMP Port. Default value is port 161. Must be a numeric value between 1-65535.	N
DESCRIPTION	Description of the switch. Alphanumeric. No limits.	N

CSV Header	Description	Required
VENDOR	Vendor of the switch. Alphanumeric between 1 and 25 characters.	N
ERL_ID	Default location for the switch/port. Alphanumeric between 1 and 31 characters in length.	Y
PORT_NAME	Port Name or * for switch. The port of the switch in the row. NOTE: Use the wildcard (*) to add a switch. Use the switch port name to create a switch port entry in the network map. Alphanumeric up to 50 characters. Only necessary if the switch port you are uploading requires an ERL ID other than the Default ERL ID for the switch.	Y
IS_SCAN	A value of 1 indicates that the EGW will scan the switch using SNMP. A value of 0 indicates that the switch will not be scanned. In this case, third party Layer 2 Discovery scanning tools can be used to populate the data in the EGW.	Y
LOGGING_LEVEL	Parameter that controls log verbosity of scan tasks. The following log verbosity levels are applicable: "OFF", "FATAL", "ERROR", "WARN", "INFO", "DEBUG", "TRACE", "ALL"	N
SWITCH_TYPE	Layer 2 discovery model that provides support for vendor switch MIBs. Possible values: Bridge-MIB.js Cisco.js Q-Bridge-MIB.js	N
SNMP_TIMEOUT	Switch timeout value in seconds. Integer, greater than zero	N
SNMP_RETRY_COUNT	Number of attempts the EGW will initiate before declaring that the switch is unreachable. Zero or positive integer.	N
TRUNK_PORT_DETECTION_ENABLED	Parameter that enables/disables trunk port detection for the switch. Integer, 0 or 1 (Boolean value)	N
ONLY_SCAN_VOICE_VLAN_ENABLED	Parameter that enables scanning to be restricted to specific VLANs. Integer, 0 or 1 (Boolean value) Required if voice VLANs are available for scanning.	N
VOICE_VLANS	List of VLANs to scan. String, a list of comma separated integers, Example: 1,3,2,5 Possible range: [1..4095]	N
IS_TRUNK_PORT	Parameter that indicates if the specified port is a trunking port. Integer, 0 or 1 (Boolean value)	N

13.4.4.1.1 Batch File Examples

Example with SNMP v3:

```
SWITCH_IP,SNMP_VERSION,SNMP_COMMUNITY,SNMP_SECURITY_NAME,SNMP_SECURITY_LEVEL,
SNMP_AUTH_PROTOCOL,SNMP_AUTH_PASSPHRASE,SNMP_ENCRPT_PROTOCOL,SNMP_ENCRYPT_PASSPHRASE,
SNMP_PORT,DESCRIPTION,VENDOR,ERL_ID,PORT_NAME,IS_SCAN,LOGGING_LEVEL,SWITCH_TYPE,
SNMP_TIMEOUT,SNMP_RETRY_COUNT,TRUNK_PORT_DETECTION_ENABLED,
ONLY_SCAN_VOICE_VLAN_ENABLED,VOICE_VLANS,IS_TRUNK_PORT
```

192.168.1.1, 3, public, security_name, authPriv, MD5, auth_password, DES, encrypt_password, 162, test Switch, Vendor, 123 Main Street, *, 1, DEBUG, cisco.js, 5, 3, 1, 1, "1,2,3,4", 0

In this example, the user adds a switch with SNMP v3 enabled. Security names, levels and authentication settings are made accordingly.

This example adds a switch with the ERL 123 main Street. The switch is set to be scanned, and the logging level for the log files is set to DEBUG. The switch type is set to Cisco, and SNMP timeout and retry counts are set. Trunk port detection is enabled, meaning that the EGW will use vendor specific MIB information to determine which port are trunking ports. Also, this file is setup to only enable scanning for specific VLANs.

Note: Double quotes around multiple VLANs not required in CSV file.

Example with SNMP v3:

```
SWITCH_IP,SNMP_VERSION,SNMP_COMMUNITY,SNMP_SECURITY_NAME,SNMP_SECURITY_LEVEL,
SNMP_PORT,DESCRIPTION,VENDOR,ERL_ID,PORT_NAME,IS_SCAN,SWITCH_TYPE,SNMP_TIMEOUT,
SNMP_RETRY_COUNT,LOGGING_LEVEL,TRUNK_PORT_DETECTION_ENABLED,
ONLY_SCAN_VOICE_VLAN_ENABLED,IS_TRUNK_PORT
```

192.168.1.1, 3, public, SNMP security name, noAuthNoPriv, 161, switch description, Cisco, DEMO_ERL, *, 1, Cisco.js, 5, 2, INFO, 1, 0, 0

This row adds a switch using SNMP v3 with noAuthNoPriv. The row adds an entire switch using the Cisco.js scanning model, which supports Cisco switches. Scanning is enabled for the switch, and the SNMP Timeout and retry counts are provided. The logging level for the switch scanning will use INFO. Trunk port detection is enabled, but scanning is not restricted to specific VLANs.

Examples with SNMP 2c:

Example of valid CSV Layer 2 batch file:

```
"SWITCH_IP","SNMP_VERSION","SNMP_COMMUNITY","ERL_ID","PORT_NAME","IS_SCAN"
"192.168.0.240","2c","public","LOC56","*","1"
"192.168.0.240","2c","public","LOC56","Fa0/1","1"
"192.168.0.240","2c","public","LOC56","Fa0/2","1"
"192.168.0.240","2c","public","LOC56","Fa0/3","1"
"192.168.0.240","2c","public","LOC56","Fa0/4","1"
"192.168.0.240","2c","public","LOC56","Fa0/5","1"
```

13.4.4.2 Structural Restrictions

Batch file structural restrictions apply in the scenario where you are assigning switch ports to different ERLs than the default ERL for the switch. If all of the ports on the switch will use the same ERL ID, it is not necessary to specify ERL IDs on a per-port basis.

The structure of the batch files must observe the following rules:

- It is not possible to upload a batch file that **only** includes switch ports. The file must also include a switch or switches.
- It is not possible to upload a file where switch port entries precede switch entries.
- Do not provision the same switch more than once in a batch file. If a switch has been provisioned with some port specific ERLs and the same switch occurs as a row later in the batch file, the proceeding switch and port specific ERL mappings are deleted.
- Example:

- Switch IP A *
- Switch IP A Port1
- Switch IP A Port2
- Switch IP A Port3
- Switch IP A *
- Switch IP A Port1
- Result: Switch IP A is provisioned with one port only

13.4.5 Batch Logs

Batch log files report on the success or failure of each entry in a submitted batch file. The batch logs are generated in response to the following actions:

- Validate

To view the batch logs

- Click on **Auto Discovery > Layer 2 Discovery > Switch**

The columns of the Batch Logs display the following information:

- Original File Name
- Log File
- Log Date
- Status

To view a log file, click on link under the column **Log File**.

The batch file results returned in the log file are displayed in CSV format. The results include an error code and description followed by the original line in the batch file entry:

"error code","error description","SWITCH_IP","SNMP_VERSION","SNMP_COMMUNITY","ERL_ID","PORT_NAME","SCAN_ENABLED"

"10", "The Switch Port ID could not be associated to a corresponding switch ID", "192.168.0.240", "2", "public", "LOC56", "*", "1"

"00", "success", "192.168.0.240", "2", "public", "LOC56", "*", "1"

If **Log File** displays **View Peer**, you must login to the Peer in order to view the log file. This scenario occurs when a batch file is processed by the Peer machine.

13.4.5.1 Batch Log Error Codes

The following table details each possible outcome resulting from a single operation.

Table 92: Batch Log Error Codes

Error #	Name	Description
3	Invalid erl id	The format of the ERL ID is invalid.
4	Invalid ip address	The format of the Switch IP Address is invalid.
6	Invalid snmp port	The format of the SNMP Port is invalid.
7	Invalid port name	The format of the Switch Port Name is invalid.
8	Invalid switch community string	The format of the SNMP Community String is invalid.
9	Port name already exists	The Switch Port Name is already assigned.
10	Ip not found in batch file	The Switch Port ID could not be associated to a corresponding switch ID.
12	Invalid csv header	'Invalid CSV Header. The following CSV header is not valid: '
13	Missing csv header	'Missing CSV Header. The following CSV header is missing: '

14	Invalid csv value	'The following value is invalid for the specified CSV header: '
15	Duplicate csv header	'Duplicate CSV header. The following CSV header is a duplicate of another CSV header: '
16	Invalid switch vendor name	Invalid switch vendor name. Switch vendor name allows all alphanumeric characters, including spaces between 1 and 25 characters.
17	Invalid SNMP version	The SNMP version is invalid. Possible values: 1, 2c or 3.

13.4.6 Text batch file format

The text batch file must be semicolon delimited and includes the fields listed below. The fields must be situated in the following specific order:

Note: Please be aware that Text Batch file format mode only supports V1/V2c and does not allow the updated parameters such as Switch Type, Log Level, etc. These parameters will be set to their default values in the text batch file.

- Switch IP address
- SNMP version
- SNMP Community String
- SNMP port
- Switch Description
- Switch vendor name
- ERL ID
- Switch Port Name



Note: If using the text batch file, the value “Scan Enabled” is set to 1 by default. This enables the EGW to scan the switches using SNMP. To batch provision switches that will be scanned using Third Party SNMP tools, use the CSV batch file format instead.

Furthermore, text files do not support SNMP v3.

The following table describes each of these fields in greater detail:

Table 93: Switches Batch File Format

Position	Field Name	Description	Req?
1	Switch_IP	The IP address of the switch. Alphanumeric.	Y
2	SNMP Version	The SNMP protocol version 1, or 2c. Default is version 2c.	N
3	SNMP Community String	String that acts as a password to authenticate messages sent between the management station (the SNMP manager) and the device (the SNMP agent). Special characters are accepted and must be 25 characters or less. The default value is set in the database as “public.”	Y
4	SNMP Port	Standard SNMP port. Numerical value. Default value is port 161. Must be a numeric value between 1-65535.	N
5	Switch Description	Description of the switch. Alphanumeric. No limits.	N
6	Switch Vendor Name	Switch Vendor name. Alphanumeric between 1 and 25 characters.	N
7	ERL ID	Emergency Response Location Identifier. Alphanumeric between 1 and 31 characters in length.	Y

Position	Field Name	Description	Req?
8	Switch Port Name* *Case sensitive	The port of the switch in the row. NOTE: Use the wildcard (*) to add a switch. Use the switch port name to create a switch port entry in the network map. Alphanumeric up to 50 characters. Only necessary if the switch port you are uploading requires an ERL ID other than the Default ERL ID for the switch.	Y

Batch uploads for network switches include only two possible operations:

- Switch creation
- Switch port creation

Batch File Examples

The following lines are an example of a batch file to upload switch data:

```
192.168.0.202;;public;161;;LOC_X;*
192.168.0.202;;public;161;;LOC_X;Fa1/1
192.168.0.202;;public;161;;LOC_X;13
```

- The first line of the batch will insert a switch with an IP address of 192.168.0.202. The second line will add the switch port Fa1/1 to ERL ID LOC_X. The third line adds switch port name 13 to ERL LOC_X.

```
192.168.0.92;;public;;;LOC_X;*
```

```
192.168.0.92;;public;;;LOC_X;Fa1/4
```

- It is possible to skip un-required fields by leaving them blank and inserting a semicolon.

Batch File Format Structure

The batch file format must observe the correct structure. Failure to observe the structure will result in error codes and the entries will have to be uploaded again. Batch files are capable of uploading switches and switch ports.

The order in which switches and switch ports are entered in the batch file is determined by the batch file format structure.



Note: Structural restrictions only apply to the scenario where switch ports are uploaded in a batch. This is done to add switch ports to a different ERL ID than the default ERL ID for the switch. If all of the ports on the switch will use the same ERL ID, it is not necessary to specify ERL IDs on a per-port basis.

The structure of the batch files must observe the following rules:

1. All switches are entered first. All switch ports follow. e.g.

Switches:

- 192.168.0.202;;public;161;;LOC_X;*
- 192.168.0.203;;public;161;;LOC_X;*
- 192.168.0.204;;public;161;;LOC_X;*

Switch ports:

- 192.168.0.202;;public;161;;LOC_4;9
- 192.168.0.203;;public;161;;LOC_5;Fa3/2
- 192.168.0.203;;public;161;;LOC_6;Fa3/3

2. A switch port is entered. Any ports that correspond to an ERL ID other than the default ERL ID follow. e.g.

Switches and Ports:

- 192.168.0.202;;public;161;;LOC_X;*
- 192.168.0.202;;public;161;;LOC_Y;9
- 192.168.0.203;;public;161;;LOC_X;*
- 192.168.0.203;;public;161;;LOC_Y;Fa3/2

- 192.168.0.203;;public;161;;LOC_E;FA3/3



Warning: It is not possible to upload a batch file that **only** includes switch ports. The file must also include a switch or switches.



Warning: It is not possible to upload a file where switch port entries precede switch entries.

Text Batch Logs

Batch log files report on the success or failure of each entry in a submitted batch file. The batch logs are generated in response to the following actions:

- Validate
- Batch Process

To view the batch logs:

- Click on **Auto Discovery > Layer 2 Discovery > Batch Upload.**

The columns of the Batch Logs display the following information:

- Original File Name
- Log File
- Log Date
- Status
- Actions (Validate, Delete, Batch Process*)

To view a log file, click on **View Log File** under **Log File**.

The log file provides a status report for each line of the processed batch file. A line will contain an error code followed by the original line in the batch file. If the operation was executed successfully, the error code will be set to 00. If the operation failed to complete successfully, the error code will be larger than 00.

The following table details each possible outcome resulting from a single operation.

Table 94: Batch File Result Log Error Codes

Error #	Description
00	The entry is successful.
01	The entry does not have the right number of fields.
03	The format of the ERL ID is invalid.
04	The format of the Switch IP Address is invalid.
05	The format of the SNMP Port is invalid.
06	The Switch IP Address is already assigned.
07	The format of the Switch Port Name is invalid.
08	The format of the SNMP Community String is invalid.
09	The Switch Port Name is already assigned.
10	The Switch Port ID could not be associated to a corresponding switch ID.
16	Invalid switch vendor name.
17	The only valid choices for SNMP version are 1 and 2c.

Log File Examples

00; 192.168.0.92;;public;21;FourthFloorSwitch;Vendor;LOC_X;*

- The switch was successfully added to the EGW.
- The switch 192.168.0.92 was assigned to ERL LOC_X.

00; 192.168.0.92;;public;21;FourthFloorSwitch;Vendor;LOC_Y;2

- Switch port 2 was successfully added to switch 192.168.0.92.
- Switch port 2 was assigned to ERL LOC_Y.

13.5 Scans

Scans can be run manually or they can be scheduled. The Layer 2 Discovery Manager manages both the manual and scheduled scan jobs. Also, it manages both regular and 3rd party scanning jobs.

13.5.1 Scan Jobs

The scan jobs screen provides a report of each scan that is processed by the Layer 2 Discovery Manager. For each scan it is possible to view the following status information.

Table 95: Layer 2 Scan Jobs

Parameter	Description	Note
Job ID	Unique Job ID assigned by Scan Manager to the scan job.	
Job Type	Scan Type: Manual or Scheduled	
Job Log Level	Logging Level applicable to the scan job	
Task Log Level	Logging level applicable to the task associated with a scan.	
Status	Status applicable to the scan job and a message associated with it. For example: Layer2 Job Complete. Layer2 Scanning completed successfully.	
Log File	Scan Job Log File.	
Scan Progress	Indicates if a scan is completed or not. For example: 1/1 means there was one scan job in progress and it has been completed.	
Number of Concurrent SNMP Connections	This field indicates the value of this parameter when this job is being executed. For more information, see section 13.4.1 “Global.”	
Submit Endpoint File	This field indicates the value of this parameter when this job is being executed. For more information, see section 13.4.1 “Global.”	
Submit Endpoint File on Failure	This field indicates the value of this parameter when this job is being executed. For more information, see section 13.4.1 “Global.”	
Start Time	Start time of the scan job.	
End Time	End time of the scan job.	
Duration	Amount of time that has elapsed from the start time to the end time of the Layer 2 scan process.	
Actions	Column that enables you to perform actions on the scan jobs: • Delete	

13.5.2 Creating a Job Manually

To manually create a scan job:

1. Click on **Auto Discovery>Layer 2 Discovery>Scan**
2. Click on **Create Job**.
3. Configure the scan using the scanning parameters defined in the table.

Table 96: Creating Scan Job

Parameter	Description	Note
Switches to scan	From the dropdown, place a checkmark next to the switches that you would like to scan. The Filter field allows a subset of switches to be listed and selected, by entering a partial IP address for example.	
Log Level	Allows overriding the Global Log Level for the duration of this scan. For more information, see section 13.4.1 “Global.”	
Number of Concurrent SNMP Connections	Setting which will override the Global setting on a per scan basis. For more information, see section 13.4.1 “Global.”	
Submit Endpoint File	Setting which will override the Global setting on a per scan basis. For more information, see section 13.4.1 “Global.”	
Submit Endpoint File on Failure	Setting which will override the Global setting on a per scan basis. For more information, see section 13.4.1 “Global.”	

4. Click on **Save**.
5. The scan job is added to the Scan Manager Queue with status of “Queued.”

13.5.3 About Layer 2 Discovery Logging

There are multiple levels of logging for Layer 2 Discovery

- Scan jobs logs
- Scan tasks logs

Scan Jobs:

On the scan screen is it possible to view the scan job logs that correspond to a specific Scan Job ID. These logs output the results of the scanning jobs, indicating the ports and ERLs, discovered forwarding MACs and other information pertaining to an EGW Layer 2 scan.

These logs are controlled by the Logging level setting at **Auto Discovery>Layer 2 Discovery>Global**.

Scan Tasks:

By expanding a specific Job ID you can see the individual switches that were scanned and the scan task logs, on a per-switch basis. These logs output the results of the scanning tasks as the EGW uses SNMP to interrogate the switches.

These logs are controlled by the Logging level setting that can be set on a per-switch basis.

Debug Logs:

The EGW also provides an interface to collect application logs at **System Status>Logs>Debug Logs**.

At this screen, debug log levels can be set for layer 2 Discovery.

This setting can be used to override the settings for both scan jobs and scan tasks.

For more information, see section 18.3 "Logs."

13.5.4 Creating a Layer 2 Discovery Scheduled Task

To run layer 2 discovery as a scheduled task:

1. Provision the ERLs inventory. For more information see section 11 "Emergency Response Locations (ERLs)."
2. Add the layer 2 switch details for the network. For more information, see section 13.4 "Configuring Layer 2 Discovery."
3. Configure the task scheduler to run the layer 2 discovery task periodically.

13.6 3rd Party Scanning

You can use a third-party scanning tool to load the EGW with endpoint location information. The data can be uploaded to allow the EGW to track the location of the endpoints.

To use 3rd party scanning you need to have endpoints already provisioned in the EGW. In addition, you must load the switches data and external scanning data into the EGW. The layer 2 switch information provides a representation of your layer 2 network which is associated to the emergency locations in the EGW. The external scanning data is processed in the EGW, and enables the EGW to track the endpoints on the network.

13.6.1 Loading 3rd Party Scanning Data

You can manually create a 3rd party processing job by uploading a batch file using the Dashboard. The Layer 2 Discovery Scan Manager processes this data using a scan job.

You can also use FTP or SOAP interface to load 3rd party Layer 2 data into the EGW that will be processed using a scheduled task **Batch 3rd Party Layer 2**.

- **Administrative Dashboard:** A batch file is uploaded using the EGW Dashboard interface. The Layer 2 Scan Manager will then process this data using the next available scan job.
- **FTP/SOAP:** The file is uploaded via FTP or SOAP. It is validated and processed based on the settings of the Scheduled Tasks: "Batch 3rd Party Layer 2," and "Layer 2 Scheduled 3rd Party."

13.6.1.1 Dashboard

To upload a batch file via the Dashboard interface

1. Prepare the batch file in accordance with the batch file format.
2. Click on **Auto Discovery > Layer 2 Discovery > 3rd Party**
3. Click on **Import**.
4. Locate the 3rd party file and add it to the Upload screen
5. Set the "Log Level" and "Process Endpoint Files Automatically" settings as required
6. Click on **Start Upload**
7. Click on **Validate.***
8. The Log File is displayed in the Import Switches Dialog Window
 - a. If the batch log file does not include any errors you may move ahead to the processing stage by clicking **Import**. Then click on **Save**.
 - b. If the batch log file contains errors, you may correct them before attempting another validation.

*When you click **Validate**, the batch file is validated and a log file is generated. The log file reports the success or failure of each entry in the batch file. If there are errors you must correct them before moving ahead to the processing stage.

9. Click on **Start Scan**. The 3rd Party Layer 2 scan job is queued and will be processed as soon as the Layer 2 Discovery Manager becomes available.

13.6.1.2 FTP

To batch upload via FTP:

1. Open a FTP connection to the EGW using the IP of the EGW, username: batchsnmp, password: 911batch.
2. Go to the **batch** directory.
3. Upload the file to the EGW.

Batch files uploaded to the EGW using FTP are governed by scheduled tasks settings. The scheduled task **Batch 3rd Party Layer 2** controls the settings for when batch processing will occur.



Note: After a batch file uploaded to the EGW via FTP is processed, it is automatically removed from the FTP directory. These files can be viewed using the Dashboard interface.

FTP Batch results

The batch logs summary and error reports are sent to the email addresses configured at **Configuration > Advanced > Batch Settings**. Logs can also be viewed from the Dashboard.

13.6.1.3 SOAP

To use the SOAP interface:

1. Upload 3rd party Layer 2 data to the EGW as described in document EGW SOAP Server Interface Description."

3rd party Layer 2 data added to the EGW using SOAP is processed by the scheduled task "Layer 2 Scheduled 3rd Party."

For more information, see the document "EGW SOAP Server Interface Description."

13.6.2 3rd Party Scan Batch File Format

The batch file for third party snmp tools uses CSV and must be in the following format:

Table 97: 3rd Party Scan Batch File Format

CSV Header	Description	Required
OPERATION	Value: 1 = Add or update 2 = Delete	Y
SWITCH_IP	Unique IP Address for the switch or fully qualified domain name (FQDN).	Y
PORT_NAME	Port Name	Y
MAC	Device(s) connected	Y
Timestamp	Time at which the row is updated.	N

Example of valid CSV 3rd party SNMP batch file:

```
"OPERATION","SWITCH_IP", "PORT_NAME", "MAC"
"1","192.168.0.240", "Fa0/1", "001AF5E882A9, 001AF5E882B0, 001AF5E882B1"
"2","192.168.0.240", "Fa0/2", "001AF5E882A1, 001AF5E882A2, 001AF5E882A3"
```

13.6.2.1 Batch Logs for External Scan

Batch log files report on the success or failure of each entry in a submitted batch file. The batch logs are generated in response to the following actions:

- Validate

To view the batch logs

- Click on **Auto Discovery > Layer 2 Discovery > 3rd Party**
- Expand the Job ID of the 3rd Party Layer 2 Scan Job. The log file is displayed.

The columns of the Batch Logs display the following information:

- File Name
- Log File (Click on the log file to open the .csv file to review)
- Log Date
- Status
- Actions (Validate, Delete, Batch Process*)

Viewing a Batch Log File

To view a log file, click on **View Log File** under **Log File**.

The batch file results returned in the log file are displayed in CSV format. The results include an error code and description followed by the original line in the batch file entry:

"error code", "error description", "SWITCH_IP", "PORT_NAME", "MAC"

"3", "supported file extensions are text or csv", "192.168.0.240", "Fa0/1", "001AF5E882A9, 001AF5E882B0, 001AF5E882B1"

"7", "Duplicate csv header", "192.168.0.240", "Fa0/1", "001AF5E882A9, 001AF5E882B0, 001AF5E882B1"

View Peer

If **Log File** displays **View Peer**, you must login to the Peer in order to view the log file. This scenario occurs when a batch file is processed by the Peer machine.

The following table details each possible outcome resulting from a single operation.

Table 98: Batch Log File Messages

Error #	Name	Description
1	Invalid row number	'Entry does not include the correct number of fields.'
2	Invalid operation	'Operation entered is invalid.'
3	Invalid file type	'Supported file extensions are .txt or .csv'
4	Invalid csv header	'Invalid CSV Header. The following CSV header is not valid: '
5	Missing csv header	'Missing CSV Header. The following CSV header is missing: '
6	Invalid csv value	'The following value is invalid for the specified CSV header: '
7	Duplicate csv header	'Duplicate CSV header. The following CSV header is a duplicate of another CSV header: '
8	Db_asynch problem	'The SNMP batch DB was modified during the processing of this file. The row has been skipped to avoid conflicting entries.'
9	SNMP_BATCH_ROW_DOESNT_EXISTS	The specified SNMP batch row does not exist

13	Layer 2 switch is set to scannable	The file contains a switch that is set to be scannable by the Layer 2 engine.
----	------------------------------------	---

13.6.3 Discovered Ports

You can use the Discovered Ports screen to review the discovered switch ports and MAC addresses of all of the EGW scanning jobs (both regular and 3rd party scans).

This page provides an overview of your network as discovered by the EGW's Layer 2 Discovery and 3rd party external Layer 2 scan. It shows every discovered port and, when applicable, lists all MAC addresses reachable from these ports. All MAC addresses are listed, not only those associated to known endpoints. This page is useful to diagnose occasional trunk port or MAC address discovery issues.

The screen displays a list of all the switches and ports discovered by EGW with the parameters defined in the following table:

Table 99: Discovered Ports Field Descriptions

Parameter	Description	Notes
Switch IP	Switch IP for the switch port.	
Number of MAC's Discovered	Number of MACs that were discovered on the switch port during the scan.	
Switch Port Name	Name of the switch port. Eg. Fa0/1	
Port Base Number	Port Base Number for the switch port.	
ERL ID	ERL ID for the switch port.	
Port Type	Field that reports the Port Type for the switch port. The following port types are possible: 0 = Not Trunk 1 = Trunk Discovered By Scanning 2 = Trunk - Manual 3 = Uplink Discovered By Scanning	
Last Update	Date and time at which the switch port was last updated by a scan job.	

13.6.3.1 MAC Results

You can click on the switch of choice to review the current status of all the MAC addresses (endpoints) that have been discovered on the switch.

To view the MACs:

- Expand the switch IP of the Switch Port
- Optionally: Use the Search field to filter for:
 - Partial or complete IP address
 - Partial or complete MAC address.
 - Partial or complete port name
 - Partial or complete ERL ID

For each discovered MAC the following information is displayed

Table 100: Discovered MACs on Port Information

Field	Description	Note
-------	-------------	------

MAC address	Discovered MAC address	
Failure Count	This field reports the current failure count. MAC addresses that fail to be discovered on the network are set to call center mode after the configured failure count has been exceeded. This failure count depends on the MAC address ageing tables of your switches and the way they have been setup.	On occasions, MAC addresses associated to active endpoints may show a non-zero failure count. This could be an indication that the switches MAC address cache table is using an ageing timeout shorter than the phone's registration period.
Active	This field will report if the MAC is active or not on the network. Useful for troubleshooting purposes.	
Last Update	Date and time at which the switch port was last updated by a scan job.	

13.7 Export Layer 2 Switch Details

Use the Reports screen to create layer 2 switch export files for your own use, for example, to back up or move a configuration. Layer 2 switches are exported from the EGW by generating a report. The report is a semicolon delimited batch file that may be re-imported using the Dashboard.

To generate a Layer 2 Switches report:

- Click on **System Status > Reports** and select **Switches and Ports**.

You can either export an Export Batch or Export Batch CSV

For more information, see section 18.4 “Reports.”

13.8 Troubleshooting Layer 2 Discovery

This section lists the most commonly seen issues in the field.

13.8.1 Undiscovered Switch Ports

Batch file provisioning may be used to assign switch ports to different ERLs than the default ERL for the switch. If this method will be used, it is important to verify that the switch port name entered in the batch file matches the switch port name on the switch. If the switch port names do not match, the batch file entry will fail, and the switch port will be assigned a status of undiscovered. A common error occurs when Gigabit Ethernet ports are incorrectly labeled as fast Ethernet ports, for example.

Undiscovered switch ports appear in the **Undiscovered Switch Ports Count** located at **System Status > Status > General Information**.

To resolve undiscovered switch ports

- Consult the switch to find the correct name.
- Locate the incorrect switch port name on the Dashboard (**Auto Discovery>Layer 2 Discovery>Switch**). It will be associated to the default ERL ID.
- Change the switch port name and the ERL ID to the appropriate settings.

For more information concerning ongoing responsibilities, see the document “EGW Appliance Standard Operating Procedures.”

13.8.2 Undiscovered Phones

There are some cases where a phone can actually be connected to a “**Trunk Port**”. Cisco switches assume that any port that does VLAN tagging is a **trunk port**, but some phones actually support VLAN tagging. In this case, the EGW will not find this phone’s MAC address on any access port.

To resolve this condition, the EGW will look for the port that only has the **Trunk Port** status and not the **Uplink port** status. Hopefully there will be only one. If there are more than one, some **Manual Trunk ports** may need to be configured.

13.8.3 Endpoint gets associated to wrong location

Possible causes:

- Switch where endpoint is connected has not been configured and MAC was detected on upstream trunk port.
- MAC was found on two or ports: Could be caused by an endpoint that moved to a different port but maximum failure count has not been reached.
- A trunk port is not getting appropriately detected. Manually configure port as trunk port.

14 Layer 3 Discovery

14.1 Understanding Layer 3 Discovery

The EGW uses Layer 3 discovery to determine the location of a phone based on its IP subnet. This capability simplifies administration for enterprises with subnets that correspond to physical locations e.g. A subnet per floor.

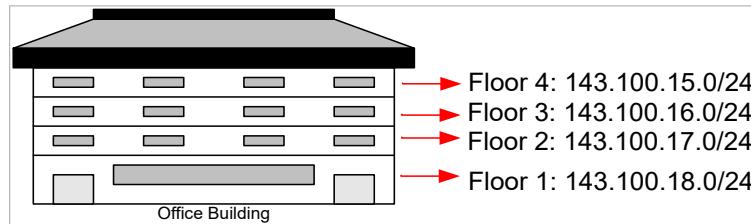


Figure 51: Layer 3 Discovery

14.2 Provisioning Subnets

To enable Layer 3 discovery, you must first create a layer 3 network map that associates your IP subnets with your ERLs. Subnets may be configured one at a time, or multiple subnets may be configured simultaneously using batch file uploads.

It is possible to summarize your networks when provisioning the EGW with subnets, because the EGW will always find the most granularly defined subnet/ERL association at call time.

14.2.1 Provisioning Subnets Individually

To upload subnets one at a time

1. Click on **Auto Discovery** → **Layer 3 Discovery** → **Add Subnets**.
2. Enter the appropriate ERL ID and the subnets that you would like to add*.

*It is possible to associate multiple subnets per ERL ID.

14.2.2 Provisioning Subnets in a Batch

EGW accepts batch provisioning of subnets using a text batch file as well as a CSV batch file.

You can batch provision subnets using:

- **Administrative Dashboard:** A batch file is uploaded using the EGW web interface. The file is validated and processed in real-time.
- **FTP:** The file is uploaded via ftp. It is validated and processed based on the settings of the Scheduled Task.

When uploading a batch file, the Batch Subnets are incrementally added and the batch file is validated as follows:

1. The ERL ID is validated to ensure that it exists.
2. The batch file is read to ensure that a Subnet entry does not appear more than once. In other words, the Subnet entry must be unique.

When the above validation steps pass, the batch processing functions as follows:

1. If the Subnet address does not already exist in the database, it is now added.
2. If the Subnet address already exists in the database and is associated with the same ERL ID (as in the text file), then the entry is simply ignored and no action is performed.

If the Subnet Address already exists in the database and is associated with a different ERL ID (as compared to the batch file), then the entry in the batch file takes precedence and the database is over-written.

Note: Please note that the entry in the batch file take precedence over the information that is already in the database.

14.2.2.1 Subnet Batch File Processing Mechanism

To upload a batch file via the Dashboard interface

1. Prepare the batch file in accordance with the batch file format. See [14.2.2.1 Text format for Batch File](#) for text files or [14.2.2.2 CSV format for Batch File](#) for CSV files.
2. Click on **Auto Discovery** → **Layer 3 Discovery** → **Batch Upload**.
3. Click on **Choose File** under **Subnets Batch Upload**. Browse and upload the file.
4. Click on **Upload**.

The subnet batch file is processed one line at a time and the operation specified is executed. The batch file is read and processed completely even if an error is detected. If any errors are detected, the erroneous line is detected and captured in the Error Log File. See [14.2.3.2 Error Log File](#).

In addition, the results of the batch process is also captured in the Log File. For more information on the Log File, please refer to section [14.2.3.1 Log File](#).

To batch upload via ftp

1. Open an ftp connection to the EGW using the IP of the EGW, username: batchsubnet, password: 911batch.
2. Go to **batch** directory.
3. Upload the file to the EGW.

Batch files uploaded to the EGW using ftp are governed by scheduled tasks settings. The scheduled task **Batch Subnets** dictates precise daily intervals at which batch processing will occur.

Note: After a batch file uploaded to the EGW via ftp is processed, it is automatically removed from the ftp directory. These files can be viewed using the Dashboard interface.

FTP Batch Results

The batch logs summary and error reports are sent to the email addresses configured at **Configuration** → **Advanced** → **Batch Settings**. Logs can also be viewed from the Dashboard.

14.2.2.2 Batch File Format

EGW accepts batch provisioning of subnets using a text batch file as well as a CSV batch file. Before a batch file is uploaded it must be prepared in accordance with the batch file format.

14.2.2.1 Text format for Batch File

If you wish to upload a batch file in text format, then the fields must be semicolon delimited and in the following order:

Table 101: Subnets Batch File Format

Position	Field Name	Description	Required?
1	ERL ID	Unique identifier of the location. Alphanumeric between 1 and 31 characters in length.	Yes
2	Subnet	The subnets for the location, comma delimited for multiple entries. Must be in CIDR notation: 192.160.0.0/16, 192.160.10.0/24. Subnets must be unique throughout all locations. An error will be generated if a subnet is submitted which already exists in another location.	Yes

Text batch file example

LOC_X;192.160.10.0/24,192.160.11.0/24,192.160.12.0/24

In the above example, the batch file associates the subnets to ERL LOC_X

14.2.2.2.2 CSV format for Batch File

The following are the fields required to batch provision subnets:

Table 102: Required Fields to Batch Provision Subnets

CSV Header	Description	Required
OPERATION	1 for Add/ Update 2 for Delete	Yes
ERL_ID	A valid, existing ERL ID.	Yes
SUBNET	One or many comma delimited valid subnets. Each subnet is	Yes (not required for the delete operation)

If the Subnet is not provided for then all subnets belonging to the specified ERL ID are deleted.

CSV Batch File Example:

	A	B	C
1	OPERATION	ERL_ID	SUBNET
2		1 LOC100	192.168.59.0/24

Figure 52: CSV Batch File Example

In the above example, the subnet 192.168.59.0/24 is being associated to the ERL LOC100.

14.2.3 Layer 3 Batch Logs

Batch log file reports on the success or failure of each entry in a submitted batch file in response to the Batch Process operation.

To view the batch logs

- Click on **Auto Discovery** → **Layer 3 Discovery** → **Batch Upload**.

The columns of the Batch Logs display the following information:

- Original File Name
- Log File
- Error Log File
- Log Date
- Status
- Actions (Batch Process and Delete)

14.2.3.1 Log File

To view a log file, click on **View Log File** under **Log File**.

The log file provides a status report for each line of the processed batch file. The line will contain a response code followed by the original line in the batch file. If the operation was executed successfully, the response code will be set to 00. If the operation failed to complete successfully, the response code will be anything other than 00.

*Note: If **Log File** displays **View Peer**, you must login to the Peer to view the log file. This scenario occurs when a batch file is processed by the Peer machine.*

14.2.3.2 Error Log File

To view the log error file, click on **View Log File** under **Error Log File**.

The **Error Log File** is only generated when an error was detected in the log file and an entry could not be processed. The lines in this file will contain a response code followed by the original entry that could not be processed.

14.2.3.3 Response Codes

Response codes returned in the Log File and the Error Log File vary depending on whether you batch uploaded a CSV file or a text file.

14.2.3.3.1 Text Batch Response Codes

The following table details each possible outcome resulting from a single operation.

Table 103: Text Batch Response Codes

Response Code #	Description
00	The entry is successful.
01	The entry does not have the right number of fields.
02	The format of the ERL ID is invalid.
03	The format of the subnet is invalid.
04	One of the subnets is already assigned to this ERL ID.
05	One of the subnets is already assigned to a different ERL ID.

Log File Examples

00;LOC_X;192.168.10.0/24,192.168.11.0/24,192.168.12.0/24

- The subnets were successfully uploaded to the EGW.

05;LOC_Y;192.168.13.0/24,192.168.14.0/24,192.168.11.0/24

- One of the subnets is already assigned to a different ERL ID.

14.2.3.3.2 CSV Batch Response Codes

The following table details each possible outcome resulting from a single operation.

Table 14-104 Text Batch Response Codes

Table 105: CSV Batch Response Codes

Response Code #	Description
0	<u>_SUCCESS_</u> Successfully processed entry.
1	<u>_INVALID_ROW_NUMBER_</u> Entry does not include the right number of fields.
2	<u>_INVALID_ERL_ID_</u> The following value is invalid for specified CSV header: ERL_ID

3	_INVALID_SUBNETS_ <value of Subnet> is invalid
4	_SUBNET_EXISTS_ <value of Subnet> is already assigned more than once to this ERL.
5	_SUBNET_EXISTS_IN_OTHER_ERL_ <value of Subnet> already assigned to another ERL in file.
24	_INVALID_OPERATION_ The following value is invalid for the specified CSV header: OPERATION
40	_INVALID_CSV_HEADER_ Invalid CSV Header. The following CSV header is not valid: <CSV header value>
41	_MISSING_CSV_HEADER_ Missing CSV Header. The following CSV header is missing: <CSV header value>
46	_DUPLICATE_CSV_HEADER_ Duplicate CSV header. The following CSV header is a duplicate of another CSV header: <CSV header value>

14.3 Export Layer 3 Discovery Details

Through the EGW dashboard, you can also export the Layer 3 discovery details of your organization's network configuration. This is useful if you wish to back up or edit your network configuration.

These reports can be downloaded in the form of text files or CSV files.

To download subnet reports:

1. Go to **System Status** → **Reports**.
2. Under **Select Reports**, choose **Subnets** from the dropdown menu.
3. Under **Report Type**, choose between **Export Batch** and **Export Batch CSV**.
4. Click **Generate Report**.
5. Click **Download Report**.

For more information, see section [18.4 Reports](#).

15 WLAN Discovery

The EGW can automatically track wireless IP phones and softphones using WLAN Discovery. This capability provides for a high level of location granularity for wireless deployments, by allowing ERLs to be assigned to the nearest access point.

In the diagram below, all wireless endpoint discovered by a WLAN scan are assigned an ERL based on the access point (AP A, AP B, AP C) to which they are attached.

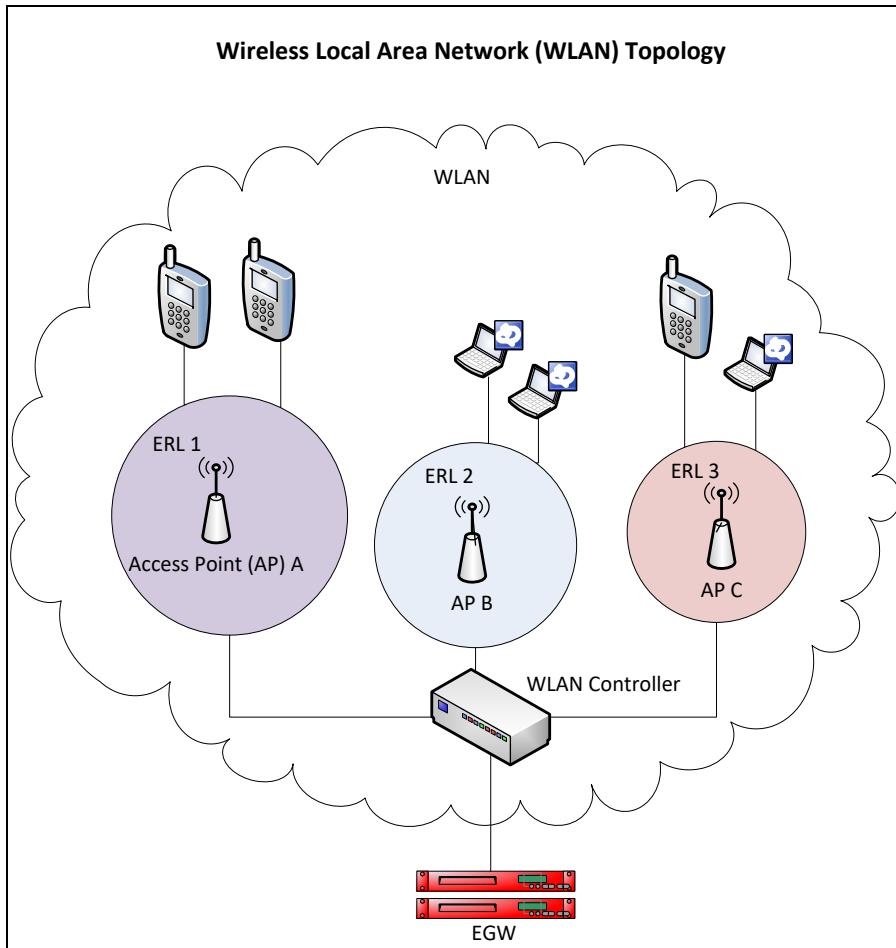


Figure 53: WLAN Discovery

15.1 WLAN Scanning and WLAN Discovery Mechanism

The WLAN scanning mechanism controls the actual scanning of controllers and access points contained in an organization's network. On the other hand, WLAN Discovery is a two-step process involving WLAN Scanning, followed by the processing of the scanned information. The actual processing involves assigning ERLs to endpoints.

The second part of the WLAN discovery process happens irrespective of whether the WLAN scanning is enabled or not. If WLAN Scanning is not enabled, the WLAN discovery process simply skips the scanning part and moves on to process the previously scanned information or the information discovered through the ESL process.

WLAN Scanning can be enabled or disabled using the dashboard. To edit WLAN Scanning settings:

1. Access the EGW dashboard.

2. Go to **Auto Discovery** → **WLAN Discovery** → **Global**.
3. Click on the **Edit** button.

The **Edit Global Settings** window appears.

4. Here, you can choose **Yes** or **No** from the dropdown menu to enable or disable WLAN Scanning.

In addition, scanning of individual wireless controllers can also be enabled or disabled using the **AP Scan** checkbox in the **Controllers** page. When the **AP Scan** is enabled but the **WLAN Scanning** is disabled, the scanning process will not take place. On the other hand, when the **WLAN Scanning** is enabled, the scanning process will take place only for the APs for which the AP Scan is enabled.

It is very important to note that other than the WLAN scanning process, only the ESL mechanism is capable of discovering wireless endpoints.

WLAN discovery depends on a mapping of your wireless controllers and access points to Emergency Response Locations (ERLs). In this map, the BSSIDs of the access points are associated to your ERL records. Once the WLAN map has been loaded into the EGW configuration, WLAN Discovery works either by scanning the access points or by using the E911 Softphone Locator.*

*Please refer to ESL specifications to determine if wireless discovery using ESL will meet the requirements of your network.

When a wireless phone is discovered in a WLAN scan, it is assigned an ERL record, based on the BSSID of the wireless Access Point to which it is attached. In E911 Softphone Locator deployments*, the ESL periodically sends information about the wireless endpoints to the EGW, including the BSSID of the current Access Point, removing the need to scan the access points.

*For ESL wireless discovery to work, the wireless endpoints behind the controller must support the ESL software.

It is very important to note that even if WLAN scanning is disabled, the WLAN discovery process can still process wireless endpoints.

15.1.1 WLAN Discovery Task

The WLAN Discovery task is enabled or disabled when the controller is added or deleted, respectively.

When a new controller is added, the WLAN discovery task is automatically enabled. This is to ensure that the information obtained from the newly-added controller is processed.

Conversely, when the existing controllers are deleted, the WLAN discovery task automatically becomes disabled.

The WLAN Discovery task can also be enabled or disabled using the dashboard.

To manually enable the WLAN Discovery task:

1. Go to **Configuration** → **Task Scheduler**.
2. Scroll down to the **Wlan Discovery** and click on **Edit**.

From the **Edit Task** page, the **Task Disabled** flag can be edited to disable (set to **Yes**) or enable (set to **No**) it.

15.1.2 Understanding WLAN Discovery and Layer 2 Discovery Interactions

Many of today's IP communications endpoints support both wired and wireless modes of operation. The EGW can be configured to appropriately discover and track phones as they move on the network in both wired and wireless modes.

The **Layer 2 Discovery Failure Count** determines the amount of Layer 2 SNMP scans that will elapse before the EGW will change the status of an undiscovered endpoint to Call Center Mode (unprovisioned). The behavior applies to endpoints that were previously discovered by Layer 2 Discovery.

The **WLAN Discovery Failure Count** determines the amount of WLAN SNMP scans that will elapse before the EGW will change the status of an undiscovered wireless endpoint to Call Center Mode (unprovisioned). The behavior applies to endpoints that were previously discovered by WLAN Discovery.

When a phone moves from wired to wireless mode, it is discovered when the next WLAN scan runs. Likewise, when a phone moves from wireless to wired mode, it is discovered when the next Layer 2 scan runs.

Consequently, it is important to set the **WLAN Discovery Failure Count** high enough so that it allows at least one Layer 2 Discovery process to complete before it expires. If a phone has moved from wireless to wired mode, this setting will provide the EGW with enough time to discover it in the next Layer 2 scan.

Note: *The above consideration does not apply to phones supported by the E911 Softphone Locator (ESL). The ESL tracks both wireless and wired endpoints. When a phone moves from wireless to wired mode, it registers on the network and a phone provisioning data “push” is immediately sent to the EGW.**

*Please refer to ESL specifications to determine if wireless discovery using ESL will meet the requirements of your network.

15.2 Setting Up the Network for WLAN Discovery

To enable WLAN Discovery, wireless controllers and access points are added to the EGW configuration. The wireless controllers can be added to the EGW either using the web Dashboard or by uploading a batch file. During this process, it is possible to make a parameter setting that specifies if the access points associated to the controller will be scanned by the EGW. The configuration of this parameter depends on the nature of your deployment:

1. ESL-only deployments. In these deployments, the ESL is used to track IP softphones as they move on the network (eg. Microsoft Lync clients, Avaya Softphone etc.) In these deployments, there is no need to scan the access points. The ESL sends the BSSIDs of the endpoint devices to the EGW when the phones move.
2. Wireless deployments. These deployments include wireless phones, and the EGW identifies them by scanning the wireless controller access points.
3. Mixed deployments. These deployments include both ESL-supported wireless devices and other wireless phones. Wireless access point scanning is enabled.

15.2.1 Controlling Access Point Scanning

When the EGW performs scanning of access points, it looks at the configured SSID (s) and discovers the registered endpoint devices. By default, the EGW will attempt to scan each SSID on the access point. However, in some cases, certain SSIDs may not contain wireless IP phones, or be otherwise inappropriate for WLAN scanning. In these situations, it is possible to filter out the SSIDs that will be used as part of the EGW's WLAN scanning process.

For more information, see section 15.3 “Provisioning WLAN Discovery.”

The EGW also depends on the configuration of the wireless controller to determine which APs and wireless clients are rogue and which are a valid part of the network. The EGW will only scan wireless access points and clients that have been authenticated by the wireless controller.

15.2.2 Support for Cisco Mobility Services Engine (MSE)

The EGW can support integration with Cisco MSE servers for advanced location based capabilities for applications and users. The EGW is integrated with MSE to provide wireless caller location and display for Desk alert clients and crisis emails.

Network Configuration

To ensure that the EGW is able to successfully query the Cisco MSE, please ensure that Port 443 is accessible.

EGW Dashboard Configuration

The EGW needs to be configured in order to successfully integrate with the Cisco MSE system. The following steps explain the configuration:

1. Configuring **Global** Settings:

- Click on **Auto Discovery** → **WLAN Discovery** → **Global**.

The Wireless Discovery and Location Servers Global settings page will be displayed as shown below:

Figure 54: WLAN Discovery Global Settings

- Click on **Edit** to change the settings on this page.

The Intrado deployment engineer can help you with this initial setup phase.

*Note: Ensure that **WLAN Discovery Enabled** is set to **Yes**.*

2. Adding **Controllers**:

- Click on **Auto Discovery** → **WLAN Discovery** → **Controllers**.
- Click on the **Add Controller** button.

The page shown below will be displayed:

Figure 55: Adding a Controller

Your organization's IT administrator will provide you with the values for the fields shown above:

3. Adding **Location Servers**:

- Click on **Auto Discovery** → **WLAN Discovery** → **Location Servers**.

- b. Click on the **Add** button.

The page shown below will be displayed:

Location Server List	
<input type="button" value="Add"/>	

Location Server	
Server Name:	<input type="text"/>
Server Type:	<input type="text" value="Cisco MSE"/>
Timeout:	<input type="text" value="10"/>
System Management URL:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Back"/>	

Figure 56: Adding a Location Server

- The **User name** and **password** are actually created by the Cisco administrator. These will be provided to you by your organization's IT administrator.
- The **System Management URL** can be either an FQDN or an IP address. This will also be provided to you by your organization's IT Administrator.
- **Server Name** can be any arbitrary name, used only for easy identification.

When an emergency call is made, your personnel can click on a special URL link from desk Alert or Crisis Alert Emails. The following information is displayed at the URL:

- A map of the floorplan
- Icon showing the location of the caller on the map
- A visual indicator showing the 95% accuracy radius.
- The text of the received location - formatted in a user friendly method: CAMPUS:xxx, Building: xxx, Floor: xxx.
- If the page needs to be printed, the confidence area has a permanent pale grey background.

The map, area of confidence and device use regular Stylesheet CSS to display the information.

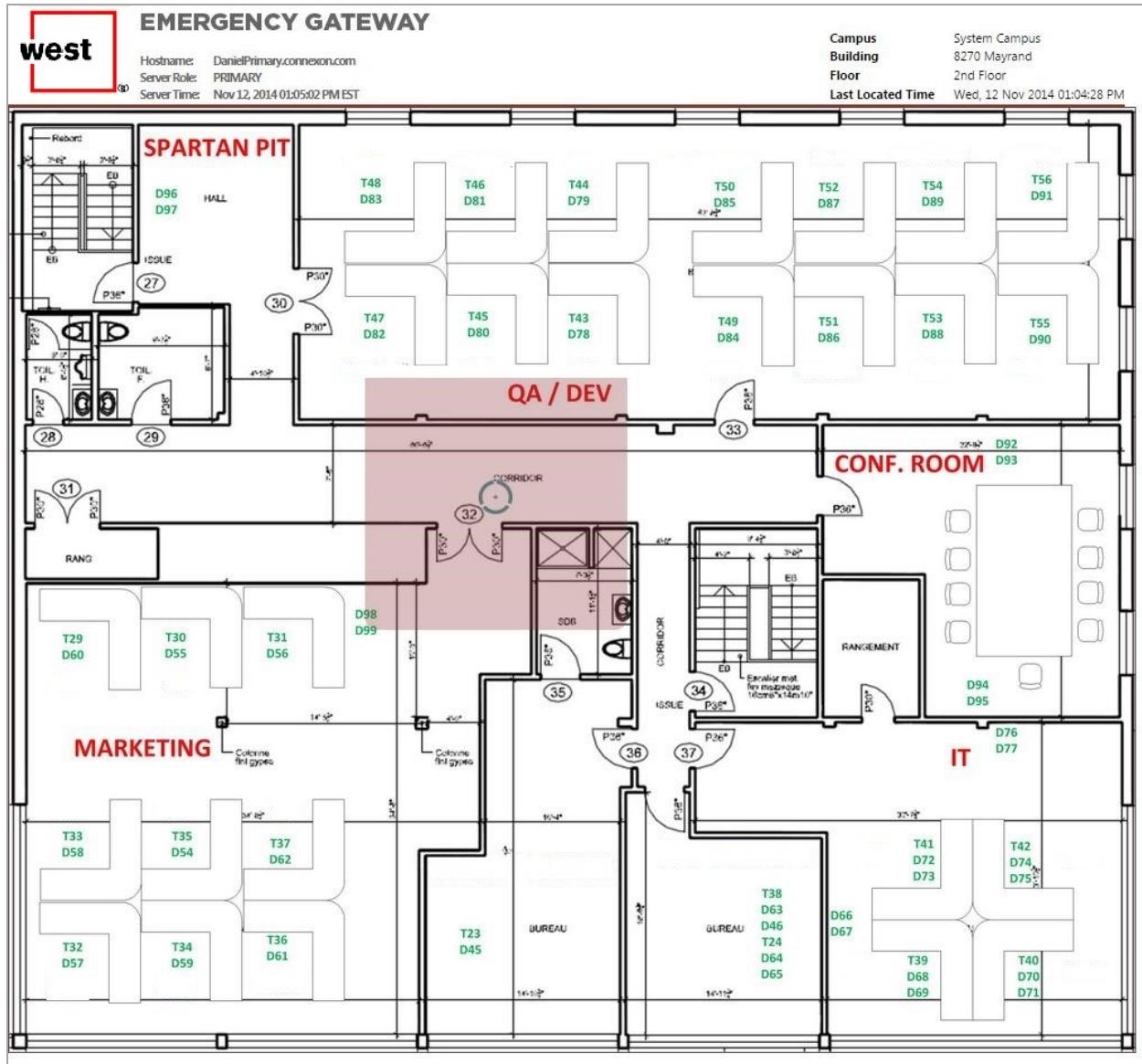


Figure 57: Map of Floor Plan

Use the configuration checklist below to configure your EGW environment for Cisco MSE support.

Configuration Checklist:

Table 106: Location Server Configuration Checklist

Configuration Task	Description	Notes/Additional Information
Provision Global settings for your location servers	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> • Ignore Locations Older Than • Authentication Token Validity Period • Map Retention Period 	See section WLAN Discovery Global Configuration.”
Add Your Location Servers	Configure Cisco MSE servers with their system management URL and credentials.	See section 15.3.6 “Adding Location Servers.”

Configure ERLs with “Wireless User Locator Enabled” set to Yes.		See section 11.2.2.2 “Add ERL Page.”
---	--	--------------------------------------

15.2.3 Support for Aruba AirWave

The EGW can support integration with Aruba AirWave Network Management System. This integration provides wireless caller location and this will in turn send crisis email alerts.

15.2.3.1 Network Configuration

The EGW is able to query the Aruba System and to provide network accurate wireless caller information by retrieving maps from the Aruba Network Management System.

To ensure seamless integration with the EGW, please be advised that Port 443 needs to be accessible.

EGW Dashboard Configuration

The EGW needs to be configured in order to successfully integrate with the Aruba ALE system . The following steps explain the configuration:

1. Configuring **Global** Settings:

- Click on **Auto Discovery** → **WLAN Discovery** → **Global**.

The Wireless Discovery and Location Servers Global settings page will be displayed as shown below:

Wireless Discovery Global Settings	
WLAN Discovery Enabled:	Yes
WLAN Discovery Failure Count:	0

Location Servers Global Settings	
Ignore Locations Older Than:	1 Hour(s)
Authentication Token Validity Period:	60 Minute(s)
Map Retention Period:	24 Hour(s)

Figure 58: WLAN Discovery Global Settings

- Click on **Edit** to change the settings on this page.

The Intrado deployment engineer can help you with this initial setup phase.

*Note: Ensure that **WLAN Discovery Enabled** is set to **Yes**.*

2. Adding **Controllers**:

- Click on **Auto Discovery** → **WLAN Discovery** → **Controllers**.
- Click on the **Add Controller** button.

The page shown below will be displayed:

Add Controller									
Controller IP	SNMP Community String	SNMP Port	Description	Vendor	Default ERL ID	AP Scan	Multi BSSID mask	SSIDs Supported	Actions
		161		Aruba		<input type="checkbox"/>	Disabled		Back Save

Figure 59: WLAN Discovery - Adding a Controller

Your organization's IT administrator will provide you with the values for the fields shown above:

3. Adding Location Servers:

- Click on Auto Discovery → WLAN Discovery → Location Servers.
- Click on the **Add** button.

The page shown below will be displayed:

Location Server List	
Add	

Location Server	
Server Name:	<input type="text"/>
Server Type:	Aruba AirWave
Timeout:	10
System Management URL:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="text"/>
Save Back	

Figure 60: Adding an Aruba Airwave Location Server

- The **User name** and **password** are actually created by the Aruba administrator. These will be provided to you by your organization's IT administrator.
- The **System Management URL** can be either an FQDN or an IP address. This will also be provided to you by your organization's IT Administrator.
- Server Name** can be any arbitrary name, used only for easy identification.

When an emergency call is made, your personnel can click on a special URL link from Desk Alert or Crisis Alert Emails. The following information is displayed at the URL.

- A map of the floorplan
- Icon showing the location of the caller on the map
- The text of the received location - formatted in a user friendly method: CAMPUS:xxx, Building: xxx, Floor: xxx.
- An approximate location of the caller is also shown on the map.

The map, area of confidence and device use regular Stylesheet CSS to display the information.

Configuration Checklist:

Table 107: Configuration Checklist of Aruba Location Server

Configuration Task	Description	Notes/Additional Information
Provision Global settings for your location servers	Configure the following parameters: Ignore Locations Older Than, Authentication Token Validity Period, Map Retention Period	See section WLAN Discovery Global Configuration."
Add Your Location Servers	Configure Aruba AirWave with their system management URL and credentials.	See section 15.3.6 "Adding Location Servers."
Configure ERLs with "Wireless User Locator Enabled" set to Yes.		See section 11.2.2.2 "Add ERL Page."

15.2.4 Support for Aruba ALE

The EGW can support integration with Aruba ALE Network Management System. This integration provides wireless caller location and this will in turn send crisis email alerts to the appropriate security personnel.

Network Configuration

The EGW is able to query the Aruba System and to provide network accurate wireless caller information by retrieving maps from the Aruba Network Management System. To ensure seamless integration with the EGW, please be advised that Port 8080 needs to be accessible.

EGW Dashboard Configuration

The EGW needs to be configured in order to successfully integrate with the Aruba ALE system . The following steps explain the configuration.:.

4. Configuring **Global** Settings:
 - a. Click on **Auto Discovery** → **WLAN Discovery** → **Global**.

The Wireless Discovery and Location Servers Global settings page will be displayed as shown below:

Figure 61: Wireless Discovery Global Settings

- b. Click on **Edit** to change the settings on this page.

The Intrado deployment engineer can help you with this initial setup phase.

*Note: Ensure that **WLAN Discovery Enabled** is set to **Yes**.*

5. Adding **Controllers**:

- a. Click on **Auto Discovery** → **WLAN Discovery** → **Controllers**.
- b. Click on the **Add Controller** button.

The page shown below will be displayed:

Figure 62: Adding a Controller

Your organization's IT administrator will provide you with the values for the fields shown above:

6. Adding **Location Servers**:

- a. Click on **Auto Discovery** → **WLAN Discovery** → **Location Servers**.
- b. Click on the **Add** button.

The page shown below will be displayed:

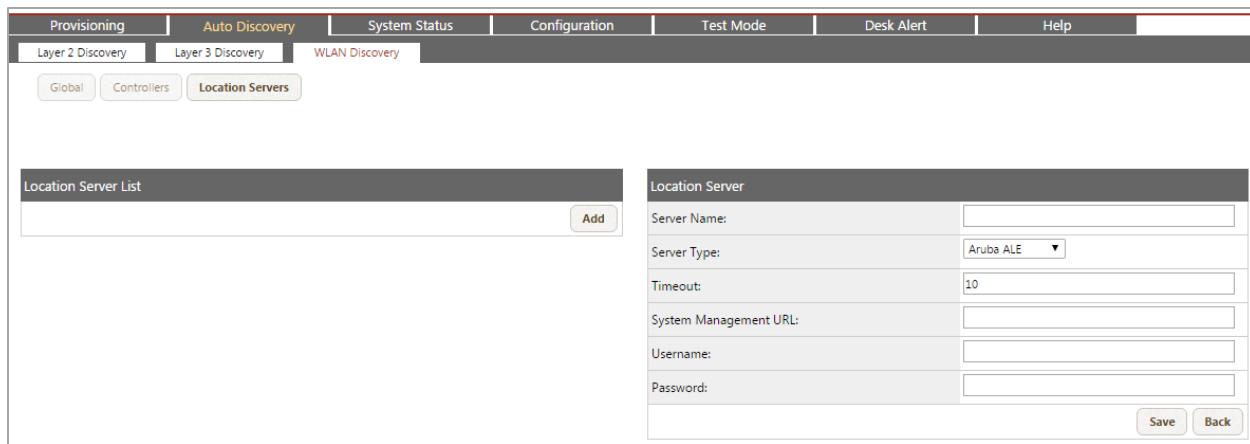


Figure 63: Adding a Location Server

- The **User name** and **password** are actually created by the Aruba administrator. These will be provided to you by your organization's IT administrator..
- The **System Management URL** can be either an FQDN or an IP address. This will also be provided to you by your organization's IT Administrator.
- **Server Name** can be any arbitrary name, used only for easy identification.

When an emergency call is made, your organization's emergency response personnel can click on a special URL link from Desk Alert or Crisis Alert Emails. The following information is displayed at the URL.

- A map of the floorplan
- Icon showing the location of the caller on the map
- The text of the received location - formatted in a user friendly method: CAMPUS:xxx, Building: xxx, Floor: xxx.
- An approximate location of the caller is also shown on the map.

The map, area of confidence and device use regular Stylesheet CSS to display the information.

Configuration Checklist

Table 108: Configuration Checklist for Aruba ALE

Configuration Task	Description	Notes/Additional Information
Provision Global settings for your location servers	Configure the following parameters: Ignore Locations Older Than, Authentication Token Validity Period, Map Retention Period	See section WLAN Discovery Global Configuration."
Add Your Location Servers	Configure Aruba ALE with their system management URL and credentials.	See section 15.3.6 "Adding Location Servers."
Configure ERLs with "Wireless User Locator Enabled" set to Yes.		See section 11.2.2.2 "Add ERL Page."

15.3 Provisioning WLAN Discovery

To enable WLAN Discovery, you must define the SNMP connection between the EGW and your wireless network, and provision the EGW with the details of the WLAN controllers and access points (AP).

If WLAN scanning is enabled for your deployment, the EGW will automatically discover access points that are added to the network. You can then assign specific ERLs to the access points, if they will be different then the default ERL assigned to the controller.

In ESL deployments, where WLAN scanning is turned off, any new Access points need to be added to the EGW configuration manually.

Note: Before provisioning WLAN Discovery information, it is necessary to have previously added ERLs to the EGW configuration. Default ERLs may not be assigned to wireless controllers unless the ERLs already exist in the configuration.

Wireless controllers and access points may be provisioned one at a time using the Dashboard, or multiple entries can be uploaded simultaneously using batch files.

15.3.1 WLAN Discovery Global Configuration

You can use the global settings to configure the wireless global settings and global settings for any applicable location servers (eg. Cisco MSE).

To configure the global settings:

1. Configure the fields, as defined in the table below:

Parameter	Description
Wireless Discovery Global Settings	
15	
WLAN Scanning Enabled	Field that enables/disables WLAN scanning
WLAN Discovery Failure Count	The WLAN Discovery Failure Count determines the number of WLAN SNMP scans that will elapse before the EGW will change the status of an undiscovered wireless endpoint to Call Center Mode (unprovisioned). The behavior applies to endpoints that were previously discovered by WLAN Discovery.
Location Servers Global Settings	
Ignore Locations Older Than	Setting which determine how long an ERL is considered valid by the EGW for MSE queries. Default value is 1 hour. This setting should be made in considering the level of wireless activity on-site as well as the mobile behavior of the users on the campuses.
Authentication Token Validity Period	At call time, when a call is provisioned and an ERL has been found with Wireless User Locator Enabled field to yes, the EGW builds the URL based on the current EGW IP address. The CPM generates a token (UUID) that will expire according to the <i>Authentication Token Validity Period</i> . This token is saved in the database along with the IP address of the caller and the expiration time. The token is required to access a map and a caller's location. Default value is 60 minutes. The token provides enhanced security and only enables access to the map data from the IP addresses tied to the authentication token.

Map Retention Period	Amount of time that the map is cached by the EGW. Default value is 24 hours. This setting prevents the EGW from needlessly downloading location data from the MSE within a short period of time.
----------------------	--

15.3.2 Provisioning Controllers and Access Points Individually

Controllers and Access Points can be entered one at a time using the Dashboard.

To enter controllers/access points one at a time:

1. Click on **Auto Discovery > WLAN Discovery > Controllers>Add Controller**
2. Configure the appropriate settings as described in the following table.

Table 109: Add Controller Screen- Field Descriptions

Parameter	Description
Controller IP	IP address of the controller. Required.
SNMP Version	Choose between SNMP Version 1, 2c and 3.
SNMP Community String*	String that acts as a password to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). Special characters are accepted and must be 25 characters or less. Default value is "public." Only applicable when SNMP Version 1 and 2c are chosen.
Security Name	Provide the security name required for SNMP Version 3. Upto 50 alphanumeric characters are accepted here. For more details, see.
Security Level	Choose between noAuthnoPriv , authnoPriv and authpriv to set the security level required for the interaction. For more details, see
SNMP Port	Standard SNMP port. Numerical value. Default value is port 161.
Description	Enter an easily identifiable description, in order to quickly locate a specific controller.
Vendor	Switch vendor. Cisco, Aruba, or Generic.
Default ERL ID	ERL that represents the location of the wireless controller. The Default ERL is assigned to an access point, if no ERL exists for that access point in the WLAN location map. Required.
AP Scan	Enable this parameter if you would like the EGW to scan the controller to detect the access points. If the parameter is left unchecked, you can use the Dashboard to enter access points individually.
Multiple BSSID Mask	Mask which will make multiple BSSIDs from the same access point appear the same. The field is used in the scenario where the BSSIDs reported by the devices, differ from the BSSID obtained by scanning the WLAN controller. Using the mask, accounts for the fact that the WLAN controller has multiple BSSIDs that use a variation of the same MAC.

Parameter	Description
	<p>Possible values:</p> <p>**3456789abc (mask the first 2 digits of the MAC address) *23456789abc (mask the first digit of the MAC address) 123456789ab* (mask the last digit of the MAC) 123456789a** (mask the last two digits of the MAC)</p>
SSIDs Supported	Enter a list of supported SSIDs or leave the field blank to automatically use all SSIDs that are detected on the access point. Entering specific SSIDs enables you to filter out SSIDs to which no wireless IP phones are associated.
Actions	<p>Save. Use this action add the controller.</p> <p>Back: Use this action to stop adding controllers. This takes you back to the Current WLAN Controllers list.</p>

Note: You can change the SNMP Community String by clicking on the **Change button. You can enter the value and click on "Apply to all WLAN Controllers" to apply the new SNMP Community string to all the controllers present.*

SNMP Version 3

SNMP version 3 is more secure than SNMP version 2c. If SNMP version 3 is chosen, additional security parameters become available, as defined below:

- When **noAuthNoPriv** is chosen as the **Security Level**, only the **Security Name** is the mandatory field. The **Security Name** is used for authentication and the data packet is passed in clear text.
- When **authNoPriv** is chosen as the **Security Level**, the **Security Name**, **Auth Protocol** and the **Auth Passphrase** need to be configured. MD5 or SHA is used for authentication and the remaining data packet is passed as clear text.
- When **authPriv** is chosen as the **Security Level**, the **Security Name**, **Auth Protocol**, **Auth Passphrase**, **Encrypt Protocol** and **Encrypt Passphrase**. MD5 or SHA is used for authentication and encryption is done with either **DES** (Data Encryption Standard) or **AES** (Advanced Encryption Standard). The entire data packet is encrypted.

15.3.2.1 Add Access Point

Table 110: Add Access Point- Field Descriptions

Parameter	Description
AP Name	The Access Point Name of the WLAN Controller. Alphanumeric up to 25 characters.
AP Location	The Access Point Location of the WLAN Controller. Alphanumeric up to 25 characters.
AP MAC	Mac Address of the AP. Use the Access Point BSSID to create an AP entry in the wireless network map. Omit this field when adding a Cisco Controller.
AP BSSID	A single BSSID or a list of BSSIDs, if AP has multiple BSSIDs.
ERL ID	Emergency Response Location Identifier. Alphanumeric between 1 and 31 characters in length.

15.3.3 Provisioning Controllers and Access Points in a Batch

To upload multiple controllers and access points simultaneously, it is possible to upload the information in a batch. These batch files can be in text format or in CSV format.

Batch files are uploaded through the dashboard or via FTP.

- **Administrative Dashboard:** A batch file is uploaded using the EGW web interface. The file may be validated and processed in real-time.
- **FTP:** The file is uploaded via ftp. It is validated and processed based on the settings of the **Batch WLAN** Scheduled Task.

15.3.3.1 Batch File Processing Mechanism

The batch process mechanism processes the batch file one line at a time and executes the operation as specified in the batch file. The batch file is read and processed completely even if an error is detected.

If any errors are detected, the erroneous line is detected and captured in the **Log Error File**.

To upload a batch file via the Dashboard interface:

1. Prepare the batch file in accordance with the batch file format.
2. Click on **Auto Discovery** → **WLAN Discovery** → **Controllers** → **Batch Upload**.
3. Click on the **Choose File** button and browse the batch file you wish to upload.
4. Click on the **Upload** button to upload the file into the EGW.

Now the **Actions** columns under the Batch Logs section become populated with the following action buttons:

- **Batch Process:** Clicking on this button will proceed to provision the endpoint batch file.
- **Delete:** Clicking on this button will delete the batch file that you just uploaded

Note: The WLAN batch upload feature functions incrementally. This means that the batch file will only add/overwrite data to the EGW for the specific controllers/access points in the batch file. The batch file will not overwrite data for controllers/access points that are not specified in the batch file. However, any errors generated during the batch upload process necessitate the re-upload of the **entire** batch file.

15.3.3.1.1 FTP

To batch upload via ftp:

1. Open an ftp connection to the EGW using the IP of the EGW, username: batchwlan, password: 911batch.
2. Go to the **batch** directory.
3. Upload the file to the EGW.

Batch files uploaded to the EGW using FTP are governed by scheduled tasks settings. The scheduled task **Batch WLAN** dictates precise daily intervals at which batch processing will occur.

Note: After a batch file uploaded to the EGW via ftp is processed, it is automatically removed from the FTP directory. These files can be viewed using the Dashboard interface.

FTP Batch results

The batch logs summary and error reports are sent to the email addresses configured at **Configuration** → **Advanced** → **Batch Settings**. Logs can also be viewed from the Dashboard.

15.3.4 Batch File Format

EGW supports bulk addition of controllers and access points using a text file as well as a CSV file.

The CSV format supports adding controllers and access points using SNMP versions 1, 2c or 3 whereas the text batch file format supports only SNMP version 1 and 2c. Furthermore, through the CSV batch file format, you can add as well as delete controllers. Deleting controllers is not possible through text batch file.

Note: If you leave the SNMP Version column empty in the batch file, EGW considers the version to be 2c.

15.3.4.1 Text format for Batch File

If the batch file to upload is in a text format, then the fields must be semicolon delimited. The fields must be in the following order and include the mandatory fields as listed in the table below:

- WLAN Controller IP address
- SNMP version
- SNMP Community String
- SNMP port
- WLAN Controller Description
- WLAN Controller vendor name
- SSIDs
- AP Scan
- ERL ID
- AP BSSID
- Access Point (AP) Name
- AP Location
- AP MAC
- Multiple BSSID Mask

Please note that controllers and access points cannot be deleted using the text batch file format.

The following table describes each of these fields in greater detail:

Table 111: Text Batch File Format for Batch Provisioning WLAN Controllers

Position	Field Name	Description	Required?
1	WLAN Controller IP Address	The IP address of the WLAN Controller. Alphanumeric.	Yes
2	SNMP Version	The SNMP protocol version 1 or 2 or 2c. Default is version 2c. This field is automatically determined by the EGW.	No
3	SNMP Community String	String that acts as a password to authenticate messages sent between the management station (the SNMP manager) and the device (the SNMP agent). Special characters are accepted and must be 25 characters or less. Default value is “public.”	Yes
4	SNMP Port	Standard SNMP port. Numerical value. Default value is port 161.	No
5	WLAN Controller Description	Description of the WLAN Controller. Alphanumeric. No limits.	No
6	WLAN Controller Vendor Name	WLAN Controller Vendor name. Alphanumeric between 1 and 25 characters.	Yes
7	SSIDs	A single SSID or a list of SSIDs that limit the scanning to specified SSIDs. The SSID are alphanumeric and multiple SSIDs can be entered as a comma separated list (i.e mobile911, wlanphones). If the field is left blank and AP scanning is enabled for the controller, all the SSIDs on the access points will be scanned by the EGW.	No
8	AP Scan	Specify to 0 (false) or 1 (true). Value 0 disables AP scanning, while a value of 1 enables it. Scanning is not required if your endpoints support the E911 Softphone Locator (ESL).	Yes

Position	Field Name	Description	Required?
9	ERL ID	Emergency Response Location Identifier. Alphanumeric between 1 and 31 characters in length. The ERL either applies to the Controller or to the access point depending on the setting of Position 10. The ERL applied to the Controller is the Default ERL. The ERL applied to the access point, is the specific ERL that is associated to the access point.	Yes
10	AP BSSID	BSSID of the Access Point. Use the wildcard (*) to add a WLAN Controller. Use the Access Point BSSID to create an AP entry in the wireless network map. Alphanumeric up to 17 characters. For multiple BSSID per AP, specify the comma separated list of BSSIDs (eg. Aruba deployments). To support this configuration, AP MAC must also be specified.	Yes
11	AP Name	The Access Point of the WLAN Controller in the row. Alphanumeric up to 25 characters. Can be left blank and it will be discovered during the scan.	No
12	AP Location	The Access Point Location of the WLAN Controller in the row. Alphanumeric up to 25 characters. Can be left blank and it will be discovered during the scan.	No
13	AP MAC	Mac Address of the AP. Use the Access Point BSSID to create an AP entry in the wireless network map. Omit this field when adding a Cisco Controller.	No
14	Multiple BSSID Mask	<p>The value of this field defines a mask which will configure the EGW to ignore certain BSSID MAC digits when processing device BSSID data. The field is used in the scenario where the BSSIDs reported by the devices, differ from the BSSID obtained by scanning the WLAN controller.</p> <p>The value is optional (defaults to 0 or no BSSID mask) and must be between -2 and 2 if specified.</p> <p>It only applies to rows that define WLAN controller (ignored for rows that define AP)</p> <ul style="list-style-type: none"> 1 indicates that the rightmost digit should be ignored when comparing an endpoints BSSID to this controller's BSSIDs 2 indicates that the two rightmost digits should be ignored when comparing an endpoints BSSID to this controller's BSSIDs -1 indicates that the leftmost digit should be ignored when comparing an endpoints BSSID to this controller's BSSIDs -2 indicates that the two leftmost digits should be ignored when comparing an endpoints BSSID to this controller's BSSIDs 	No

Batch text format examples:

Below are examples of text batch file data to upload WLAN controllers and Access points:

- In the following example, a wireless controller with default SNMP (version 2c) and community string is being added to the configuration. The WLAN controller vendor is Cisco and the SSIDs are test911 and mobile911. The AP Scan field is set to 1, which means that the EGW will scan the controller to automatically discover the access points. The Default ERL for the controller is LOC56, and the (*) indicates that a controller is being added to the configuration, rather than an access point BSSID.
 - 192.168.0.221;2c;public;161;;Cisco;test911,mobile911;1;LOC56;*;;;;

- In the following example, a wireless access point with BSSID 0024C48E1F90 is added to controller IP 192.168.0.221
 - 192.168.0.221;2c;West;161;;Cisco;test911,mobile911,test;1;LOC56;0024C48E1F90;;;
- In this example, an access point with MAC address 0024C48E1FAA is added with 2 BSSID associated: 0024C48E1F91 and 0024C48E1F92
 - 192.168.0.221;2c;public;161;;Aruba;test911,mobile911;1;LOC56;0024C48E1F91,0024C48E1F92;;;0024C48E1FAA;

15.3.4.2 CSV format for Batch File

The CSV batch file format for bulk provisioning of WLAN controllers contains the following headers, as shown in the table below alongwith the descriptions and limitations:

Table 112: CSV Batch File Format for Adding WLAN Controllers

CSV Header	Description	Required
OPERATION	1 for Add/ Update 2 for Delete	Yes
CONTROLLER_IP	IP address of the controller	Yes
SNMP_VERSION	SNMP Version of the switch. 1, 2c, or 3. If left empty, EGW considers the SNMP version as 2c.	No
SNMP_COMMUNITY	SNMP Community String. Special characters are accepted and must be 25 characters or less. Default value is “public.”	Yes
SNMP_SECURITY_NAME	Security name required for SNMP Version 3. Alphanumeric up to 50 characters.	Yes (required for SNMP Version 3)
SNMP_SECURITY_LEVEL	V3 (noAuthNoPriv), V3 (authNoPriv), V3 (authPriv)	Yes (required for SNMP Version 3)
SNMP_AUTH_PROTOCOL	MD5 or SHA	Yes (required for SNMP Version 3)
SNMP_AUTH_PASSPHRASE	Alphanumeric up to 50 characters.	Yes (required for SNMP Version 3)
SNMP_ENCRYPT_PROTOCOL	DES or AES	Yes (required for SNMP Version 3)

CSV Header	Description	Required
SNMP_ENCRYPT_PASSPHRASE	Alphanumeric. A minimum of 8 characters are required in this field.	Yes (required for SNMP Version 3)
SNMP_PORT	SNMP Port. Must be a numeric value between 1 and 65535. If left empty, EGW considers the default value as 161.	No
DESCRIPTION	Description of the controller. No limits to the number of characters you can enter here.	No
VENDOR	Vendor of the controller. Must be Aruba, Cisco or Generic. Alphanumeric between 1 and 25 characters.	Yes
SSID_NAME	A single SSID or a list of SSIDs that limit the scanning to specified SSIDs. The SSID are alphanumeric and multiple SSIDs can be entered as a comma separated list (i.e. mobile911, wlanphones). If the field is left blank and AP scanning is enabled for the controller, all the SSIDs on the access points will be scanned by the EGW.	No
AP_SCAN_ENABLED	Specify to 0 (false) or 1 (true). Value 0 disables AP scanning, while a value of 1 enables it. Scanning is not required if your endpoints support the E911 Softphone Locator (ESL). If left empty, EGW considers the AP scanning to be disabled.	No
ERL_ID	Emergency Response Location Identifier. Alphanumeric between 1 and 31 characters in length. The ERL either applies to the Controller or to the access point depending on the setting of Position 10. The ERL applied to the Controller is the Default ERL. The ERL applied to the access point, is the specific ERL that is associated to the access point.	Yes
AP_BSSID	BSSID of the Access Point. Use the wildcard (*) to add a WLAN Controller. Use the Access Point BSSID to create an AP entry in the wireless network map. Alphanumeric up to 17 characters. For multiple BSSIDs per AP, specify the comma separated list of BSSIDs (e.g. Aruba deployments). To support this configuration, AP_MAC (mac address of the access point) must also be specified.	Yes

CSV Header	Description	Required
AP_NAME	The Access Point of the WLAN Controller. Alphanumeric up to 25 characters. Can be left blank and it will be discovered during the scan.	No
AP_LOCATION	The Access Point Location of the WLAN Controller in the row. Alphanumeric up to 25 characters. Can be left blank and it will be discovered during the scan.	Yes
AP_MAC	Mac Address of the Access Point. Use the Access Point BSSID to create an AP entry in the wireless network map. Omit this field when adding a Cisco Controller.	No
MULTI_BSSID_MASK	<p>The value of this field defines a mask which will configure the EGW to ignore certain BSSID MAC digits when processing device BSSID data. The field is used in the scenario where the BSSIDs reported by the devices, differ from the BSSID obtained by scanning the WLAN controller.</p> <p>The value is optional (defaults to 0 for no BSSID mask) and must be between -2 and 2 if specified.</p> <p>It only applies to rows that define WLAN controller (ignored for rows that define AP)</p> <p>For more details, see Multiple BSSID Mask</p>	Yes

Note: The column **Required** in the table above provides the mandatory fields required when adding or updating the controllers and access points through a batch CSV file. When deleting controllers and access points through a batch CSV file, only the **Operation** and the **Controller_IP** fields are mandatory. The **AP_Name** field is not required for the delete operation but it is used as an identifier to delete the Access point. On the other hand, only for Aruba controllers, the **AP_MAC** and the **AP_BSSID** can be used together to identify and delete the access point.

Batch CSV format examples:

An example of the CSV batch file format is shown below:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
1	OPERATIC_CONTROLLER_IP	SNMP_V3	SNMP_SE	SNMP_SE	SNMP_SE	SNMP_AU	SNMP_AU	SNMP_EN	SNMP_EN	SNMP_EN	SNMP_EN	DESCRIPTI	VENDOR	SSID_NAM	AP_SCAN	ERL_ID	AP_BSSID	AP_NAME
2	1 192.168.210.1	2c	theconnexon						161		Cisco	911E-QA-C	0	LOC100	*			
3	1 192.168.210.1													LOC200	0008305CC	MTL-AP02		
4	1 192.168.210.1													LOC100	0008305CC	MTL-AP01		
5	1 192.168.210.1													LOC100	0024C48E1	IT-AP02		
6	1 192.168.210.1													LOC100	0024C48E1	IT-AP01		

Figure 64: CSV Batch File Example

In the above example, in the first row, a wireless controller with SNMP version 3 is being added to the configuration. The SNMP auth protocol is set to SHA and the SNMP Encrypt protocol is set to AES. Access Point scanning is enabled (set to 1), meaning the EGW scans the controllers to automatically discover the access points. The Default ERL for the controller is LOC100 and the (*) in the first row for AP_BSSID indicates that a controller is being added to the configuration, rather than an access point BSSID.

Multiple BSSID Mask

Example: Multiple BSSID Mask = 2

When the multiple BSSID mask is 2., EGW ignores the 2 rightmost digits when comparing the endpoint's BSSID to the controller's BSSID.

For example, in the following MAC address "123456789abc", if 2 is entered as the Multiple BSSID Mask, then the rightmost digits, "b" and "c", are ignored when comparing it to the endpoint's BSSID. In other words, the MAC address is considered as 123456789a**.

Example: Multiple BSSID Mask = -1

When the multiple BSSID mask is -1, EGW ignores the leftmost digit when comparing the endpoint's BSSID to the controller's BSSID.

For example, in the following MAC address "123456789abc", if -1 is entered as the Multiple BSSID Mask, then the leftmost digit "1" is ignored when comparing it to the endpoint's BSSID. In other words, the MAC address is considered as *23456789abc.

15.3.5 WLAN Discovery Batch Logs

Batch log files report on the success or failure of each entry in a submitted batch file in response to the Batch Process operation.

To view the batch logs

- Click on **Auto Discovery** → **WLAN Discovery** → **Controllers** → **Batch Upload**.

The columns of the Batch Logs display the following information:

- Original File Name
- Log File
- Error Log File
- Log Date
- Status
- Actions (Batch Process and Delete*)

15.3.5.1 Log File

To view a log file, click on **View Log File** under **Log File**.

The log file provides a status report for each line of the processed batch file. A line will contain an response code followed by the original line in the batch file. If the operation was executed successfully, the response code will be set to 00 for text batch file and 0 for CSV batch file. Any other response code means that the operation did not complete successfully. The log file is generated even when there are no errors in your batch file.

The log file as a result of batching a text file is returned as a text file whereas a log file resulting from batching a CSV file is returned as a CSV file.

Any response code other than 00 or 0 indicate that there was an error in the batch file. In such a case, the error log file will be generated as well. See

Note: If Log File displays View Peer, you must login to the Peer to view the log file. This scenario occurs when a batch file was processed by the Peer machine.

Example

- Below is an example from a log file following the processing of a batch text file. 00 indicates that the batch file was properly formatted and passed validation without error.
 - 00;192.168.0.221;2c;public;161;;Cisco;test911,mobile911;1;LOC56;*;;
- Below is an example from a log file following the processing of a batch CSV file. 0 indicates that the batch file was properly formatted and passed validation without error.

A	B	C	D	E	F	G	H	I	J	K	L	M	P	Q	R
1	OUTPUT	MESSAGE	OPERATION	CONTROLL	SNMP_V	SNMP_C	SNMP_S	SNMP_A	SNMP_AU	SNMP_AUTH	SNMP_EN	SNMP_ENCRYPT_PA	SNMP_P	SNMP_SCAN_ERL_ID	
2	0	Successfully created controller.	1	192.168.210	3	WEST	authPriv	SHA	PaSSphRASE	AES	####	161		1	LOC200

Figure 65: Batch Log File

15.3.5.2 Error Log File

To view the log error file, click on **View Log File** under **Error Log File**.

The **Error Log File** is only generated when an error was detected in the log file and an entry could not be processed.

The error log file that results from batching a text file is returned as a text file whereas an error log file resulting from batching a CSV file is returned as a CSV file.

The lines in the error log text file will contain a response code followed by the original entry that could not be processed. For more information **Text Batch Response Codes**.

If a CSV batch file was uploaded and there were errors with the validation, then two additional columns, “OUTPUT” and “MESSAGE” are added to the CSV log error file to record the response code and their description respectively. See **CSV Batch Response Codes**.

15.3.5.2.1 Text Batch Response Codes

The following table details each possible outcome resulting from a single operation.

Table 113: Text Batch Response Codes

Response Code #	Description
00	_SUCCESS_ The entry is successful.
01	_INVALID_ROW_NUMBER_ The entry does not have the right number of fields.
02	_INVALID_ERL_ID_ The format of the ERL ID is invalid.
03	_INVALID_CONTROLLER_IP_ The format of the WLAN Controller IP Address is invalid.
04	_INVALID_SNMP_COMMUNITY_ The format of the WLAN Controller SNMP community string is invalid.
05	_INVALID_SNMP_PORT_ The format of the WLAN Controller SNMP Port is invalid.
06	_INVALID_VENDOR_ The WLAN Controller Vendor name is invalid.
07	_INVALID_SSID_ The WLAN Controller SSID is invalid

08	_INVALID_AP_SCAN_ The WLAN Controller AP Scan setting is invalid. The setting can only be 0 or 1.
09	_INVALID_BSSID_ The WLAN Controller Access Point BSSID is invalid.
10	_INVALID_AP_NAME_ The WLAN Controller Access Point Name is invalid.
11	_SSID_EXISTS_ The specified SSID already exists.
12	_CONTROLLER_IP_NOT_CREATED_ An unexpected error has occurred.
13	_CONTROLLER_IP_EXISTS_ The specified IP address of the WLAN Controller already exists.
14	BSSID_EXISTS The specified BSSID already exists.
15	INVALID_BSSID_LIST_MISSING_MAC Happens if BSSID is a list and no MAC was specified in that list.

Example

Below is a line from a log error file following the processing of a batch text file. 01 indicates that that the batch file failed validation since it did not have the correct number of fields.

01;192.168.0.221;2c;161;;Cisco;test911,mobile911,test;1;LOC56;0024C48E1F90;ConfRoom;Conf. Room B;

15.3.5.2.2 CSV Batch Response Codes

Table 15-4 CSV Batch Response Codes

Error #	Description
0	_SUCCESS_ The entry is successful. One the following messages are returned depending on the operation: <ul style="list-style-type: none"> • Successfully created access point. • Successfully created controller. • Successfully validated. • Successfully deleted controller. • Successfully deleted access point.
1	_INVALID_ROW_NUMBER_ The entry does not include the correct number of fields.

2	<p><u>_INVALID_ERL_ID_</u></p> <p>The following value is invalid for the specified CSV header: ERL_ID</p>
3	<p><u>_INVALID_CONTROLLER_IP_</u></p> <p>The following value is invalid for the specified CSV header: CONTROLLER_IP</p>
4	<p><u>_INVALID_SNMP_COMMUNITY_</u></p> <p>The following value is invalid for the specified CSV header: SNMP_COMMUNITY</p>
05	<p><u>_INVALID_SNMP_PORT_</u></p> <p>The following value is invalid for the specified CSV header: SNMP_PORT</p>
6	<p><u>_INVALID_VENDOR_</u></p> <p>The following value is invalid for the specified CSV header: VENDOR</p>
7	<p><u>_INVALID_SSID_</u></p> <p>The following value is invalid for the specified CSV header: SSID</p>
8	<p><u>_INVALID_AP_SCAN_</u></p> <p>The following value is invalid for the specified CSV header: AP_SCAN</p>
9	<p><u>_INVALID_BSSID_</u></p> <p>The following value is invalid for the specified CSV header: AP_BSSID</p>
10	<p><u>_INVALID_AP_NAME_</u></p> <p>The following value is invalid for the specified CSV header: AP_NAME</p>
11	<p><u>_SSID_EXISTS_</u></p> <p>The following value is invalid for the specified CSV header: SSID</p>
12	<p><u>_CONTROLLER_NO_EXIST_</u></p> <p>Controller does not exist.</p>
13	<p><u>_AP_NO_EXIST_</u></p> <p>Access point does not exist.</p>
14	<p><u>_BSSID_EXISTS_</u></p> <p>The following value is invalid for the specified CSV header: AP_BSSID</p>
15	<p><u>_INVALID_BSSID_LIST_MISSING_MAC_</u></p> <p>The following value is invalid for the specified CSV header: AP_BSSID</p>
16	<p><u>_INVALID_BSSID_MASK_</u></p> <p>The following value is invalid for the specified CSV header: MULTI_BSSID_MASK</p>

17	<p><u>_INVALID_SNMP_VERSION_</u></p> <p>The following value is invalid for the specified CSV header: SNMP_VERSION</p>
18	<p><u>_INVALID_SNMP_SECURITY_NAME_</u></p> <p>The following value is invalid for the specified CSV header: SNMP_SECURITY_NAME</p>
19	<p><u>_INVALID_SNMP_SECURITY_LEVEL_</u></p> <p>The following value is invalid for the specified CSV header: SNMP_SECURITY_LEVEL</p>
20	<p><u>_INVALID_SNMP_AUTH_PROTOCOL_</u></p> <p>The following value is invalid for the specified CSV header: SNMP_AUTH_PROTOCOL</p>
21	<p><u>_INVALID_SNMP_AUTH_PASSPHRASE_</u></p> <p>The following value is invalid for the specified CSV header: SNMP_AUTH_PASSPHRASE</p>
22	<p><u>_INVALID_SNMP_ENCRYPT_PASSPHRASE_</u></p> <p>The following value is invalid for the specified CSV header: SNMP_ENCRYPT_PASSPHRASE</p>
23	<p><u>_INVALID_SNMP_ENCRYPT_PROTOCOL_</u></p> <p>The following value is invalid for the specified CSV header: SNMP_ENCRYPT_PROTOCOL</p>
24	<p><u>_INVALID_OPERATION_</u></p> <p>The following value is invalid for the specified CSV header: OPERATION</p>
25	<p><u>_CONTROLLER_NOT_CREATED_</u></p> <p>Error creating controller.</p>
26	<p><u>_AP_NOT_CREATED_</u></p> <p>Error creating access point.</p>
27	<p><u>_CONTROLLER_NOT_DELETED_</u></p> <p>Error deleting controller.</p>
28	<p><u>_AP_NOT_DELETED_</u></p> <p>Error deleting access point.</p>
40	<p><u>_INVALID_CSV_HEADER_</u></p> <p>Invalid CSV Header. The following CSV header is not valid:</p>
41	<p><u>_MISSING_CSV_HEADER_</u></p> <p>Missing CSV Header. The following CSV header is missing:</p>
46	<p><u>_DUPLICATE_CSV_HEADER_</u></p> <p>Duplicate CSV header. The following CSV header is a duplicate of another CSV header:</p>

Example

Below is a row from a log error file following the processing of a batch CSV file. The “OUTPUT” column displays the response code of 19 indicating that the value provided in the SNMP_SECURITY_LEVEL field was invalid. .

A	B	C	D	E	F	G	H	I
OUTPUT MESSAGE 19 The following value is invalid for the specified CSV header: SNMP_SECURITY_LEVEL accepts only the following values: noAuthNoPriv, authNoPriv or authPriv.		OPERATIC	CONTROL	SNMP_V	SNMP_CO	SNMP_SE	SNMP_SE	SNMP_AU

Figure 66: Log File Example

15.3.6 Adding Location Servers

You need to add location servers for use with the Cisco MSE, Aruba Airwave and Aruba ALE.

To add a server:

1. Go to **Auto Discovery** → **WLAN Discovery** → **Location Servers**.
2. Click **Add**.

Configure the fields as described in the table below:

Parameter	Description	Limitations/ Notes
Server Name	Name of the Server	<ul style="list-style-type: none"> • Must be unique • Cannot exceed 50 characters • Space is supported
Server Type	Type of server	<ul style="list-style-type: none"> • Default is set as Aruba Airwave • Other choices are Aruba ALE and Cisco MSE.
Timeout	When this timeout value is reached, alarm is raised:	<ul style="list-style-type: none"> • Default value is 4 seconds for Aruba • Default value is 10 seconds for Cisco
System Management URL	URL that connects to the server. This is where the EGW will get the map data from at call time.	The URL that connects to the Cisco or the Aruba server.
Username	Username to connect to the server.	This information must be provided to the person configuring the EGW by the IT System Administrator of his/her organization.
Password	Password to connect to the server.	This information must be provided to the person configuring the EGW by the IT System Administrator of his/her organization.

15.3.7 Wireless Infrastructure Maintenance Using the Dashboard

If changes are made to your wireless network (eg. Controllers/access point added/removed) you must update the EGW configuration accordingly.

In deployments with wireless phones, the EGW will automatically discover access points that are added to the network. You can then assign specific ERLs to the access points, if they will be different then the default ERL assigned to the controller.

In ESL deployments, where WLAN scanning is turned off, any new Access points need to be added to the EGW configuration manually.

15.4 Export WLAN Discovery Details

Through the EGW dashboard, you can also export the WLAN discovery details of your organization's network configuration. This is useful if you wish to back up or edit your network configuration.

These reports can be downloaded in the form of text files or CSV files.

To download WLAN Controllers and Access Point reports:

6. Go to **System Status** → **Reports**.
7. Under **Select Reports**, choose **WLAN Controllers and Access Points** from the dropdown menu.
8. Under **Report Type**, choose between **Export Batch** and **Export Batch CSV**.
9. Click **Generate Report**.
10. Click **Download Report**.

15.5 Troubleshooting WLAN Discovery

The following topics addresses issues that are commonly seen in the field.

15.5.1 Accuracy of ERL Assignment to the Access Switches

ERL assignment for wireless phones is administered down to the access point level. The BSSID of the access switch is mapped to an ERL record in the EGW, enabling the EGW to identify the locations of wireless phones to the nearest access point. However, it should be noted that it is possible for AP signals to propagate to floors above or below the physical space that is described by that AP's ERL record. To help mitigate this issue, it is best practices for administrators to direct access point signals in a horizontal fashion. Nevertheless, emergency personnel should be made aware of the inherent limitations of wireless location determination, so that they can best organize their emergency response efforts.

Intrado recommends including a description in the ERL record to indicate that the ERL belongs to a wireless access point. Doing so provides on-site responders with the knowledge that they may need to undertake a more extensive search, in order to find the precise location of the caller (eg. Adjacent floors, hallways, rooms etc.).

15.5.2 WLAN Discovery and Layer 2 Discovery Interactions

It is important to set the **WLAN Discovery Failure Count** high enough so that it allows at least one Layer 2 Discovery process to complete before it expires. If a phone has moved from wireless to wired mode, this will provide the EGW with enough time to discover it in the next Layer 2 scan.

Note: *The above consideration does not apply to phones that support the E911 softphone locator (ESL). The ESL tracks both wireless and wired endpoints. When a phone moves from wireless to wired mode, it registers on the network and an ESL push is immediately sent to the EGW.*

16 NENA 2 Provisioning

16.1 Overview of NENA 2 Files

The NENA 2 format specifies a standard file format that is used to synchronize data between enterprise databases and Automatic Location Identification (ALI) databases. The EGW is capable of generating NENA 2 files on a periodic basis, to synchronize its database with a LEC PS-ALI or an on-site security desk P-ALI.

Note: *If you will be exporting ALI data to a LEC PS-ALI database, verify the formatting requirements of your carrier. If the format is different, you will have to edit NENA files before they may be uploaded to the regional ALI.*

For more information concerning Local Trunking, see section 6 “Configuring Local Trunking (LEC Call Routing)” and the document “NENA Standard Data Formats for ALI Data Exchange and GIS Mapping.”

16.2 Understanding the EGW’s NENA 2 Feature

The EGW generates NENA 2 files based on its inventory of ELINs. The feature runs as a scheduled task, and will generate a new file only if changes to the ELIN inventory have been made since the last NENA 2 file was generated. It is possible to limit the feature to specific NPA-NXX number ranges within the ELIN inventory. This addresses deployments where specific NPA-NXX ranges are applicable for NENA 2 file generation while other number ranges need to be excluded.

The following functionality is observed for either the entire ELIN inventory or defined NPA-NXX range(s):

- When the NENA 2 report feature is enabled, the report will be generated based on the settings of the scheduled task Generate NENA 2 File
- If changes are made to the ELIN inventory (inserts, adds, changes) a new NENA 2 report is generated at the next scheduled task run time and stored at FTP of EGW. The file is also accessible from the Dashboard interface at **Provisioning > NENA 2 > File Generation**. If no changes have been made to the ELINs no report is generated at task runtime
- A new NENA 2 file may be generated manually at **Provisioning > NENA 2 > File Generation** by clicking on **Generate NENA 2 File** (number of modified entries since last report generated is indicated)
- Two types of NENA 2 files are supported: **Incremental** and **Full**.

Incremental: Includes Inserts, Changes and Deletions since last NENA 2 file was generated.*

Full: Includes entire ELIN inventory: Only Inserts and Changes are included.**

*Incremental NENA 2 reports are suitable for customers that update a LEC PS-ALI.

**Full NENA 2 reports are suitable for large enterprise customers with Private ALI databases used by Security Desks.

16.2.1 NENA 2 ELIN Filtering

The NENA 2 ELIN Filtering feature enables you to specify specific ELIN NPA-NXX ranges which will be included in NENA 2 reports. The ELINs not included in the NPA-NXX ranges are excluded from the NENA 2 reports.

If you have some ELINs in the EGW inventory and the NENA 2 reports feature is enabled, all of the ELINs will be included in the next NENA 2 report when the generate NENA 2 task is run. When NPA-NXX ELIN ranges are specified in the NENA 2 file generation settings, subsequent reports will only include entries for the ELINs which are a part of these NPA-NXX ranges.

For more information, see section 16.3 “EGW Configuration for NENA 2 Feature.”

16.2.2 Cycle Counter

A sequence number is added to the NENA 2 files generated by the EGW. The sequence number ensures that the files are processed in the correct sequence by the ALI database. The sequence number that is applied to a NENA 2 file is controlled by the **Cycle Counter** parameter.

The cycle counter may be reset in the instance where a PS-ALI database needs to be re-built. Also, you may change it if it becomes unsynchronized with the sequence submitted to your service provider.

16.2.3 NENA 2 Reports

All of the NENA 2 file generation methods will increment the cycle counter, except for NENA 2 report generation at **System Status** → **Reports** → **NENA 2**. A NENA 2 report generates a **Full** file that includes an entry for the entire ELIN inventory.

You may change the cycle counter value that will apply to the generated NENA 2 Report. However, this cycle counter value only applies to the generated NENA 2 report, and does not increment the cycle counter value that applies globally to the NENA 2 file generation scheduled task.

16.3 EGW Configuration for NENA 2 Feature

To configure the NENA 2 feature the following must be performed:

- **Configure Global Settings:** Set **NENA CAN Enabled***, and/or **NENA US Enabled**, to **Yes**, based on applicability.**
- **Configure the scheduled task:** Task scheduler may be configured to run multiple times per day.
- **Configure NENA 2 fields:** The NENA 2 feature depends on data in the ERL configuration. Additional information that is required for the NENA 2 file format is entered on the NENA 2 Configuration screen.
- **Configure NENA 2 ELIN filtering if applicable**

*CAN is short for Canada. Parameter should only be available if you need to generate NENA 2 files for a Canadian ALI database.

**Unless one of these parameters is enabled, the NENA 2 Configuration and scheduled task screens will not be available from the Dashboard.

To configure the Global setting:

1. Click on **Configuration** → **Advanced** → **Global**.
2. Scroll to the bottom of the page and click **Edit**.
3. Set the drop down box to **Yes** for the **NENA 2** feature.

To configure the scheduled task:

1. Click on **Configuration** → **Task Scheduler**.
2. Click on **Edit** in the **Generate NENA 2 File** row.
3. Configure settings as required*.

*In most cases only default settings are required.

16.3.1 Configuring NENA 2 Fields

The NENA 2 feature depends on the data in your ERL configuration. It also depends on information that is entered at the NENA 2 Configuration screen.

To Configure NENA 2 fields:

1. Click on **Provisioning → NENA 2 → Configuration**
2. Configure the fields based on the description in the table below:

Table 114: NENA 2 Fields Configuration

Field	Description
Report Type	<p>Type of NENA 2 Report to be generated: Incremental or Complete.</p> <p>C = Change D = Delete I = Insert</p> <p>Incremental: Includes Inserts, Changes and Deletions since last NENA 2 file was generated.*</p> <p>Full: Includes entire ELIN inventory: Only Inserts and Changes are included.**</p> <p>*Incremental NENA 2 reports are suitable for customers that update a LEC PS-ALI. **Full NENA 2 reports are suitable for large enterprise customers with Private ALI databases used by Security Desks.</p>
Cycle Counter	Sequential number, 1-999,999,999
Customer Name	Name of Company forwarding file. By default, the NENA 2 file generation depends on the data in the ERL record to fill this field. If the ERL record field is empty, the configured Customer Name is used instead.
Company ID	Company ID of a PS/911data provider or a Reseller. NENA registered Company Identification code.
Customer Code	Code used to uniquely identify a customer.
Source ID	<p>Code that indicates whether data is part of the initial data base creation process or part of the daily update process.</p> <p>Daily = Space, Initial Load = C</p>
Class of Service	<p>Value of:</p> <p>1 = Residence 8 = Mobile 2 = Business 9 = ResidenceOPX 3 = Residence PBX 0 = Business OPX 4 = Business PBX A = Customer Owned Coin Telephone(COCT) 5 = Centrex B = Not Available</p> <p><i>Footnote 4</i></p> <p>6 = Coin 1 Way out G = Wireless Phasel 7 = Coin 2 Way H = Wireless Phasel I = Wireless Phasel with Phase I information V = VoIP Services Default COS C = VoIP Residence D = VoIP Business E = VoIP Coin/Pay Phone F = VoIP Wireless J = VoIP Nomadic</p>

Field	Description
Type of Service	Value of: 0 = Not FX nor Non-Published 1 = FX in 911 serving area 2 = FX outside 911 serving area 3 = Non-Published 4 = Non-Published FX in serving area 5 = Non-Published FX outside 911 serving area 6 = Local Ported Number (LNP) 7 = Interim Ported Number
Exchange	Local Exchange Carrier exchange identifier for the serving telephone office of the customer.
Tar Code	Taxing Area Rate Code.
Reserved	This field is reserved for the Data Base Management System Provider's use.

For more information, see the document, "NENA Standard Data Formats for ALI Data Exchange and GIS Mapping," and consult with your local carrier.

16.3.1.1 NENA 2 ELIN Filtering

To configure NENA 2 ELIN filtering:

1. Click on **Provisioning** → **NENA 2** → **Configuration**
2. Click on NENA 2 ELIN Filtering
3. Specify an NPA-NXX range. Eg.514745 (any DIDs in the range 514745xxx will be included)
4. Click Add

There is no limit to the amount of ranges that can be specified.

17 Provisioning Off-Campus Users

17.1 Overview of Support for Off-campus Users

Off-campus users cannot be automatically tracked by the EGW. Location information may be self-provisioned for off-campus users such as teleworkers and work-at-home employees.

Note: *Off-campus provisioning is only for enterprises that deliver calls to the Emergency Routing Service (ERS).*

The EGW offers two off-campus location reporting tools:

- Remote Location Manager (RLM)
- SOAP interface

Remote Location Manager (RLM)

The RLM is an application that allows users to self-report locations using their IP phones. The RLM runs on supported Cisco, Avaya, and Microsoft IP phones and softphones and may also be used by on-site users.

In addition, users with Cisco Jabber and Webex Teams clients can also use the Cisco Expressway for Mobile and Remote access. This enables employees to utilize their organization's E-911 coverage without using VPN.

RLM for softphones

RLM is a service running on Windows and Mac operating systems, which communicates with the EGW. It triggers a provisioning window pop-up, in response to IP softphone events (ie. Start-up or network change); this prompts the user to confirm/self report their emergency location.

For more information, see the document "RLM for Windows Softphone Installation and Configuration Guide."

SOAP Interface

The SOAP interface may be used to create a corporate provisioning web page. The web page may be used by off-campus users to perform self-provisioning.

For more information, see the document "SOAP Server Interface Description Document."

17.2 RLM Settings

You can configure the settings of the RLM according to your organization's preferences.

To edit RLM settings, click on **Configuration**→**Advanced**→**RLM**. The following table gives an explanation of the various fields on the RLM settings page and their description:

Table 115: RLM Settings Field Descriptions

Field	Description	Notes
RLM Enabled	Enables use of the Remote Location Management module (RLM). This module provides support for off-campus users.	Requires additional IP-PBX configuration, which varies by vendor. See section 17 "Provisioning Off-Campus Users."
RLM Local Enabled	Setting which determines how the phones will connect to Intrado's hosted address validation service. The default setting is Yes, which allows the phones to connect to the EGW via the SOAP client module.	Do not change this setting without consulting Intrado.
On-Site RLM Enabled	Setting that enables the on-site RLM feature.	

On-site RLM Max Search Results	Setting that determines that maximum amount of search results returned for a query, before the user is prompted to refine the search criteria.	
RLM Disclaimer Enabled	<p>Setting that determines whether you want to enable a custom disclaimer. If you choose a setting other than Never, you will be asked to enter a custom disclaimer text. For more information on the RLM disclaimer, please see section 17.2.2 RLM Disclaimer.</p> <p>The following three values are possible for the RLM Disclaimer setting:</p> <p>Never: This means the disclaimer is disabled.</p> <p>First Time: This means that the disclaimer will only be displayed when RLM is started for the first time. Subsequent restarts or pop-ups of the RLM will not display the disclaimer.</p> <p>Always: This means that the disclaimer will always be displayed when the RLM is opened or it pops-up.</p>	By default, the RLM Disclaimer is disabled.
RLM Notifier Enabled	Enables RLM Notifier service. The RLM Notifier uses CTI to listen for IP phone registration events on the network. When an IP phone registration event is detected, the RLM Notifier instructs the IP phone to request the RLM phone service from the EGW. The RLM provisioning page is then displayed on the phone's XML browser, prompting the user to verify if their location is up-to-date.	Requires additional IP-PBX and EGW configuration. See the document "Configuring the CUCM for the EGW Appliance," for more information.
EGW Server Assignment for RLM Notifier	Specifies the EGW machine on which the RLM Notifier service will run.	Primary or secondary.
RLM Notifier Server IP	IP address of the CTI server hosting the RLM Notifier CTI application user. The IP phones that will use the RLM Notifier are associated to the CTI Application user.	See the document "Configuring the CUCM for the EGW Hardware Appliance," for more information.
VPN Subnets	VPN Subnet that the RLM will detect when the end user uses the VPN connection to connect remotely to the organization's network.	

17.2.1 RLM Proxy Uplink Settings

To enable RLM Proxy Uplink, choose Yes under Enable Proxy Uplink menu. When this is enabled EGW prompts you to upload the .tgz file sent to you by the Intradis support staff. See EGW Cisco Expressway Configuration Guide.

The fields marked with an asterisk (*) get auto-populated as soon as you upload the .tgz file.

Table 116: RLM Proxy Uplink Settings

Field	Description	Notes
Enable Proxy Uplink	Setting that enables or disables proxy uplink for the EGW.	Required if you wish to use Cisco Expressway for mobile and remote access.
Uplink Server IP/FQDN/Hostname	IP, FQDN or Hostname of the uplink server.	Auto-populated when you upload the .tgz file.
Proxy Port	Proxy port of the uplink server.	Auto-populated when you upload the .tgz file.

Proxy Username	User name of the proxy.	Auto-populated when you upload the .tgz file.
----------------	-------------------------	---

17.2.2 RLM Disclaimer

Using the RLM Disclaimer settings, your organization can add custom disclaimer messages that you may want to display to the RLM users.

You can set up the RLM disclaimer in three different ways:

Table 117: RLM Disclaimer Configuration

Option	Description
Never	Use this option if you want to disable the disclaimer.
First Time	Use this option if you want the disclaimer to be displayed only for the first time the RLM is started for the user. <i>Note: If you reset the registry settings, the RLM will be displayed at the first start-up.</i>
Always	Use this option if you want the disclaimer to be always displayed when the RLM is started-up or when the RLM pops-up.

When the RLM Disclaimer is enabled and you choose either First Time or Always, you will be provided with two new options, as follows:

Table 118: RLM Disclaimer Configuration Settings

Option	Description
RLM Disclaimer Text	Enter text here that you want to be displayed as a part of your organization's disclaimer to the RLM's end users.
RLM Disclaimer Button Text	Enter the text here that you want to be displayed as your label.

17.3 Understanding On-site and Off-site Provisioning

The RLM allows users to perform self-provisioning when they are off-site. On-site IP hardphone and softphone users, on the other hand, are automatically tracked by the EGW. In some cases, a network may only partially support layer 2/3 discovery (e.g. only portions of the network are suitably wired/configured to support phone tracking), or may not support automatic discovery at all. In these cases, it is possible to use the RLM in on-site mode to perform self provisioning.

When users are off-site, they may manually enter an address into the RLM and validate it in real time. However, if users are on-site, the RLM can only be used to select a location from a list of pre-validated enterprise ERLs (provisioned by an administrator). When users access the RLM while on-site, they cannot create new on-site ERLs.

The RLM for softphones is a service running on Windows and Mac operating systems, which triggers a provisioning window pop-up, in response to IP softphone events (ie. Start-up): This prompts the user to confirm/self report the emergency location.

If you have a combination of layer 2 discovery enabled on-site and some off-site users, the ESL must be installed on the machines of the off-site users. The ESL delivers the networking parameters that enable the EGW to determine the locations of the on-site and off-site users.

For off-site endpoints that do not support the RLM, the EGW SOAP interface can integrate with an existing corporate webpage or network asset management tool to permit provisioning.

For more information, see the document “RLM for Windows Softphone Installation and Configuration Guide,” and “E911 Softphone Locator Installation and Configuration Guide.”

17.4 Configuring the Network for Off-Campus Users

Off-site users may be provisioned using the RLM or SOAP API Interface. Configuration tasks are required to set up the network to support these users.

17.4.1 Configuring the SOAP API

The SOAP interface may be used to create a corporate provisioning web page. Development work is required to integrate the SOAP interface into the webpage, based on WSDL specifications.

The administrative Dashboard is used to activate the SOAP provisioning service using the EGW SOAP Server.

To activate the SOAP interface:

1. Click on **Configuration** → **Advanced** → **SOAP Server**.
2. Enable **SOAP Server Locations** and **SOAP Server Endpoints**.
3. Provide a username and password for locations and endpoints.

Note: When you send function calls to the EGW SOAP Server, the username/password that you provide must match those provisioned using the Dashboard.

To learn how to send function calls to the EGW SOAP server in the correct format, see the document “SOAP Server Interface Description Document.”

17.4.2 Configuring the Remote Location Manager (RLM) for IP Hardphones

Configuration of the RLM will vary, depending on your phone system (Cisco, Avaya, Microsoft, etc.).

To configure your phone system for the RLM, see the configuration guide that pertains to your IP-PBX model.



Note: In order to configure redundancy for the RLM feature, the use of load balancers is required.

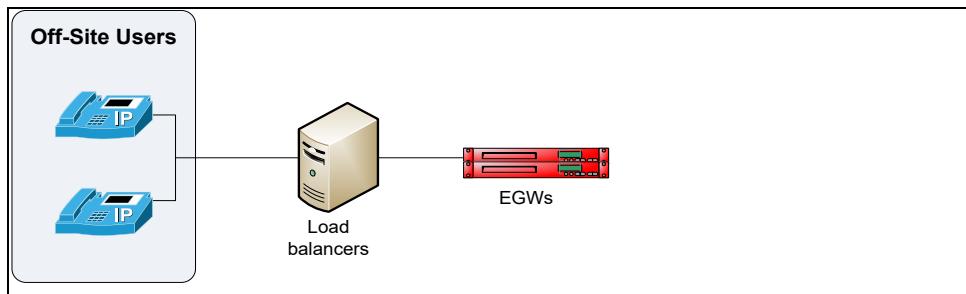


Figure 67: RLM URI Load Balancing

17.4.2.1 Cisco

The Remote Location Manager is available to Cisco IP phones equipped with an XML browser. By configuring the URL of the EGW/load balancer via CUCM Administration, the RLM provisioning page will be displayed on Cisco IP phones when the Services button is pressed. The provisioning page allows users to provision emergency locations in real-time.

For more information, see the document “Configuring the CUCM for the EGW Appliance.”

The RLM Notifier uses CTI to listen for IP phone registration events on the network. When an IP phone registration event is detected, the RLM Notifier instructs the IP phone to request the RLM phone service from the EGW. The RLM provisioning page is then displayed on the phone's XML browser, prompting the user to verify that their location is up-to-date.

To enable the RLM Notifier feature, the following information is required:

- IP address and credentials of CUCM server(s) running CTI Manager

In addition to EGW configuration, you must also create a CTI application user via CUCM Administration. The IP phones that use the RLM Notifier are associated to the CTI Application user.

For more information, see “Configuring the CUCM for the EGW Appliance.”

17.4.2.2 Avaya

The EGW uses the Avaya Push interface to support the Remote Location Manager feature.

The RLM is available to Avaya 46xx and 96xx phones. When a user requests the service, the RLM uses the Display Push capabilities of ACM to send the RLM provisioning page to the WML browser of the Avaya IP phone. The provisioning page allows users to provision emergency locations in real-time.

This feature is configured by adding the URL of the EGW/load balancer to the settings text file (46xx) of the IP phones.

Note: In Aura deployments with multiple CMs it is important that each CM config points to the correct IP-PBX ID configured on the Dashboard. This enables the EGW to keep track of which IP-PBX (CM) the phones are registered to.

For more information, see the document “Configuring the Avaya Communication Manager for the EGW Appliance.”

17.5 Mobile and Remote Access

The Cisco Expressway is a mobile and remote access collaboration gateway that provides many services to remote employees. It enables employees with Cisco Webex Teams and Cisco Jabber softphones installed on their Windows environments to connect to the CUCM without the extra step of establishing a VPN. The Expressway also ensures that your employee's hard phones can access the CUCM and other related services such as the EGW.

The EGW supports remote employees using the RLM application. Remote Cisco Webex Teams and Jabber users can use the RLM without the use of the VPN since the RLM connects to the EGW through the RLM proxy service in the cloud.

The EGW supports off-campus users using the RLM application installed on their Windows OS. EGW connects to the ERS through the RLM proxy service. See [RLM Proxy Uplink Settings](#).

18 System Status

18.1 Overview

This section describes the fields of the web Dashboard administrative interface. The following screens are covered:

- System Status
 - Status
 - Logs
 - Reports
 - CDRs
 - Alarms
 - Maintenance
- Search (ERLs, endpoints)
- Help

18.2 System Status Overview

The status screen is viewable at **System Status > Status**.

The status screen is available to users with Provisioning and Full access.

The status screen may be used to link to other screens that allow you to find and list the following:

- PBX Count (links to **Configuration > IP-PBX**)
- ERLs Count (links to **Search > ERLs**)
- Endpoints Count (links to **Search > Endpoints**)
- Maximum Endpoints Allowed
- Endpoints Count (links to **Provisioning → Endpoints → Endpoints**)
- Billable Endpoints (links to **Provisioning → Endpoints → Endpoints**)
- Provisioned Endpoints Count (links to **Provisioning → Endpoints → Endpoints**)
- Active Alarms Count (links to **System Status > Alarms**)
- Switches Count (links to **Auto Discovery → Layer 2 Discovery → Switch**)
- Discovered Switch Ports Count (links to **Auto Discovery → Layer 2 Discovery → Discovered Ports**)
- Undiscovered Switch Ports Count (links to **Auto Discovery → Layer 2 Discovery → Switch**)
- *WLAN Controller Count (links to **Auto Discovery → WLAN Discovery → Controllers**)
- WLAN Discovered Devices Count (links to **Auto Discovery → WLAN Discovery → Controllers**)
- Dynamic ELINs Available (links to **Provisioning → ELIN Pool**)

*Undiscovered switch ports are all switch ports which could not be associated to a switch (e.g. incorrect port identifiers provided in batch file). For more information, see section 13 “Layer 2 Discovery”.

Note: Dashboard access settings restrict a user’s ability to link to associated screens by clicking on counter numbers.

18.2.1 General Information

The General Information displays some of the most relevant EGW status counters:

Server Role: Reports if the EGW server is Primary or Secondary.

PBX Count: Total number of IP-PBX servers that have been configured for the EGW. Clicking on this directs you to the IP-PBX dashboard screen which displays all of the IP-PBX systems and their configured parameters.

View IP-PBX is available to users with Full access privileges.

ERLs Count:

Maximum Endpoints Allowed: Total amount of all endpoints that you are permitted in the system based on the purchased EGW endpoints license.

Note: When Cisco UWL support is enabled, the parameter “Maximum Endpoints Allowed” comprises the following: standalone endpoints + total number of users.

Endpoints Count: Total number of endpoints in the system that are assigned to a PBX system in the EGW (the endpoint is associated to a PBX ID).

Vendor-specific considerations are also applicable. For more information, see section 7 “Configuring IP-PBX Settings.”

Provisioned Endpoints Count: Total amount of provisioned endpoints in the system.

An endpoint is considered “provisioned” if it has a location (ERL) associated to it.

The Provisioned endpoints count includes ERS endpoints, as well as local trunking endpoints and direct call delivery endpoints.

Billable Endpoints:

Total amount of provisioned endpoints with an ERL configured to route to the ERS. This counter does not include Local Trunking endpoints or Direct Call Delivery endpoints.

For more information, see section 13.5 “Scans.”

18.2.2 Routepoint Status

Routepoint status displays the subscribers that are registered with the primary and secondary EGW routepoints on the various Cisco IP-PBX systems (clusters). The status light report the following:

Green: Route point is up. PBX is connected to at least one server.

Yellow: PBX is in the process of connecting to a server

Red: Route point is down. PBX is not connected to any servers.

Grey: No subscribers are currently assigned to the route point. Data may be pending update.

Orange: Server that is currently assigned to the route point is unreachable.

For more information see section 7.1 “Configuring Cisco UCM Settings.”

18.2.2.1 Reset CTI

You can reset a CTI route point from the route point status dialog box on the System Status screen. CTI route points are restarted on a per EGW server basis (ie. Primary or secondary). When the primary is restarted, for example, the secondary CTI route point will maintain CTI services.

To reset a CTI route point:

1. Click on **System Status>Status**
2. The service will restart when you agree to the prompt. The status of the CTI route point will change to yellow, indicating that route point is connecting. Once the route point is connected the status should change to green

18.2.3 Last 12 Months Endpoints Peak Reported

This counter displays the peak number of billable endpoints on the system per month for a range of 12 months. This number displayed normally equals the **Billable Endpoints** plus the **Billable Users Count**.

For more information concerning endpoint reporting, see the device inventory section for your IP-PBX system in section 7 “Configuring IP-PBX Settings.”

18.2.4 Database Synchronization

If either the primary or secondary EGW database is out of sync, you will see the following error message:

“The databases are not synchronized. Sync to Peer or Sync from Peer.”

If you see this message, you should investigate the database issue and take the required action (Sync to Peer or Sync from Peer). It should be noted that a Sync to Peer or Sync from Peer will completely overwrite the target server, and that care should be taken when performing these actions to avoid loss of data.

For more information, see section 19 “Maintenance.”

18.2.5 Search Layer 3

You may find and display a list of IP subnets by clicking on **Auto Discovery > Layer 3 Discovery**.

This page is only available to users with Provisioning or Full access privileges.

Table 119: Layer 3 Discovery Search Options

Field	Description
Layer 3 Discovery	Type the IP subnet that you would like to display. The search results will automatically change depending on the parameters that are entered in the search box.
Layer 3 Discovery Search Results	Displays the main parameters for the IP subnet: ERL ID, Subnets. Click on More Details to view: Subnet, ELIN, Crisis Email Alert, URL Data, Security Desk Name, Security Desk Number. Click Edit if you would like to add/edit subnet addresses. Click Clear Subnets to remove the subnets from the system.

18.2.6 View Switches

You may find and display a list of configured switches by clicking on **Auto Discovery > Layer 2 Discovery>Switch**

This page is only available to users with Provisioning or Full access.

Table 120: View Switches

Field	Description
Current Switch List	You may view the following parameters from the current switch list: Switch IP, SNMP Community String, SNMP Port, Default ERL ID, Last Update. Click View/Edit to see a list of current switch ports. Click Edit to edit a switch port. Click Add a Switch to add a new switch. Click Batch Upload to upload more than one switch at the same time using a batch file.

18.2.7 View WLAN Controllers and Access Points

You may find and display a list of configured Controllers and access points by clicking on **Auto Discovery > WLAN Discovery**.

This page is only available to users with Provisioning or Full access.

Table 121: View WLAN Controllers and Access Points

Field	Description
Controller Information,	<p>You may view the following parameters from this screen: Controller IP, SNMP Community String, SNMP Port, Description, Vendor, Default ERL ID, AP Scan, SSIDs Supported.</p> <p>Click View/Edit to see a list of current access points</p> <p>Click Edit to edit a switch port.</p> <p>Click Add a Controller to add a new controller</p> <p>Click Batch Upload to upload more than one controller/access point at the same time using a batch file.</p>
Current Access Points	<p>You may view the following parameters from this screen: AP Name, AP Location, AP BSSID, MAC Address, ERL ID, Last Update</p> <p>Click Edit to edit an access point</p> <p>Click Delete to delete an access point</p> <p>Click Add Access Point to add a new access point</p>

18.3 Logs

You may view the logs by clicking on **System Status > Logs**.

Logs are available to users with Full access privileges.

18.3.1 Configuration Logs

Configuration Logs display each system configuration change made from the **Configuration** tab. For example, when changes are made to **Mail Server Settings** or **Global Settings**, they are reflected in the Configuration Logs.

This page is only available to users with Provisioning or Full access.

Table 122: Configuration Logs

Field	Description
Search Logs	Type the date range within which you would like to display all recorded logs. You may click on the calendar drop-down to select the dates from the calendar display box.
Configuration Logs	<p>Displays the following fields: Configuration Name, Action (add, update, delete) Old Value, New Value, Modified By, Time.</p> <p>If there are problems with the configuration, check to see what parameter changed at what time to track down configuration changes that may have destabilized the system. The Modified By field indicates the username of the administrator responsible for the configuration change. The old value may be changed to restore the configuration.</p>

18.3.2 Alarms Logs

Alarms Logs display the complete list of alarms that have been generated to report monitoring and application problems. If a problem is detected, an alarm is generated and a log of the alarm is kept in the **Alarms Logs** section.

This page is only available to users with Provisioning or Full access.

Table 123: Alarm Logs

Field	Description
Alarms Logs Search	Type the date range within which you would like to display all recorded alarms. You may click on the calendar drop-down to select the dates from the calendar display box.
Alarms Logs	<p>Displays the following fields:</p> <ul style="list-style-type: none"> • Alarm ID • Alarm Name • Alarm Information • Alarm Level • Alarm Status • Time Occurred • Alarm Notification Sent • Alarm Cleared By • Alarm Raised By <p>Alarms may be reviewed to pinpoint alarms that are chronic in nature. Administrators may review the logs to see how many are Critical, Warning, or Info.</p>

18.3.3 EGW Debug Logs

The EGW Dashboard provides an interface to collect application logs. The log files can be downloaded as a zipped file including individual text files per log. For each log item it is possible to set the level of log verbosity. Additional information such as a DB backup and packet captures (SIP, H.323 call routing) can also be included as part of the zipped log files.

18.3.3.1 About EGW Application Logs

The default set of logs included in the log file is described below.

Dashboard Configuration-log of operations initiated through the Dashboard

Call Processing Module (CPM)-log of calls processed by the CPM.

Layer 2 Discovery-log of devices discovered by layer 2 discovery, and operations executed by layer 2 scanning module

WLAN Discovery-log of devices discovered by WLAN discovery, and operations executed by WLAN discovery module.

E911 Softphone Locator-logs of ESL push requests and results.

Desk Alert-logs of communications between the desk alert clients and desk alert server on EGW.

Network Configuration-logs of changes made to the networking configuration. Eg. Reactivations, LAN/WAN settings, DNS settings etc.

Licensing-logs of communications between EGW servers and ERS remote licensing server.

Third Party LIS-logs of transactions between Microsoft Lync clients and EGW, when EGW acts as 3rd party LIS interface.

PDM Mac resolver-logs of transactions between the LIS DB and the PDM.

Certificates-Logs pertaining to authentication transactions using certificates.

Tenant Enabler-Logs pertaining to the Tenant Enabler scheduled task.

SOAP 3rd party Layer 2 -logs of SOAP transactions for the third party SNMP soap server on EGW.

SOAP Subnet-SOAP server provisioning transactions for subnets.

SOAP Tenant-SOAP server provisioning transactions for tenants.

Batch Location-Logs of batch file processing. Eg. Modules called, DB insertions, deletions etc.

Batch Endpoint- Logs of batch file processing. Eg. Modules called, DB insertions, deletions etc.

Batch 3rd party Layer 2- Logs of batch file processing. Eg. Modules called, DB insertions, deletions etc.

Batch Switch- Logs of batch file processing. Eg. Modules called, DB insertions, deletions etc.

Default-logs of other operations performed on the EGW.

18.3.3.2 Additional Logs

The additional data which may be exported is described below

Database backup-include a database backup with the debug logs (db_backup.sql).

Packet captures.-include SIP and H.323 packet captures based on log rotate schedule.

System config-include network scripts eth, aliases etc.

Batch Files: Last 5 batch files for endpoints and locations including batch logs

Cisco CTI Logs-include CPM echo requests, code requests, asterisk log package

Microsoft Lync-logs pertaining to Microsoft client location requests with EGW

18.3.3.3 Generate Debug Logs

To generate a Debug log dump

1. Click on **System status>Logs>Debug Logs**
2. Click on **Generate Package**
3. Scroll to bottom of page and click on .gz file to obtain zipped log files.

Setting Log Verbosity:

It is possible to set the log level verbosity for the default set of EGW application logs. This means that you can control the type of events that will be included in the log file for the default modules (set of EGW modules included in the debug logs by default).

The following log verbosity levels are applicable. The selected verbosity level is inclusive with any higher level. For example, a setting of critical will result in events of critical, alert and emergency for the applicable module.

-emergency
-alert
-critical
-error
-warning
-notice
-info
-debug

To set log verbosity:

1. Click on **System status>Logs>Debug Logs**
2. Click on edit within the Configure Debug Log Levels dialog box.
3. Set log verbosity level as required.

Clearing a log file:

You can clear a log file in the situation where you would like to reset the time period within which events will be included in the generated Debug log file. For example, if you are experiencing an error condition for a specific module, it may be useful to clear a log file, to start capturing events from a proscribed moment in time.

To clear a log file:

1. Click on **System Status>Logs>Debug Logs**
2. Click on **Clear Log file** next to the module of choice.

18.4 Reports

Reports may be generated for the following:

- ERLs
- Endpoints
- Subnets
- Switches and ports
- NENA 2
- WLAN Controllers and Access Points
- 3rd party Layer 2
- Users

Reports are viewable by users with Full or Provisioning access privileges.

Description

There are two different report types available on the EGW depending on the report:

- Summary reports
- Export batch reports in CSV and text format
- On-Site summary report
- Off-Site summary report
- All-Endpoints Report
- All Unprovisioned Endpoints Report

Summary reports include all of the data on record for the selected parameter and are generated as .csv files.

Export batch reports are appropriate for restoring configuration or for creating a backup of the configuration, and can be generated as text or CSV files.

To download the reports:

1. Click on **System Status > Reports**.
2. Select the report and report type that you want to view.
3. Click **Generate Report**.

18.4.1 ERL Reports

ERL reports include summary reports and export batch reports in CSV and text formats.

Summary Reports

Summary reports are .CSV files that include all of the information on record for the selected parameter.

The following information is included in the summary report for an ERL:

- ERL ID
- Address*
- Local Gateway Enabled

- Direct Call Delivery
- Remote
- Endpoints Count
- Customer Name
- ELINS
- Security Desk Name
- Security Desk Number
- Subnets
- Crisis Email Alert List

*the fields which are displayed as part of the address information in the report are customizable by modifying the Single Line Address Template. You can modify this template to add, remove or re-arrange the PIDF-LO address fields that comprise the address displayed. For more information see section 8.7 "Customize Address."

Export Batch Reports in text format

The Export Batch file is specially formatted for bulk data upload. In the example below, the operation field has been set to add/update to facilitate the upload process:

```
1;LOC_X;800;MAIN ST;APARTMENT 500;NEW YORK;NY;USA;10044;0;0;O'NEIL
COMPANY;;MONTREAL_PUBLIC_CENTRAL_1;192.168.10.0/24;administrator@companyabc.com
```

Export Batch Reports in CSV format

Batch Reports are also available in CSV format. The following fields are available:

- OPERATION
- ERL_ID
- LOC
- A3
- A1
- COUNTRY
- PC
- NAM
- SECURITY_DESK
- LOCAL_TRUNKING
- DIRECT_CALL_DELIVERY
- HNO
- POD
- STS
- RD
- WIRELESS_LOCATOR
- ELIN
- CRISIS_EMAIL

18.4.2 Endpoint Reports

Endpoint reports can be generated as the following types of reports:

- Export Batch
- On-Site Summary Report
- Off-Site Summary Report
- All Endpoints Report
- All Unprovisioned Endpoints Report

Export Batch Reports

The Export Batch file is specially formatted for bulk data upload. In the example below, the operation field has been set to add/update to facilitate the upload process:

1;LOC_X;; SEP0022156CAA52;;;;

On-site Summary Report

The following information is displayed for on-site endpoint reports:

- IP-PBX Name
- Extension
- MAC Address
- IP Address
- Device Name
- Username
- IP Address
- Display Name
- ERL ID
- Location Assignment Method
- Address
- Local Gateway Enabled
- Direct Call Delivery
- Customer Name
- Subnets
- ELINS
- Crisis Email Alert List
- Security Desk Name
- Security Desk Number
- Switch IP
- Switch Port Name
- Last Update

Off-site Summary Report

The off-site summary reports are for remote users and work-at-home employees.

The following information is displayed for off-site endpoint reports:

- IP-PBX Name
- Extension
- MAC Address
- Device Name
- Username
- Address*

*the fields which are displayed as part of the address information in the report are customizable by modifying the Single Line Address Template. You can modify this template to add, remove or re-arrange the PIDF-LO address fields that comprise the address displayed. For more information see section 8.7 "Customize Address."

All Endpoints Report

The All Endpoints Report will include on-site provisioned, off-site provisioned and unprovisioned endpoints.

*Note: Please note that the All Endpoints Reports must be generated only after running the "**Statistics Scheduled Task**". Failing to do so will result in incorrectly tagging the provisioned endpoints as unprovisioned in the report.*

The following information is displayed for the All Endpoints Report:

- IP-PBX Name
- Extension

- MAC Address
- Device Name
- Username
- IP Address
- Display Name
- ERL ID
- Location Assignment Method
- Address
- Local Gateway Enabled
- Direct Call Delivery
- Customer Name
- Subnets
- ELINS
- Crisis Email Alert List
- Security Desk Name
- Security Desk Number
- Switch IP
- Switch Port Name
- Last Update

All Unprovisioned Endpoints Report

The All Unprovisioned Endpoints Report will show the endpoints that are not provisioned. The following information is displayed for the All Unprovisioned Endpoints Report:

- IP-PBX Name
- Extension
- MAC Address
- Device Name
- Username
- IP Address
- Display Name
- Last Update

18.4.3 Subnets

For subnets, you can generate subnet reports in CSV and text format.

The export batch file is specially formatted for bulk data upload. You can make changes to the CSV or text report file and re-upload to the EGW for batch provisioning of subnets.

Text subnet report example: LOC_X;192.160.10.0/24,192.160.11.0/24,192.160.12.0/24

CSV subnet report example:

	A	B	C
1	OPERATION	ERL_ID	SUBNET
2	1	LOC100	192.168.59.0/24

Figure 68: CSV Subnet Report Example

18.4.4 Switches and Ports

For switches and ports, it is only possible to generate export batch reports.

The export batch file is specially formatted for bulk data upload.

192.168.0.202;;public;0;;LOC_X;13

18.4.5 NENA 2 Reports

A NENA 2 file may be generated from the reports section of the Dashboard.

A NENA 2 report generates a **Full** file that includes an entry for the entire ELIN inventory.

You may change the cycle counter value that will apply to the generated NENA 2 Report. However, this cycle counter value only applies to the generated NENA 2 report, and does not increment the cycle counter value that applies globally to the NENA 2 file generation scheduled task.

To generate a NENA 2 file from the Reports screen

- Click on **System Status > Reports**
- Select **NENA 2** from the **Select Reports** drop down menu
- Enter the appropriate number in the **Cycle Counter** dialog box (if applicable)
- Click **Generate Report**

For more information, see section 16 “NENA 2 Provisioning.”

18.4.6 WLAN and Access Point Reports

Through the EGW dashboard, you can generate WLAN Controllers and Access Point reports. These reports can be exported in CSV format as well as text format. See 15.4 Export WLAN Discovery Details for more details.

You can also edit these reports and re-use them for batch upload.

18.4.7 User Reports

For user reports it is only possible to generate a Summary report.

The file contains a list of all user associated endpoints, followed by the list of standalone endpoints. Endpoints associated to a user id are in bold/italics. The User ID Is listed at the end of each endpoint, and is underlined. Non-bold entries represent Standalone endpoints.

Example:

```
Cisco-Test;;;ERL_1;;;;user1JABBER;user1
Cisco-Test;;;ERL_1;;;;DELLIPCOM;user1
Cisco-Test;;;ERL_1;;;;user2IPCOM;user2
Cisco-Test;;;ERL_1;;;;DELLIPCOM;user2
Cisco-Test;;;ERL_1;;;;user2IPCOM;user2
Cisco-Test;;;ERL_1;;;;user2JABBER;user2
Cisco-Test;;;ERL_1;;;;user3IPCOM;user3
Cisco-Test;;;ERL_1;;;;user3JABBER;user3
Cisco-Test;000413412FE6;;;;SEP000413412FE6
Cisco-Test;001DA266F922;;;;SEP001DA266F922
Cisco-Test;001EF729CEFO;ERL_1;;;;SEP001EF729CEFO
Cisco-Test;C48508FBAB7B;ERL_1;192.168.55.72;;;SEPC48508FBAB7B
```

18.5 Call Detail Records

You may view CDRs by clicking on **System Status → CDRs**.

You can also access CDRs from ftp. CDRs are added to the ftp by a daily scheduled task which appends data to the existing report. The reports are generated on a monthly basis. For more information see section 18.5.2 “CDR Export to FTP.”

This page is only available to users with Provisioning or Full access privileges.

You might need to review CDRs to report on usage or to troubleshoot call routing problems.

Table 124: Call Detail Records

Parameter	Description
Search CDRs	Type the date range within which you would like to display all call detail records. You may click on the calendar drop-down to select the dates from the calendar display box.
Start time	Start time of the call.
Duration (s)	Length of the call in seconds.
Endpoint Caller ID	Extension number of the phone.
ERL ID	The ERL to which the phone is assigned.
Callback Number	The ten-digit number assigned to the phone for the callback. Can be DID, ELIN, or Extension-Bind.
Call Destination	<p>ECRC/PSTN, ERS, Unprovisioned, Security Desk, Local Trunking.</p> <p>ECRC/PSTN: The call was routed to the Emergency Call Response Center by the IP-PBX using PSTN.</p> <p>ERS: The call was routed to the Emergency Routing Service (provisioned call) and was terminated to a PSAP.</p> <p>Unprovisioned: The call was routed to the ERS but no routing instructions could be determined. The call was routed to the ECRC.</p> <p>Security Desk: The call was routed to an on-site security desk.</p> <p>Local Trunking: The call was routed to the local PSAP via the appropriate IP-PBX server, gateway(s) and 911 trunks.</p>
DNIS (Dialed Number)	Displays the number dialed to reach the EGW.
Wave File	<p>Wave file that is generated if the status of the call is Answer.</p> <p>If View Peer is displayed, the wave file is available by logging into the Secondary EGW. This occurs when the primary EGW is unavailable and a call has been delivered to the PSAP using the Secondary EGW. In this scenario, the administrator logs into the Dashboard of the secondary EGW in order to access the wave file.</p>
Call Status	<p>Outcome of the call. There are three settings for call status:</p> <p>Answer: The call was answered by the PSAP.</p> <p>No Answer: The call was terminated before it could be answered by the PSAP.</p> <p>Cancel: The call was terminated by the 911 caller during call setup.</p> <p>Misdial: The call was hung up within the misdial protection timer. The call was not routed to a PSAP.</p>

Parameter	Description
url data	The url link can contain static and dynamic variables that will point to ERL data that you would like to deliver with Desk Alert or Crisis Alert notifications. This ERL data provided in the url link can be used to integrate with other systems.

CDRs allow you to:

- Click on the wave file to listen to the recording of the call.
- Review performance metrics by checking the status of 911 calls (Answer, Busy, or Cancel).
- Filter the logs by month using the search feature to quickly retrieve a specific record.
- Review parameters per call under a variety of troubleshooting scenarios.
- Determine the destination IP and Call Destination of each 911 call

18.5.1 Call Destination

A 911 call may have one of the following destinations: ERS, ECRC/PSTN, Unprovisioned, Security Desk, Local Trunking.

ERS: Provisioned calls are routed to the ERS where they are terminated to the appropriate PSAP.

ECRC/PSTN: If a 911 call cannot be properly processed by the EGW, the call is returned to the IP-PBX with the ten-digit number of the ECRC.

Unprovisioned: If the ERS cannot retrieve routing instructions for a 911 call, the call is routed to the ECRC.

Security Desk: If security desk settings are configured for the ERL, the 911 call is routed to an on-site security desk.

Local Trunking: If local trunking settings are configured for the ERL, the 911 call is routed to the appropriate local PSAP, via the IP-PBX system, gateway(s), and trunks.



Note: You may view the destination IP by hovering the mouse over the entry in the **Call Destination** field.

18.5.1.1 CDRs and the EGW Dial Plan

If you have configured a dial plan number to route emergency calls to a security desk, and if you have set the **Default Security Desk** parameter to **None**, then calls made to those digits from unprovisioned endpoints will be blocked by the EGW. If this is the case for a security desk call instance, the CDR will display **Cancel** as **Call Status**. The **Call Destination** field will display **No Route**.

To learn how CDRs are used for maintenance tasks, see the document “EGW Appliance Standard Operating Procedures.”

To learn how to configure a Multiple Route Plan, see section 5.2 “EGW Dial Plan.”

18.5.2 CDR Export to FTP

CDRs are exported to FTP using the **CDR Export** Scheduled Task. The task is configured to append data to a monthly CDR report on a daily basis. Each time that the report runs, data that is older than 3 years is deleted from FTP.

18.5.2.1 Export CDR File Types

You can configure the **CDR Export** scheduled task to generate CDR reports using the following formats:

- CSV
- Text

It is also possible to setup the scheduled task so that both report types are generated.

To configure CDR Export Format Type

1. Click on **Configuration>Advanced>Global**
2. Select CSV, text or All for the parameter **CDR Export Format Type**

CSV:

The following provides sample output using the CSV setting.

Column CSV header	Description
call_detail_recording_id	id for the CDR record
call_start_time	Start Time
call_end_time	End time
call_duration	Duration (s)
call_endpoint_caller_id	Endpoint Caller ID
call_endpoint_mac_address	Endpoint Mac Address
call_elin_cbn	Callback Number
call_destination_address	Call Destination
call_wave_file_link	Wave File
location_key_id	Location key id
call_status	Call Status
session_id	Session ID
server_type	Server Type
demo_call	Is it a Demo Call?
erl_id	ERL ID
call_destination	Call Destination
building_number	Building Number
street_name	Street Name
address_type	PIDF-LO field: LOC (More precise information about the location)
city	PIDF-LO field: A3 (City, township)
state	PIDF-LO field: A1 (The state or province or county of the location)
country	PIDF-LO field: country (The ISO 3166 alpha-2)
zip_code	PIDF-LO field: PC (Postal Code)
hno	PIDF-LO field: HNO (House number)
hns	PIDF-LO field: HNS (House number suffix)
bld	PIDF-LO field: BLD (Building (structure))
lmk	PIDF-LO field: LMK (Landmark or vanity address)
prd	PIDF-LO field: PRD (Leading street direction)
pod	PIDF-LO field: POD (Trailing street suffix)
sts	PIDF-LO field: STS (Street suffix)
rd	PIDF-LO field: RD (Primary road or street)
rdsec	PIDF-LO field: RDSEC (Road section)
rdbr	PIDF-LO field: RDBR (Road branch)
rdsubbr	PIDF-LO field: RDSUBBR (Road sub-branch)
prm	PIDF-LO field: PRM (Road pre-modifier)
pom	PIDF-LO field: POM (Road post-modifier)
addcode	PIDF-LO field: ADDCODE (Additional code)
seat	PIDF-LO field: SEAT (Seat (desk, cubicle, workstation))
unit	PIDF-LO field: UNIT (Unit (apartment, suite))
room	PIDF-LO field: ROOM (Room)
plc	PIDF-LO field: PLC (Place-type)
flr	PIDF-LO field: FLR (Floor)
a2	PIDF-LO field: A2 (County, parish, district)

a4	PIDF-LO field: A4 (City division, borough, city district, ward)
a5	PIDF-LO field: A5 (Neighborhood, block)
pcn	PIDF-LO field: PCN (Postal community name)
pobox	PIDF-LO field: POBOX (Post office box)
customer_name	PIDF-LO field: NAM (The name of the customer)

Text:

The text file format is used to summarize CDRs one by one. Depending on the global configurable parameter **CDR Export Address Template**, the address will use the single or multiple lines customizable address template.



Note: The EGW uses two address templates to generate output of location data. For example, a multi-line address template will populate the body of crisis email alerts, while the address columns displayed at Search ERLs are defined by the configuration of the Single Line Address Template.

The following provides sample output using the Test file setting.

ID: 235
Start Time: "2010-08-11 23:40"
Duration (s): 54 seconds
Endpoint Caller ID: "John Doe" <19640909>
ERL ID: ERL4
Callback Number: 5145555191
Call Destination: ERS
Wave File: https://192.168.0.21/recording/85486e00-c6411035-56d4-bf00a8c0@192.168.0.191.wav
Call Status: ANSWER
Address: <Single Line Address Template from the Customizable address feature>
or depending on SERVER_CDR_ADDRESS_TEMPLATE
<MultiLine Address Template from the Customizable address feature>

ID: 236
Start Time: "2010-08-11 23:47"
Duration (s): 73 seconds
Endpoint Caller ID: "Jane Doe" <19541350>
ERL ID: No Location
Callback Number: "Jane Doe" <19541350>
Call Destination: ECRC
Wave File: https://192.168.0.21/recording/67c6d480-c6410e56-56cf-bf00a8c0@192.168.0.191.wav
Call Status: CANCEL
Address: <Single Line Address Template from the Customizable address feature>
or depending on SERVER_CDR_ADDRESS_TEMPLATE
<MultiLine Address Template from the Customizable address feature>

18.5.2.2 Accessing Records by FTP

To access records via FTP

1. Open an FTP connection to the EGW using the IP of the EGW, username: cdrftp, password: 911cdr911.
2. Download the CDR report

18.6 Alarms

All the active alarms in the EGW are displayed in the dashboard under **System Status → Alarms**.

The **Alarms** page is only available to users with Provisioning or Full access. The alarms available are categorized by their severity: **Critical**, **Warning** and **Info**.

The **Critical** alarms are represented by a red square; **Warning** alarms by yellow and the **Info** alarms by green.

The header bar displays the severity of the alarm as well as the **Clear** button.

For each alarm you can view: **Alarm ID**, **Alarm Name**, **Alarm Information**, **First Occurrence**, **Last Occurrence**, **Number of Occurrences**, **Number of Notifications Sent**, **Last Notification Sent**, **Last Occurrence Raised By** and **Actions**.

18.6.1 Clearing Alarms

As part of ongoing maintenance, it is necessary to respond to active alarms and resolve them as quickly as possible. Depending on the individual user settings, you will also receive an email notification when the alarm is cleared.

Clearing the alarm removes it from the active alarms list. But the cleared alarm will still be displayed on the **Alarms Logs** page with the status as “**Cleared**”.

You can choose to clear individual or multiple alarms, as described below.

18.6.1.1 Clearing Individual Alarms

Individual alarms can be cleared using the **Clear** button under the **Actions** column.

18.6.1.2 Clearing Multiple Alarms

Multiple alarms or multiple occurrences of the same alarm can be cleared using the **Clear** button on the header row of each alarm category.

To clear multiple alarms:

1. Scroll to the alarm section.
2. In the header row, choose from the dropdown menu beside **Clear All**. You may choose by the alarm severity level or by the Alarm ID.
3. Click on the **Clear** button.

Example 1: For instance, to clear all the alarms with the severity level of **Info**, scroll down to the section where the **Info** alarms are displayed. Choose **Info** in the dropdown menu beside **Clear All** and click on the **Clear** button. This will clear all alarms with the severity level of **Info**.

Example 2: To clear all instances of the **AXL-02** alarm, choose **AXL-02** from the dropdown menu and click the **Clear** button. This will clear all instances of the AXL-02 alarm that have been generated.

19 Maintenance

Using the settings of the maintenance screens you can perform serviceability tasks such as starting/stopping services, running upgrades, changing network settings, or activating new features.

The Maintenance section has the following screens:

1. Server Maintenance
2. Upgrade EGW
3. Network Settings
4. Feature Activation

19.1 Server Maintenance

The following service maintenance actions may be performed:

- Shutdown EGW/Restart EGW
- Sync to Peer, Sync from Peer*
- Lockdown, Unlock
- Stop/Start database replication
- Stop/Start SBC Service
- Enable/Disable Alarms

*Peer refers to the other EGW in the redundant pair.

Shutdown EGW/Restart EGW

You may stop and then restart an EGW server using the EGW Dashboard web interface. You might find this helpful if you are trying to debug a problem, or during data center/server room maintenance activities.

To shutdown/restart an EGW server

1. Click on **System Status > Maintenance > Server Maintenance**.
2. Click **Shutdown EGW** or **Restart EGW**.
3. When you click **Shutdown**, the message “Are you sure you want to shut down the EGW” displays.
4. If you click **Yes**, you are logged out of the interface and the EGW is turned off.



Note: If the EGW is turned off from the server maintenance screen, the EGW must be manually powered up to resume functionality.

1. When you click **Restart EGW**, the message “Are you sure you want to reboot the EGW” displays.
2. If you click **Yes**, you are logged out of the interface and the EGW restarts.



Note: It may take a few minutes before you may log back into the EGW administrative interface.

Sync to Peer/Sync From Peer

Your network monitoring staff will receive alerts when problems with EGW services are detected. These alerts report on service states and running processes, and will report when the EGW databases are out-of-sync. If a database out-of-sync alert is received, re-synchronization may be performed using the Dashboard interface.

To re-sync an EGW

1. Click on **System Status > Status** (the databases out-of-sync error message is displayed on the status screen).
2. Click on **Sync to Peer** or **Sync from Peer**.

You may sync either EGW from the administrative Dashboard of both the Primary and Secondary servers.

Examples:

- If you are logged into the Primary EGW and the Secondary EGW is out of sync, click on **Sync to Peer**.
- If you are logged into the Primary EGW and the Primary EGW is out of sync, click on **Sync from Peer**.
- If you are logged into the Secondary EGW and the Primary EGW is out of sync, click **Sync to Peer**.
- If you are logged into the Secondary EGW and the Secondary EGW is out of sync, click **Sync from Peer**.

Note: Performing a Sync to Peer or Sync from Peer will overwrite data on the target server. As such, care should be taken before performing either of these operations.

Lockdown/Unlock

See section **Error! Reference source not found. “Error! Reference source not found..”**

Enable/Disable alarms:

You can disable the alarms on an EGW server if you would like to perform networking changes/maintenance without triggering alarm notifications in the process. To perform the required action, simply click on the button of your choice.

To Enable/ Disable alarms:

1. Go to **System Status** → **Maintenance** → **Server Maintenance**.
2. Under the **Actions** section, you can choose to **Disable Alarms** or **Enable Alarms**.

Note: When alarms are disabled, EGW will display a message on top of the screen saying “EGW ALARMS ARE DISABLED!”.

19.2 Network Settings

Network settings include basic network connectivity information such as server hostname, IP, mask and gateway.

You can view your network settings at **System Status>Maintenance>Network Settings** to make changes.



Note: After first run configuration/activation, changes to your network settings (eg. Changing an EGW IP address, NIC card, or server assignment) will deactivate your EGW and your EGW will be put into Grace mode. You will need to re-activate by clicking on the Re-activate button.

For more information concerning Grace mode see section 19.2.3 “Grace Mode”

To change the network settings

1. Click on **Network Configuration**
2. Configure the information included in the table below
3. Click on **Apply Settings**

Network Configuration:

Table 125: Network Settings

Field	Description	Note
Server Type	Select primary, secondary, or standalone. Delegates the EGW instance as either the primary or secondary for redundancy. The EGW can also be activated without a Peer, in standalone mode.	If you are operating in Redundant mode, ensure that you configure one primary EGW server and one secondary EGW server. In standalone mode, only one EGW server is necessary, and replication setup is not required.

Hostname	Hostname for the EGW server. Eg. CompanyXEGWPrimary, CompanyXEGWSecondary.		
Domain name	Domain name for the egw server. Eg. www.egw.com		
Interface 0	IP address	IP address assigned to Interface 0 on the EGW	The EGW has two NIC cards that can be configured to suit the needs of your networking environment. For more information see section 3.1.1 "Network Interfaces."
	Network mask	Network mask for Interface 0	
	Default gateway	Default GW for Interface 0	
Interface 1 (optional)	IP address	IP address assigned to Interface 1 (optional)	The EGW has two NIC cards that can be configured to suit the needs of your networking environment. For more information see section 3.1.1 "Network Interfaces."
	Network mask	Network mask on Interface 1	
	Default gateway	Default Gateway of Interface 1	
Primary DNS	IP address or FQDN of the primary DNS server for the EGW.		
Secondary DNS	IP address or FQDN of the secondary DNS server for the EGW.		
NTP Server	NTP server name(s) added to the pool. The format name: centos.pool.ntp.org. To add new server name click on Add Server. To delete server name click the delete button next to the server name.		

19.2.1 Replication Setup

If you will be using the EGW in redundant mode, replication setup must be successfully completed before the activation process can take place. Replication setup is not required in standalone mode.

To enable replication setup

1. Enter the Peer IP and Peer hostname under **Replication Setup**
2. Click on **Apply settings**

19.2.2 Deactivate EGW

You can deactivate the EGW from the Network Settings screen. When the EGW is deactivated the web interface will display the EGW Reactivation screen (the Network Configuration and Replication Setup screens are also available). Deactivation is the only means by which you change the server type (primary/secondary) of an EGW.

To deactivate an EGW

1. Click on **System Status>Maintenance>Network Settings>Deactivate EGW**
2. Click Deactivate EGW
3. The EGW is deactivated and the web interface displays the EGW Reactivation screen

19.2.3 Grace Mode

If you make changes to your networking settings (eg. Changing an EGW IP address, NIC card, or server assignment), your EGW will become de-activated. When an EGW is de-activated it goes into grace mode.

In Grace mode, the following functionality is observed:

- **EGW functionality is unaffected**
- Administrative Dashboard access is limited to the Activation/re-activation screen

The length of the grace period is precisely 3 days from the time that the EGW went into grace mode. After the grace mode period has elapsed the EGW goes into inactive mode. A reminder alarm/email notification is raised every 24 hours while the EGW is in grace mode.

For more information on inactive mode see section 19.2.4 “Inactive Mode”

To move out of grace mode, and re-activate your EGW license, simply click Reactivate. Provided that there are no problems with your license, the EGW will be immediately re-activated to the Full license. You can also re-activate manually. For more information concerning manual re-activation, see section 2.3.2 “Activation.”

When an EGW goes into grace period, an alarm is raised for immediate notification. In addition, every 24 hours while in grace period, the EGW will generate a grace period notification alarm/email, as a reminder that you should take action.



Note: A software license will enable you to change a server IP address 3 times. Each time that an IP is changed, your EGW will go into Grace mode and will need to be re-activated. If you change the IP address for a fourth time, the EGW will go into inactive mode, and the re-activation process will be unsuccessful. You will need to contact Intrado.

19.2.4 Inactive Mode

An EGW will go into Inactive mode if the Grace period has elapsed. The grace period is precisely 3 days after the point at which the EGW was de-activated and put into Grace mode.

In inactive mode, the following is observed:

- **EGW functionality is suspended**

- Administrative Dashboard access is limited to the Activation/re-activation screen

In Inactive mode, the EGW call processing module is inactive. Your IP-PBX will route calls to the emergency call response center (ECRC) via local gateways and trunks.

To move out of inactive mode, and re-activate your EGW license, you will need to contact Intrado and reactivate automatically or manually.



Note: Before you can re-activate your license from inactive mode you will need to contact Intrado.



Note: the expiration of the trial period will also cause the EGW to go into inactive mode. To extend the trial period or purchase a Full license you will need to contact Intrado.

19.3 Upgrade EGW

The EGW can be upgraded to a minor or a major version through the EGW dashboard. Major upgrades are performed through ISO files whereas minor upgrades are performed through upgrade script files. All the upgrade files required will be provided to you by the Intrado deployment staff.

Prior to starting the upgrade procedure, the following steps need to be performed:

- Database replication between the primary and the secondary EGW must be stopped.
- The EGW that you wish to upgrade must be put in lockdown mode.

The **Upgrade EGW** tab enables you to perform the upgrade through the dashboard. It contains the following columns: **File Name**, **Size** and **Status**. Using the **Add Files** and **Start Upload** buttons, you can choose the upgrade file and upload it into the EGW.

This page also contains a table with the **File Name**, **File Size**, **Last Modified**, **Log File**, **Status** and **Action** columns to give you a real-time status of the upgrade procedure.

Please note the following points prior to starting the upgrade:

- *If the EGW is not locked down, the user will be unable to perform the upgrade.*
- *Only users with "Full" access can perform the upgrade.*

19.3.1 Requirements

To upgrade the EGW to the latest software version or patch, you must hold a valid EGW license and an up-to-date support agreement in place. Before the upgrade file is processed, the EGW will check with the Intrado licensing server to verify that the license is valid. If the license check fails, the upgrade will not proceed.

19.3.1.1 Backup

Prior to starting the upgrade procedure, a backup copy of the EGW must be made.

For small VM EGWs (less than 300 GB), a snapshot must be taken using the VMware vSphere client. For more information on how to do this, please refer to the *VMware ESX Host EGW Installation Guide*.

For large VM EGWs (more than 300 GB) and hardware EGWs, a physical backup copy of the current version of the EGW must be made. To do this, perform the following steps:

1. Stop **MySQL** using this command: `systemctl stop mysql`
2. Take a snapshot of the EGW using this command: `/opt/911Gateway/sudo/egwSnapshot`

The above step copies the entire content of the root partition to the backup partition and creates a log file under `/tmp/egwSnapshot-YYMMDD-HHMMSS.log`.

3. Restart MySQL using this command, once the backup is completed: `systemctl start MySQL`.

19.3.2 Upgrade Procedure

It is strongly recommended to upgrade the secondary EGW first. This is to ensure that emergency calls can be handled by the primary EGW when the upgrade is being performed.

Please perform the following steps to upgrade the EGW using the dashboard:

1. Login to the EGW dashboard.
2. Go to **System Status**→ **Maintenance**→ **Upgrade EGW**.
3. Click on the **Add Files** button and browse the file you want to upload. You may also drag and drop the upgrade file into the window.
4. Once the file is uploaded, click on the **Start Upload** button.

The file now undergoes a preliminary validation process to ensure that it is valid.

If the file is deemed invalid, an error message saying that “The File you attempted to load is invalid” is displayed.

If the file is valid, it is accepted and inserted and the **Status** is changed to **Uploaded**. In addition, the EGW also analyses the file to determine whether the upgrade file uploaded will result in a minor or a major upgrade.

*Please note that at this stage, if the **Run Upgrade** button is greyed out and inactive, then the EGW was not locked down. Please lockdown the EGW in order to continue with the upgrade operation.*

5. Now click on the **Run Upgrade** button. This will check the validity of the license to ensure that the user can in fact perform an upgrade and then execute the upgrade.

At this state, all the buttons on this page are disabled and the **Status** is changed to **Installing**. Log file is also available for the user to view the progress of the installation in real time.

Special Consideration- Manual Upgrade

There are cases where automatic upgrade may not be possible. For instance, when the EGW is not allowed to connect outside of the corporate network. In this situation, manual upgrade is the recommended solution. The manual upgrade authentication screen is displayed if you attempt to upgrade the EGW without a connection to the internet. However when performing a manual upgrade, you will have to contact the Intrado technical support staff.

To perform a manual upgrade:

1. Copy the key displayed in the **Manual Upgrade Authentication** screen
2. Provide this key to your Intrado support staff.
3. Obtain the **Activation code** from the support staff.
4. Paste the **Activation code** into the appropriate field on the **Manual Authentication** screen.
5. Click **OK**.

19.3.2.1 Results of the Upgrade

After the EGW upgrade is executed, the Status column on this page can take the following values:

- Successful
- Intervention Required
- Failed

Depending on the outcome, user actions are required, as explained below:

19.3.2.1.1 Successful

When **Successful** status is displayed, this means that the upgrade was successful. Please follow the **Post Upgrade Procedure** to complete the installation.

19.3.2.1.2 Intervention Required

When **Intervention Required** status is required, this means that the upgrade did not complete and user intervention is required to complete the upgrade. The **Action** column is greyed out and the **Intervention Required** link becomes active. The EGW remains locked down at this stage.

The **Intervention Required** link displays the path to the files with “rpmnew” and/or “rpmsave” extension that were detected. For example: These files need to be deleted to proceed with the upgrade. Please call the Intrado support staff to address these files.

If all files have been addressed, the **Status** will change to **Successful**.

Finally, follow the **Post Upgrade Procedure** to complete the installation.

19.3.2.1.3 Failed

This means that the upgrade failed. Please contact the Intrado Support staff for assistance. Meanwhile, you can revert to the initial version of the EGW, if required.

19.3.2.1.4 Reversion

If during the upgrade, the installation fails, the EGW can be reverted to its original state using the snapshot or the backup copy.

For small EGW VMs, the EGW can then be reverted to the snapshot created using the VMware vSphere Client.

For hardware and large EGW VMs, see the following commands to revert to the initial EGW version:

```
systemctl stop
mysql/opt/911Gateway/sudo/egwSnapshot --revert
systemctl daemon-reload
systemctl start mysql
```

A reboot will be required after the reversion.

19.3.2.1.5 Reboot

When a major upgrade is performed, a message appears prompting the user to reboot the EGW to complete the installation process.

19.3.3 Post Upgrade Procedure

After the upgrade of the EGW has been successful, the following actions need to be performed:

1. Unlock the EGW that was just upgraded.
2. Reboot the EGW, if a major upgrade was performed.
3. Perform test calls to verify 911 call functionality and quality.
4. Now lockdown the secondary EGW and perform the upgrade on the Secondary EGW and then perform the previous three steps.
5. Finally, restore replication between the Primary and the Secondary EGW.

19.3.3.1 Log File

Log files are available under the **Log File** column. Log files are produced under the following circumstances:

- When the upgrade file is installing
- When the upgrade was successful or has failed
- When user intervention is required

19.4 Help

The **Help** tab on the Dashboard allows administrators to view support contact information and user documentation.

Support Info

The **Support Info** page displays a link to Intrado's email support, website, and support site. These links can be used to submit trouble tickets and view additional documentation.

About

Displays the software version number and the license key.

Documentation

Displays links to the Technical Resource Center that contains the EGW System Guide as well as all related configuration guides.

20 EGW Alarms

The EGW sends alarm notifications via email or SNMP traps for EGW application alarms and service/host alarms.

Various application modules of the EGW will raise alarms under various error conditions.

The following modules will raise alarms:

- AXL
- Configuration
- CTI
- Dashboard
- Discovery
- Monitoring
- Routing
- Scheduler
- System Status

Furthermore, the EGW will also raise alarms and notifications will be sent if it detects any issues with its services. The EGW servers are themselves self-monitored and will raise host alarms.

20.1 EGW Application Alarms by Module

This section describes the various alarms that are available on the EGW. They are separated by module. In addition, the user can set the severity level and the frequency of each alarm using the Alarm Frequency settings page.

20.1.1 AXL

Alarm ID	Alarm Name and Description	Level (Default)	Frequency (Default)	Troubleshooting Guidelines/ Actions to perform
AXL-01*	AXL - Failed to complete for the PBX AXL could not complete for the PBX. <i>Note: The description for this alarm displayed on the dashboard could be different when there are connection or configuration issues pertaining to AXL. See section 20.1.1.1 Special Considerations for more information.</i>	Warning	Always	This alarm is raised when the AXL process fails for a PBX. Actions: If this issue is occurring frequently, further investigation is required. Could be caused by AXL application user permission/missing roles, internal firewalls blocking EGW connectivity to CUCM cluster (port 443 and 8443), application user credentials mismatch, CUCM services disabled.
				Clearing Instructions: When the AXL runs successfully in subsequent runs for the same PBX for which the alarm was raised.
AXL-02	AXL - Failed to retrieve IP Addresses from CUCM AXL query used to retrieve phones failed.	Warning	Always	This alarm is raised when the AXL is unable to connect to the PBX for getting the IP of devices. Actions: If this issue is occurring frequently, further investigation is required. Could be

Alarm ID	Alarm Name and Description	Level (Default)	Frequency (Default)	Troubleshooting Guidelines/ Actions to perform
				<p>caused by AXL application user permission/missing roles, internal firewalls blocking EGW connectivity to CUCM cluster (port 443 and 8443), application user credentials mismatch, CUCM services disabled.</p> <p>Clearing Instructions: When the AXL runs successfully in subsequent runs for the same PBX for which the alarm was raised.</p>
AXL-03*	<p>AXL - Failed to retrieve phones from the CUCM</p> <p>AXL query used to retrieve phones failed.</p> <p><i>Note: The description for this alarm displayed on the dashboard could be different when there are connection or configuration issues pertaining to AXL. See section 20.1.1.1 Special Considerations for more information.</i></p>	Warning	Always	<p>This alarm is raised when AXL is unable to get devices from the CUCM.</p> <p>When the AXL runs successfully in subsequent runs for the same PBX for which the alarm was raised.</p> <p>Actions: Verify that the login settings for the Cisco AXL service are correct. If Secure AXL is in use, ensure that port 8443 is not blocked. If secure AXL is not in use, ensure that port 80 is not blocked.</p> <p>Any IP phone adds or changes will not be provisioned by the EGW.</p> <p>Clearing Instructions: When the AXL runs successfully in subsequent runs for the same PBX for which the alarm was raised.</p>
AXL-04	<p>AXL - Peer Check Failed</p> <p>AXL encountered an exception while checking the status of the peer EGW in its database.</p>	Critical	Once an hour	<p>This alarm is raised when AXL is unable to get the status of the peer EGW from its database.</p> <p>Actions: Verify the Peer status, to ensure that the EGW servers are properly reporting the Server Role Parameter.</p> <p>Clearing Instructions: When the peer checks passes in its next run. Peer check happens every 5 seconds.</p>
AXL-05*	<p>AXL - Failed to retrieve Device Names from CUCM</p> <p>AXL query used to retrieve Device Names failed.</p> <p><i>Note: The description for this alarm displayed on the dashboard could be different when there are connection or configuration issues pertaining to AXL. See section 20.1.1.1 Special Considerations for more information.</i></p>	Critical	Always	<p>This alarm is raised when the AXL is unable to connect to the PBX for retrieving the device names.</p> <p>Actions: If this issue is occurring frequently, further investigation is required. Could be caused by AXL application user permission/missing roles, internal firewalls blocking EGW connectivity to CUCM cluster (port 443 and 8443), application user credentials mismatch, CUCM services disabled.</p>

Alarm ID	Alarm Name and Description	Level (Default)	Frequency (Default)	Troubleshooting Guidelines/ Actions to perform
				<p>Clearing Instructions: When the AXL runs successfully in subsequent runs for the same PBX for which the alarm was raised.</p>
AXL-06	<p>Spark client could not be provisioned.</p> <p>AXL was unable to match a Device Name to a Spark client on the CUCM.</p>	Info	Once a day	<p>Raised when the AXL task is unable to find a device name that matches the Spark user information supplied by RLM or ESL (First, middle and last name, Email address, account name).</p> <p>Actions: Make sure that the user information being retrieved from the Active Directory on the client computer matches the information being retrieved from the Active Directory on the CUCM:</p> <ul style="list-style-type: none"> • First + middle + last name • Email address • Account name <p>At least one of the above must match between the client and CUCM Active Directory data.</p>

20.1.1.1 Special Considerations

On the occasion that AXL is experiencing connection issues or the AXL preferences have not be properly configured, the AXL alarms **AXL-01**, **AXL-03** and **AXL-05** will display one of the following associated messages:

Alarm ID	Alarm Name and Description	Level (Default)	Frequency (Default)	Troubleshooting Guidelines/ Actions to perform
AXL-01, AXL-03, AXL-05	Cause: Connection issue on AXL IP port ##### and IP-PBX ID ##.	Warning	Always	<p>If this issue is occurring frequently, further investigation is required. Could be caused by AXL application user permission/missing roles, internal firewalls blocking EGW connectivity to CUCM cluster (port 443 and 8443), application user credentials mismatch, CUCM services disabled.</p> <p>Clearing Instructions: When the AXL runs successfully in subsequent runs for the same PBX for which the alarm was raised.</p>

Alarm ID	Alarm Name and Description	Level (Default)	Frequency (Default)	Troubleshooting Guidelines/ Actions to perform
AXL-01, AXL-03, AXL-05	Cause: AXL Preferences not properly configured for IP-PBX ID ##.	Warning	Always	Review and ensure that the AXL preferences are configured properly.
				Clearing Instructions: When the AXL runs successfully in subsequent runs for the same PBX for which the alarm was raised.

20.1.2 Configuration

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
CFG-01	LDAP Directory is not available. Dashboard failed to reach the requested LDAP Directory for user authentication.	Warning	Once an hour	Check if LDAP directory is available. Actions: Check the LDAP servers' configurations on the EGW Dashboard. Make sure that servers are reachable from the EGW on the selected ports.
				Clearing Instructions: This alarm will be cleared when the LDAP directory is reachable on the next LDAP connection.
CFG-02	LDAP server unreachable Dashboard failed to reach LDAP server for user authentication.	Warning	Once an hour	Check if a LDAP server is reachable. Actions: One of the configured servers is not responding. Check the LDAP server configurations on the EGW Dashboard. Make sure the server is reachable from the EGW on the selected port.
				Clearing Instructions: This alarm will be cleared when the LDAP directory is reachable on the next LDAP connection.
CFG-03	Location Server Misconfiguration A Location Server has a bad configuration that prevents the EGW to locate a user.	Warning	Once an hour	Check if the location server authentication is successful. Actions: Verify System Management URL is configured correctly in the Local Servers settings under Auto Discovery > WLAN Discovery > Location Servers . Verify username/password credentials to connect to the associated Location Service are correct.

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
				Clearing Instructions: This alarm will be cleared when the Location Server is authenticated properly on the next scan
CFG-04	Location Server Time Out The communication with the location server timed out.	Warning	Once an hour	<p>This alarm is raised when there is a communication timeout with a location server.</p> <p>Actions: Verify System Management URL is configured correctly in the Local Servers settings under Auto Discovery > WLAN Discovery > Location Servers.</p> <p>Verify username/password credentials to connect to the associated Location Service are correct.</p>

20.1.3 CTI

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
CTI-01	CTI could not create Routepoint The CTI service on EGW could not create terminal on the PBX	Critical	Once an hour	<p>This alarm is raised when the CTI is unable to connect with the CUCM</p> <p>Actions: Verify firewall and ACL settings and verify connectivity between the CTI Server and the EGW.</p> <p>Ensure that TCP port 2748 is not blocked to the CUCM from the EGW.</p>
				Clearing Instructions: This alarm will be cleared when the CTI Server is back up on the next Cisco check.
CTI-02	CTI server login failure The CTI service on EGW could not login on the PBX with the configured credentials	Critical	Once an hour	<p>Check that the login to the Cisco Call Manager is successful.</p> <p>Actions: Please verify username and password and ensure Call Manager server is on.</p>
				Clearing Instructions: This alarm will be cleared on the next successful login to the CUCM .
CTI-03	RLM Notifier CTI Login failed The RLM Notifier service on EGW could not login on the PBX with the configured credentials	Warning	Once an hour	<p>Check that the login to the RLM Notifier CTI is successful.</p> <p>Actions: Verify that the RLM Notifier login settings are correct.</p>

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
				Clearing Instructions: This alarm will be cleared when the login to the RLM notifier is successful on the next Cisco scan.
CTI-04	RLM Notifier push to phone failed RLM Notifier Push failed. The EGW was unable to display the RLM provisioning page to a Cisco phone.	Info	Once a day	Notification error sent when the PUSH failed. Actions: Verify that the RLM Notifier login settings are correct.
CTI-05	The CTI Service is flapping EGW has detected that the CTI Service is flapping	Warning	Once an hour	This alarm is raised by the CTI service when it notices that the connection with the CUCM flaps. Actions: Please ensure that there are no network problems between the EGW and CUCM. In the absence of any network issues, ensure that the CUCM CTI service is stable.

20.1.4 Dashboard

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
DSH-01	Dashboard login failed. User failed to login to the Dashboard.	Warning	Once an hour	Notification error sent when the login to the dashboard is failing. Actions: Verify username and password is correct. If problem persists, please contact EGW system administrator and/or the Intrado Support team.
DSH-02	Sending test SNMP trap* A test SNMP trap was sent.	Info	Always	Notification when sending a test SNMP Trap. Actions: The user does not need to take any action for this alarm.

20.1.5 Discovery

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
DIS-01	<p>Layer 2 Discovery - Could Not Scan Switch</p> <p>Layer 2 Discovery encountered an exception while scanning a switch.</p>	Warning	Once an hour	<p>This alarm is raised when Layer 2 Discovery could not scan the switch.</p> <p>Actions: The user needs to perform the following actions:</p> <ul style="list-style-type: none"> • Verify that the switch IP is reachable via the EGW. • Verify the switch IP is correct. • Verify the switch community string and/ or ACL settings are correct. • Verify any firewall logs that could be blocking UDP/Port 161 traffic between the EGW and the specified switch/ network.
DIS-02	<p>Layer 2 Discovery - Duplicate MAC Found</p> <p>Layer 2 Discovery found a MAC active on more than one switch.</p>	Warning	Once an hour	<p>This alarm is raised when Layer 2 Discovery could not resolve a MAC to its port.</p> <p>Actions: Verify the alarm log to obtain the specific switches and ports where the duplicates have been detected. In addition, verify that the persistent MAC address feature has not been enabled on the switch configuration.</p>
DIS-03	<p>Layer 2 Discovery - Invalid Scan</p> <p>Layer 2 Discovery did not get any MACs from a switch.</p>	Warning	Once an hour	<p>This alarm is raised when Layer 2 Discovery did not retrieve any forwarding MACs.</p> <p>Actions: The user needs to perform the following actions:</p> <ul style="list-style-type: none"> • Verify that the switch is reachable. • Verify if the community string is valid. • Verify that devices are attached to the switch at the time of scan. • Verify if the SNMP Timeout setting is not set too low at the EGW. • Ensure that the switch type setting is accurate, or enable auto-detect for the EGW to automatically detect the switch type. • Check the Switch type or set it to Auto-Detect. <p>Clearing Instructions: This alarm will be cleared when the Layer 2 Discovery is able to scan the switch during the next scheduled run.</p>

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
DIS-04	Layer 2 Discovery - MAC Location Has Changed Layer 2 Discovery changed the location of a MAC.	Info	Never	This alarm is raised when Layer 2 Discovery is moving a MAC to a different location. Actions: No action is required on the user's part.
DIS-05	Layer 2 Discovery - MAC Location Has Changed To ECRC Layer 2 Discovery changed the location of a MAC to ECRC.	Warning	Always	This alarm is raised when Layer 2 Discovery is moving a MAC to ECRC. Actions: Investigate why the endpoint is no longer being provisioned to an ERL
DIS-06	Layer 2 Discovery - Peer Check Failed Layer 2 encountered an exception while checking the status of the peer EGW in its database.	Critical	Once an hour	This alarm is raised when Layer 2 Discovery is unable to get the status of the peer EGW from its database Actions: Verify the Peer status, to ensure that the EGW servers are properly reporting the Server Role Parameter.
DIS-07	WLAN Controller is unreachable WLAN Discovery encountered an exception while scanning a controller.	Warning	Once every 15 minutes	This alarm is raised when the WLAN Discovery could not scan a controller. Actions: The user should perform the following actions: <ul style="list-style-type: none"> Verify SNMP community string is correct Verify that the Controller IP is reachable from the EGW. Verify the internal firewall logs (UDP/ Port 161) for connectivity issues between WLAN controller and the EGW attempting to scan the controller. Please contact the Intrado support team if the problem is persistent.
				Clearing Instructions: This alarm will be cleared when the WLAN controller can be reached on the next scheduled WLAN scan.

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
DIS-08	Wlan Discovery - Multiple Access Points found for a BSSID WLAN Discovery found more than one Access Points linked to the same BSSID.	Critical	Once an hour	This alarm is raised when more than one access point is found for a BSSID. Alarm will be raised even if the same ERL is assigned to both access points. Actions: Please check the configuration of the WLAN controller(s). It is possible that the multi BSSID mask is too generic and provides multiple access points for the same BSSID.
				Clearing Instructions: The user should manually clear this alarm after correcting the WLAN configuration. Or else, the alarm will be raised as per the default frequency settings.

20.1.6 Monitoring

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
MON-01	All routes are down EGW has detected that all routes are down.	Critical	Once every 5 minutes	Check if all peers are down (ERS, IP-PBX servers). Actions: The user should: <ul style="list-style-type: none"> Verify firewall logs for connectivity issues, blocking SIP tcp/5060 and/or udp/5060 originating from the EGWs to the ERS SIP peers. Verify NATing of private IPs to public IPs has not been altered, which would prevent deep packet translation of private IPs to the expected public IPs in the SIP payload.
				Clearing Instructions: This alarm will be cleared when at least one of the peers is reachable on the Peer Monitoring scheduled task.
MON-05	EGW license successfully activated The EGW license was successfully activated. The EGW is now active.	Critical	Never	Notification to let the user know that the EGW is successfully activated Actions: The user does not need to perform any action when this alarm is raised.
MON-06	EGW licensing problem: Entering Grace Period.	Critical	Once a day	Notification to let the user know that the EGW is entering the grace period mode.

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
	The EGW is currently in Grace mode. EGW functionality is unaffected, but web Dashboard access has been limited. Full functionality of the EGW will be maintained for 3 days, at which point the EGW will be deactivated. Please obtain web access to the EGW and click on re-activate, or perform a manual activation.			Actions: Please contact the Intrado support team for assistance
MON-07	EGW licensing problem: Grace period over Grace period for this EGW has expired, and the EGW has been deactivated. EGW functionality has been suspended.	Critical	Always	Notification to let the user know that the grace period is over and the EGW is locked down. Actions: Please contact the Intrado support team for assistance.
MON-08	EGW licensing problem: Reminder EGW currently in grace period Reminder for EGW currently in grace mode.	Critical	Once a day	Notification to remind the user that the EGW is now in Grace mode. Actions: Please contact the Intrado support team for assistance.
MON-09	Unreachable ERS server. EGW has detected that one of the links to the ERS is down.	Warning	Once an hour	Notification to let the user know that the EGW is unreachable. Actions: Verify firewall logs for connectivity issues, blocking SIP TCP/5060 and/or UDP/5060 originating from the EGWs to the ERS SIP peers. Verify NATing of private IPs to public IPs has not been altered, which would prevent deep packet translation of private IPs to the expected public IPs in the SIP payload.
				Clearing Instructions: This alarm will be cleared when the corresponding ERS host is reachable on the Peer Monitoring scheduled task.
MON-10	Unreachable PBX Server. EGW has detected that a PBX server node is unreachable.	Warning	Once an hour	One of the PBX is unreachable. Actions: Verify firewall logs for connectivity issues, blocking SIP TCP/5060 and/or UDP/5060 originating from the EGWs to the PBX SIP peers.
				Clearing Instructions: This alarm will be cleared when the corresponding IP-PBX server is reachable on the Peer Monitoring scheduled task.

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
MON-11	RLM Proxy Uplink Failed Connectivity to RLM Proxy server was lost.	Warning	Once an hour	Alarm to let the user know that connection to the RLM Proxy Uplink was lost. Actions: Verify firewall logs for connectivity issues, blocking SIP TCP/5060 and/or UDP/5060 originating from the EGWs to the PBX SIP peers.
	Clearing Instructions: This alarm will be cleared when the corresponding uplink gets re-established.			
MON-12	Logged in users warning Alarm has been raised to inform you that 20 users are logged into the EGW through SSH.	Info	Once an hour	This alarm is raised when 20 or more (but less than 50) users are logged into the EGW through SSH. This could be the result of one or more of the following conditions: <ul style="list-style-type: none"> • Malfunction of the SSH connection used between the EGW peers. • New connections are being made to the EGW without deleting the older connections. Could indicate automated logins. Actions: Identify all active SSH sessions and the users and IP addresses that have established the sessions. If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
	Clearing Instructions: This alarm is automatically cleared when the number of logged in users falls below 20.			
MON-13	Logged in users critical Alarm has been raised to inform you that 50 users are logged into the EGW	Warning	Once an hour	This alarm is raised when 50 or more users are logged into the EGW through SSH. This could be the result of one or more of the following conditions: <ul style="list-style-type: none"> • Malfunction of the SSH connection used between the EGW peers. • New connections are being made to the EGW without deleting the older connections. Could indicate automated logins. Actions: Identify all active SSH sessions and the users and IP addresses that have established the sessions. If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
				Clearing Instructions: This alarm is automatically cleared when the number of users logged into the EGW falls below 50.
MON-14	SSH Unavailable The primary EGW's SSH service is unavailable since port 22 cannot be reached.	Warning	Once an hour	Alarm to inform the user that the SSH port (port 22) on the local EGW cannot be accessed. Actions: If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
				Clearing Instructions: This alarm is automatically cleared when EGW's SSH service becomes available.
MON-15	Local HTTP Unavailable HTTPD service is unreachable on the Primary EGW.	Critical	Once every 15 minutes	Alarm to inform the user that the local HTTPD service is unreachable. Actions: If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
				Clearing Instructions: This alarm is automatically cleared the primary EGW's HTTPD service becomes available.
MON-16	Peer HTTP Unavailable HTTPD Service is unreachable on the peer EGW	Critical	Once every 15 minutes	Alarm to inform the user that the peer HTTPD service is unreachable. Actions If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
				Clearing Instructions: This alarm is automatically cleared the peer EGW's HTTPD service becomes available.
MON-17	Local EGW DB Unavailable The Primary EGW'S database cannot be accessed Alarm information displayed is one of the following: a. Slave IO: No Slave SQL: No Seconds Behind Master: (null) b. Cant connect to MySQL server on 999.999.999.999(999) c. Unknown database 'gateway_db'	Critical	Once every 15 minutes	Alarm raised to inform you that one of the conditions displayed in the "Alarm Information" section is present. Please see below for detailed description of the condition shown in the "Alarm Information": a. Slave IO: No Slave SQL: No Seconds Behind Master: (null): Indicates that MySQL replication between the EGW peers is broken. If you have manually stopped the replication for maintenance purposes, this alarm can be ignored. b. Cant connect to MySQL server on 999.999.999.999(999): Indicates that

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
				<p>the local MySQL server cannot be reached.</p> <p>c. Unknown database 'gateway_db': Indicates that the EGW database is not present in the MySQL server or if MySQL server is unavailable.</p> <p>Actions: Depending on the condition listed in the "Alarm Information" section, the action to perform changes. The conditions and specific actions to perform are listed below:</p> <ul style="list-style-type: none"> a. Slave IO: No Slave SQL: No Seconds Behind Master: (null): Re-initiate the replication using the "Start Replication" option or "Sync to/from Peer" option on the EGW dashboard. If this issue persists, please contact Intrado support team. b. Cant connect to MySQL server on 999.999.999.999(999): Ensure that MySQL service is running and that all the firewall rules are appropriate. c. Unknown database 'gateway_db': Restart replication by clicking on the Re-try Sync to/Peer from the peer EGW from the point where the database was intact. <p>If the alarm is not automatically cleared and the issue persists, please contact the Intrado support team.</p>
MON-18	<p>Peer EGW DB Unavailable The Secondary EGW's database cannot be accessed.</p> <p>Alarm information displayed is one of the following:</p> <ul style="list-style-type: none"> a. Slave IO: No Slave SQL: No Seconds Behind Master: (null) b. Cant connect to MySQL server on 999.999.999.999(999) 	Critical	Once every 15 minutes	<p>Alarm raised to inform you that one of the conditions displayed in the "Alarm Information" section is present.</p> <p>Please see below for detailed description of the condition shown in the "Alarm Information":</p> <ul style="list-style-type: none"> a. Slave IO: No Slave SQL: No Seconds Behind Master: (null): Indicates that MySQL replication between the EGW peers is broken. If you have manually stopped the replication for maintenance purposes, this alarm can be ignored.

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
	<p>c. Unknown database 'gateway_db'</p>			<p>b. Cant connect to MySQL server on 999.999.999.999(999): Indicates that the local MySQL server cannot be reached.</p> <p>c. Unknown database 'gateway_db': Indicates that the EGW database is not present in the MySQL server or if MySQL server is unavailable.</p> <p>Actions: Depending on the condition listed in the “Alarm Information” section, the action to perform changes. The conditions and specific actions to perform are listed below:</p> <ul style="list-style-type: none"> a. Slave IO: No Slave SQL: No Seconds Behind Master: (null): Re-initiate the replication using the “Start Replication” option or “Sync to/from Peer” option on the EGW dashboard. If this issue persists, please contact Intrado support team. b. Cant connect to MySQL server on 999.999.999.999(999): Ensure that MySQL service is running and that all the firewall rules are appropriate. c. Unknown database 'gateway_db': Retry Sync to/Peer from the peer EGW from the point where the database was intact. <p>If the alarm is not automatically cleared and the issue persists, please contact the Intrado support team.</p> <p>Clearing Instructions: This alarm is automatically cleared when the underlying condition is resolved.</p>
MON-19	<p>MySQL port unavailable</p> <p>Port TCP/3306 used to access the MySQL server is inaccessible on the local EGW.</p>	Critical	Once every 15 minutes	<p>Actions:</p> <ul style="list-style-type: none"> • Verify firewall logs for connectivity issues. • Ensure there are no rules blocking port TCP/3306 from accessing the MySQL server on the EGW. <p>If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.</p> <p>Clearing Instructions: This alarm is automatically cleared when MySQL server becomes available on the local EGW.</p>

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
MON-20	Peer MySQL port unavailable Port TCP/3306 used to access the MySQL server is inaccessible on the peer EGW or MySQL server cannot be reached on the peer EGW.	Critical	Once every 15 minutes	Actions: <ul style="list-style-type: none"> Verify firewall logs for connectivity issues. Ensure there are no rules blocking port TCP/3306 from accessing the MySQL server on the EGW. Verify that MySQL server can be reached on the peer EGW. If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
	Clearing Instructions: This alarm is automatically cleared when MySQL server becomes available on the peer EGW.			
MON-21	Mail Server unavailable Alarm raised when EGW's mail server is unreachable	Critical	Once every 15 minutes	Actions: Ensure there are no rules blocking access to port TCP/25 on the EGW. If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
	Clearing Instructions: This alarm is automatically cleared when connection to the EGW's mail server is re-established.			
MON-22	SBC unavailable The local EGW's SBC is unreachable	Critical	Once every 15 minutes	Actions: Ensure that there are no firewall rules blocking access to port TCP/5060 and UDP/5060 on the local EGW. If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
	Clearing Instructions: This alarm is automatically cleared when connection to the local EGW's SBC is re-established.			
MON-23	Peer SBC unavailable The Secondary EGW's SBC is unreachable	Critical	Once every 15 minutes	Actions: Ensure that there are no firewall rules blocking access to port TCP/5060 and UDP/5060 on the peer EGW. If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
	Clearing Instructions: This alarm is automatically cleared when the peer EGW's SBC becomes available.			

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
MON-25	/boot FS warning Alarm raised to warn you that /boot file system has reached 85% of its capacity.	Warning	Once every 15 minutes	Actions: This alarm indicates that the /boot file system has reached 85% of its capacity. If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
				Clearing Instructions: This alarm is automatically cleared when the space in the /boot file system reaches an acceptable level.
MON-26	/boot FS critical Alarm raised to warn you that /boot file system has reached 95% of its capacity.	Critical	Once every 15 minutes	Actions: This alarm indicates that the /boot file system has reached 95% of its capacity. If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
				Clearing Instructions: This alarm is automatically cleared when the space in the /boot file system reaches an acceptable level.
MON-27	Root FS warning Alarm raised to warn you that /root file system has reached 85% of its capacity	Warning	Once every 15 minutes	Actions: This alarm indicates that the root file system (containing the EGW operating system, applications software and database) has reached 85% of its capacity. If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
				Clearing Instructions: This alarm is automatically cleared when more space becomes available on the root file system.
MON-28	Root FS critical Alarm raised to warn you that /root file system has reached 95% of its capacity	Critical	Once every 15 minutes	This alarm indicates that the root file system (containing the EGW operating system, applications software and database) has reached 95% of its capacity. Actions: If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
				Clearing Instructions: This alarm is automatically cleared when more space becomes available on the root file system.
MON-29	/var/spool FS warning	Warning	Once every 15 minutes	This alarm indicates that the /var/spool file system that contains the audio recordings of emergency calls processed by the EGW has reached 85% of its capacity. This could be

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
	Alarm raised to warn you that /var/spool file system has reached 85% of its capacity.			<p>caused due to a service running with a log level “debug”</p> <p>Actions: If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.</p>
MON-30	/var/spool FS critical Alarm raised to warn you that /var/spool file system has reached 95% of its capacity.	Critical	Once every 15 minutes	<p>This alarm indicates that the /var/spool file system that contains the audio recordings of emergency calls processed by the EGW has reached 95% of its capacity. This could be caused due to a service running with a log level “debug”</p> <p>Actions: If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.</p>
MON-31	/var/log FS warning Alarm raised to warn you that the /var/log file system has reached 85% of its capacity.	Warning	Once every 15 minutes	<p>This alarm indicates that the /var/log file system that contains log files created by various services running on the EGW, has reached 85% of its capacity. This could be caused due to a service running with a log level “debug”</p> <p>Actions: If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.</p>
MON-32	/var/log FS critical Alarm raised to warn you that the /var/log file system has reached 95% of its capacity.	Critical	Once every 15 minutes	<p>This alarm indicates that the /var/log file system that contains log files created by various services running on the EGW, has reached 95% of its capacity. This could be caused due to a service running with a log level “debug”</p> <p>Actions: If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.</p>

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
				Clearing Instructions: This alarm is automatically cleared when sufficient space becomes available on the /var/log file system disk.
MON-33	/home FS warning Alarm raised to warn you that the /home file system disk space has reached 85 % of its capacity.	Warning	Once every 15 minutes	This alarm indicates that the /home file system (containing the batch files uploaded through FTP, etc) has reached 85% of its capacity. Actions: If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
				Clearing Instructions: This alarm is automatically cleared when sufficient space becomes available on the /var/log file system disk.
MON-34	/home FS critical Alarm raised to warn you that the /home file system disk space has reached 95% of its capacity.	Critical	Once every 15 minutes	This alarm indicates that the /home file system (containing the batch files uploaded through FTP, etc) has reached 95% of its capacity. Actions: If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.
				Clearing Instructions: This alarm is automatically cleared when sufficient space becomes available on the /var/log file system disk.
MON-35	/opt/911Gateway/core FS warning Alarm raised to inform you that the /opt/911Gateway/core file system disk space has reached 85 % of its capacity.	Warning	Once every 15 minutes	This alarm indicates that the /opt/911Gateway/core file system contains a core dump file following a process crash. Normally, this file system should be empty. Actions: Contact the Intrado support team for assistance.
				Clearing Instructions: This alarm is automatically cleared when the files in the /opt/911Gateway/core FS are cleared.
MON-36	/opt/911Gateway/core FS critical Alarm raised to inform you that the /opt/911Gateway/core file system disk space has reached 95 % of its capacity.	Critical	Once every 15 minutes	This alarm indicates that the /opt/911Gateway/core file system contains a core dump file following a process crash. Normally, this file system should be empty. Actions: Contact the Intrado support team for assistance.
				Clearing Instructions: This alarm is automatically cleared when the files in the /opt/911Gateway/core FS are cleared.

20.1.7 Routing

Alarm ID	Alarm Name and Description	Level (Default)	Frequency (Default)	Troubleshooting Guidelines/ Actions to perform
RTE-01	Call detail records request failed on main call leg. During hang up process, the call detail record for a call could not be created.	Critical	Always	Notification error sent when a CDR request fails from the AGI console (main leg) Actions: Please contact the Intrado Support team immediately.
RTE-02	Call detail records request failed on security desk call leg. During hang up process the call detail record for a call could not be created.	Critical	Always	Notification error sent when a CDR request fails from the AGI console (other legs). Actions: Please contact the Intrado Support team immediately.
RTE-03	Call leg to ERS SBC failed Call routing to ERS IP address has failed. No other ERS fail over IP address could be attempted. Failover to ECRC initiated.	Critical	Always	Notification error sent when the call to the ERS is failing for one of the following reasons: <ul style="list-style-type: none"> • The call to one of the SBCs failed. • None of the SBCs has been able to process the call. Actions: Investigate if it is an isolated event or affecting all calls. This can occur if the called party (e.g. PSAP) is busy, or if the called system (IP) is experiencing issues with answering the call.
RTE-04	Call route to ECRC via ERS unavailable. The system was unable to route a call to the ECRC through the ERS. Failover initiated to another ERS route.	Warning	Once every 5 minutes	Notification error sent when the call to ECRC ERS is failing. Actions: Open a ticket with Intrado support team for investigation. ERS SIP peers may be unreachable from EGW perspective. Could be caused by customer network, firewall, PBX misconfiguration.
RTE-05	Call route to ERS SBC unavailable Call routing to an ERS IP address has failed. Failover initiated to another ERS SBC IP address.	Warning	Once every 5 minutes	Notification error sent when the call to the ERS is failing for one of the following reasons: <ul style="list-style-type: none"> • The call to one of the SBCs failed. • None of the SBCs has been able to process the call. Actions: Open a ticket with Intrado support team for investigation. ERS SIP peers may be unreachable from EGW perspective. Could be caused by customer network, firewall, PBX misconfiguration.

Alarm ID	Alarm Name and Description	Level (Default)	Frequency (Default)	Troubleshooting Guidelines/ Actions to perform
RTE-06	<p>Call to ECRC via ERS failed.</p> <p>The system was unable to route a call to the ECRC through the ERS. No other fail over destination could be attempted. Take immediate action.</p>	Critical	Always	<p>Notification error sent when the call to ECRC ERS is failing.</p> <p>Actions: Open a ticket with Intrado support team for investigation. ERS SIP peers may be unreachable from EGW perspective. Could be caused by customer network, firewall, PBX misconfiguration.</p>
RTE-07	<p>Callback call leg failed.</p> <p>The system was unable to route a callback through any of the specified PBX servers. Take immediate action.</p>	Critical	Always	<p>Notification error sent when the Callback call is failing.</p> <p>Actions: Open a ticket with Intrado support team for investigation. PBX SIP peers may be unreachable from EGW perspective. Could be caused by customer network, firewall, PBX misconfiguration.</p>
RTE-08	<p>Callback call route unavailable</p> <p>The system was unable to route a callback through one of the specified PBX servers. Failover initiated to another PBX server.</p>	Warning	Once every 5 minutes	<p>Notification error sent when the Callback call is failing.</p> <p>Actions: Open a ticket with Intrado support team for investigation. PBX SIP peers may be unreachable from EGW perspective. Could be caused by customer network, firewall, PBX misconfiguration.</p>
RTE-10	<p>ECRC call leg failed.</p> <p>The system was unable to route a call to the ECRC through any of the specified PBX servers. Immediate action required.</p>	Critical	Always	<p>Notification error sent when the call to ECRC PBX is failing.</p> <p>Actions: Verify PBX logs for cause/reason for rejecting call setup from EGW perspective. Could be caused by customer network, firewall, PBX misconfiguration. If investigation is non-conclusive, it may be necessary engage the Intrado support team to troubleshoot and review application logs.</p>
RTE-11	<p>ECRC call route unavailable.</p> <p>The system was unable to route a call to the ECRC through one of the specified PBX servers. Either the DNIS is invalid or the PBX is currently down. Failover initiated to another PBX server.</p>	Warning	Always	<p>Notification error sent when the call to ECRC PBX is failing.</p> <p>Actions: Verify PBX logs for cause/reason for rejecting call setup from EGW perspective. Could be caused by customer network, firewall, PBX misconfiguration. If investigation is non-conclusive, it may be necessary engage the Intrado support team to troubleshoot and review application logs.</p>

Alarm ID	Alarm Name and Description	Level (Default)	Frequency (Default)	Troubleshooting Guidelines/ Actions to perform
RTE-12	Extension Missing The EGW received a call from a station without an extension. Callback and locating the caller is impossible.	Critical	Always	Notification error sent when a call contains no extension. Actions: Verify any public unknown numbering tables and or translation or route patterns for caller ID masking/removal
RTE-13	Fallback call failed. The system was unable to route to the fallback URI. Take immediate action.	Critical	Always	Notification error sent when the Fallback call is failing. Actions: Verify fallback URI on global settings page on EGW. Verify IP and DNIS, Add a 9 and 1 if necessary in your dial plan.
RTE-14	IP-PBX not found A call was made from an IP-PBX that was unrecognized by the EGW.	Critical	Always	Notification error sent when the IP-PBX is not found during a call. Actions: Ensure that the signaling IP address of the IP-PBX is correctly entered in the EGW Dashboard. Verify that all IP-PBX signaling servers are added to the Dashboard.
RTE-15	Local trunking call leg failed. The system was unable to route a call to the local trunk through any of the specified PBX servers. Failover initiated to ECRC.	Warning	Always	Notification error sent when the call to Local Trunking is failing. Actions: Verify PBX logs for cause/reason for rejecting call setup from EGW perspective. Could be caused by customer network, firewall, PBX misconfiguration. If investigation is non-conclusive, it may be necessary engage the Intrado support team to troubleshoot and review application logs.
RTE-16	Local trunking call route unavailable. The system was unable to route a call to the local trunk through one of the specified PBX servers. Either the DNIS is invalid or the PBX is currently down. Failure initiated to another PBX server.	Warning	Once every 5 minutes	Notification error sent when the call to Local Trunking is failing. Actions: Verify PBX logs for cause/reason for rejecting call setup from EGW perspective. Could be caused by customer network, firewall, PBX misconfiguration. If investigation is non-conclusive, it may be necessary to engage the Intrado support team to troubleshoot and review application logs.
RTE-17	SBC unable to retrieve routing instructions from CPM. The SBC was unable to retrieve routing instructions from the CPM module.	Critical	Always	Notification error sent when CPM fails to process call instructions. This can occur if the web service is down, the database is down or the connection is refused. Take immediate action. Actions: Contact the Intrado support team immediately.

Alarm ID	Alarm Name and Description	Level (Default)	Frequency (Default)	Troubleshooting Guidelines/ Actions to perform
RTE-18	Security desk call leg failed. The system was unable to route a call to the security desk through any of the specified PBX servers. Take immediate action.	Critical	Always	Notification error sent when the call to Security Desk is failing. Actions: Verify PBX logs for cause/reason for rejecting call setup from EGW perspective. Could be caused by customer network, firewall, PBX misconfiguration. If investigation is non-conclusive, it may be necessary to engage the Intrado support team to troubleshoot and review application logs.
RTE-19	Security desk call route unavailable. The system was unable to route a call to the security desk through one of the specified PBX servers. Either the DNIS is invalid or the PBX is currently down. Failover initiated to another PBX server.	Warning	Once every 5 minutes	Notification error sent when the call to Security Desk is failing. Actions: Verify PBX logs for cause/reason for rejecting call setup from EGW perspective. Could be caused by customer network, firewall, PBX misconfiguration. If investigation is non-conclusive, it may be necessary to engage the Intrado support team to troubleshoot and review application logs.
RTE-20	Caller location from location server could not be retrieved Unable to retrieve the location/map from location server, preventing the caller to be located.	Warning	Always	Notification error sent when the map from the location server could not be retrieved. Actions: Verify if there is any misconfiguration on PBX side that is preventing the EGW from identifying the calling party's MAC address (e.g. Avaya Push not working successfully). Requires further investigation and possibly assistance from Intrado support team.

20.1.8 Scheduler

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
SCH-02	CDR Export Scheduled Task Failed The CDR Export scheduled report to FTP has failed.	Critical	Once a day	Notification error when an error occurs while creating CDR reports for FTP export. Actions: Contact Intrado support team for assistance.
SCH-03	Unresolved configured PBX server Domain/IP Cannot resolve the provided Signaling IP Address/FQDN.	Critical	Once a day	The Lync PBX server(s) cannot be resolved. Actions: Verify the correct signaling FQDN has been configured on the EGW. Verify DNS servers are up-to-date.

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
				<p>Verify internal firewall settings that may be preventing the EGW from resolving FQDN.</p> <p>Test with the IP address instead of the FQDN in the IP-PBX configuration settings on the EGW Dashboard.</p> <p>Clearing Instructions: This alarm will be cleared when the corresponding PBX server can be resolved on the Resolved Domains scheduled task.</p>

20.1.9 System Status

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
SYS-01	Database Connection Failure Database connection failure. EGW could not connect to internal database.	Critical	Once every 5 minutes	<p>Generic DB connectivity issue.</p> <p>Actions: Please contact Intrado support team for assistance.</p>
SYS-02	EGW Status Error The EGW is unable to determine its status (Primary or Secondary). This could result in loss of critical functionality.	Warning	Once every 15 minutes	<p>The EGW has no valid PRIMARY or SECONDARY set up.</p> <p>Actions: Please contact Intrado support team for assistance.</p> <p>Clearing Instructions: This alarm will be cleared when the server is set with the right type on the EGW Peer check scheduled task.</p>
SYS-03	Mail Server down Mail Server is not reachable.	Warning	Once every 15 minutes	<p>Notification error sent when the mail server is down while trying to send batch report by mail.</p> <p>Actions: Verify firewall and ACL settings and verify connectivity between the Mail Server and the EGW. Ensure that TCP port 25 is not blocked between the EGW and the Mail Server.</p> <p>Please contact Intrado support team for assistance if the problem persists.</p>

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
SYS-04	Max Endpoints Exceeded The amount of endpoints added to the system exceeds the current license.	Critical	Once an hour	Check if the maximum number of endpoints has been reached on the system Actions: Please contact Intrado Safety Services support team for assistance. Remove unused or unnecessary endpoints from the EGW using the EGW Dashboard (Provisioning), which can be a necessity for PBXes that do not clean up obsolete devices (e.g. Avaya).
	Clearing Instructions: This alarm will be cleared when the number of provisioned endpoints is below the maximum allowed number of endpoints on the next endpoint limitation check.			
SYS-05	Primary EGW server down A CTI request to the Primary CPM module timed out. Failover to secondary EGW was initiated.	Warning	Once every 15 minutes	Notification error sent when the PRIMARY EGW is down. Actions: Please contact Intrado support team for assistance.
SYS-06	SOAP call failure SOAP call failure. SOAP Provisioning transaction could not be completed.	Critical	Once every 15 minutes	Generic SOAP call failure to the ERS. Actions: Verify network connectivity between EGW and ERS Provisioning servers. All SOAP requests originating from the EGW have destination FQDN of provisioning.911.west.com using TCP/443. Verify web proxy configuration under Configuration > Advanced > ERS Account . Verify SOAP Username and SOAP Password credentials have not been modified under Configuration > Advanced > ERS Account . Verify the Account ID and Token have not been modified under Configuration > Advanced > ERS Account . Please contact Intrado support team for assistance if the problem persists.
SYS-07	Total processes warning The number of active processes on the server has reached 800.	Info	Once an hour	Under normal operation the number of active processes should be less than 800. If the number of active processes has reached 800, this could mean one of the following: <ul style="list-style-type: none"> Service misconfiguration or malfunction may be causing too many processes to be launched simultaneously.

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
				<ul style="list-style-type: none"> Service misconfiguration or malfunction may be causing processes to remain active indefinitely. <p>Actions: If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.</p>
SYS-08	<p>Total processes critical The number of active processes on the server has reached 1000.</p>	Warning	Once an hour	<p>Under normal operation the number of active processes should be less than 1000. If the number of active processes has reached 1000, this could mean one of the following:</p> <ul style="list-style-type: none"> Service misconfiguration or malfunction may be causing too many processes to be launched simultaneously. Service misconfiguration or malfunction may be causing processes to remain active indefinitely. <p>Actions: If the alarm does not clear automatically and the issue persists, please contact the Intrado support team for assistance.</p>
SYS-09	<p>CPU Average load warning CPU Average load has reached warning level.</p>	Info	Once an hour	<p>The CPU load average gives an general idea of the level of activity on the system for the past 15 minutes.</p> <p>Actions: It is recommended to monitor the situation closely to ensure if it goes back to normal.</p> <p>However, if the alarm is not automatically cleared and the issue persists, please contact the Intrado support team for assistance.</p> <p>Clearing Instructions: This alarm is automatically cleared when the CPU load average goes back to normal.</p>

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
SYS-10	CPU Average load critical CPU Average load has reached critical level.	Warning	Once an hour	<p>The CPU load average gives an general idea of the level of activity on the system for the past 15 minutes.</p> <p>Actions: It is recommended to monitor the situation closely to ensure if it goes back to normal.</p> <p>However, if the alarm is not automatically cleared and the issue persists, please contact the Intrado support team for assistance.</p>
	<p>Clearing Instructions: This alarm is automatically cleared when the CPU load average goes back to normal.</p>			
SYS-11	SWAP usage warning Swap usage has reached warning level (20% free space remaining)	Warning	Once an hour	<p>The SWAP usage gives a general idea of the percentage of virtual memory being used to store inactive processes.</p> <p>Actions: It is recommended to monitor the situation closely to ensure if it goes back to normal.</p> <p>However, if the alarm is not automatically cleared and the issue persists, please contact the Intrado support team for assistance.</p>
	<p>Clearing Instructions: This alarm is automatically cleared when the SWAP usage goes back to normal.</p>			
SYS-12	SWAP usage critical Swap usage has reached critical level (10% free space remaining)	Critical	Once an hour	<p>The SWAP usage gives a general idea of the percentage of virtual memory being used to store inactive processes.</p> <p>Actions: It is recommended to monitor the situation closely to ensure that it goes back to normal.</p> <p>However, if the alarm is not automatically cleared and the issue persists, please contact the Intrado support team for assistance.</p>
	<p>Clearing Instructions: This alarm is automatically cleared when the SWAP usage goes back to normal.</p>			
SYS-13	Local system failure Local system is unreachable	Critical	Once every 5 minutes	<p>Actions: Please contact the Intrado support team for assistance.</p>

Alarm ID	Alarm Name and Description	Level	Frequency	Troubleshooting Guidelines/ Actions to perform
SYS-14	Peer system failure Peer system is unreachable	Critical	Once every 5 minutes	Actions: Please contact the Intrado support team for assistance.

21 Glossary

Table 21-1 Glossary

Acronym	Description
ALI (Automatic Location Identifier)	A database that relates a specific telephone number (TN) to an address/location and to emergency services information.
nALI (National ALI)	The nALI is a central repository for Emergency Response Location (ERL) records. The VPC uses the nALI to obtain the caller's address during a 911 call. The nALI accepts records from all 50 states and Canada, eliminating the need to manage multiple regional ALI databases.
ANI (Automatic Number Identification)	The business or residential customer's billing number. Used to automatically identify the telephone number of the calling party.
CAMA (Centralized Automatic Message Accounting)	A type of in-band analog transmission protocol that transmits telephone numbers via multi-frequency encoding.
CAMA trunk	A telephone circuit used for a single purpose, such as the transmission of 911 calls. Normally a T1 timeslot or analog line with MF signaling tones and CAMA signaling. Used to interface with Selective Routers and PSAPs.
CBN (Callback Number)	A 10 digit PSTN number that is used by the PSAP or security desk to call back the telephone extension, in the event that the 911 call is dropped.
CLEC (Competitive Local Exchange Carrier)	A Telecommunications Carrier (TC) under the state/local Public Utilities Act that provides local exchange telecommunications services. A CLEC acts as an alternative to the existing local phone company.
CDR (Call Detail Record)	A call detail record provides detailed information for each 911 call that is made. It may include the following information: call duration, call status, dialed digits, etc.
DID (Direct Inward Dialing)	A feature of local telephone service whereby each person in an organization has his or her own ten-digit telephone number. Calls to DID numbers do not have to be answered by onsite operators. They go directly to the person assigned to the 10 digit DID telephone number.
DNIS (Dialed Number Identification Service)	The DNIS number is the dialed number in a SIP call. The service is used to identify and route toll free and 900 numbers to particular agents or devices within a customer site. For example, if a customer has multiple 800 numbers, the network provider routes each toll-free number to a different four-digit number at the customer's telephone system. The onsite PBX, key system, or Centrex system then routes the call to a particular group of agents, voice response system, or department.
ECRC (Emergency Call Response Center)	The Intrado ECRC is staffed with APCO-trained personnel. A trained call-taker answers the 911 call, confirms the caller's location, and manually routes the call to the appropriate PSAP. The call will be an enhanced 911 call, if selective routing is available for the destination PSAP.
ELIN (Emergency Location Identification Number)	ELINs are 10 digit numbers which are used to route location data to the correct PSAP when 911 is dialed. These ELINs are purchased from the local carrier and are mapped to physical locations in the service provider's ALI database. When 911 is dialed, the call server maps the station's number to the ELIN, enabling the service provider to identify the caller's location. The call server caches a record of the last phone that used the ELIN so that the PSAP can perform a callback if necessary.

Acronym	Description
ERL (Emergency Response Location)	An ERL describes a location at the enterprise. When 911 is dialed from a phone assigned to a specific ERL, the ERL address is delivered in the ALI data to the PSAP and/or security desk. Certain states mandate the maximum size of an ERL, requiring businesses to specify the floor number, building, wing, or branch, in addition to the main address.
ERS (Emergency Routing Service)	The Intrado Emergency Routing Service is a subscription service that allows enterprises to route 911 calls to the appropriate PSAP. The ERS service eliminates the need to establish local trunks or populate ELIN records in local carrier-managed ALI databases and includes support for off-campus users. With the largest E911 coverage in the industry, the ERS delivers the caller's location information and callback number to the appropriate Public Safety Answering Point (PSAP).
EGW (Emergency Gateway)	The Intrado EGW is a software appliance that integrates with the enterprise network. It pinpoints the location of 911 callers and forwards the call to the Intrado Emergency Routing Service. The EGW also provides support for advanced IP-PBX features such as shared line appearance and extension mobility.
ESGW (Emergency Services Gateway)	The ESGW is the signaling and media interworking point between the IP domain and the conventional selective routing trunks. ESGWs have redundant SS7 or CAMA trunks to each regional selective router (SR), ensuring high service availability. The ESGW converts calls from IP to PSTN, and uses routing information provided by the VPC to deliver the call to the appropriate selective router. The ESGW is interconnected to PSAPs across the US, via dedicated selective routing trunks.
LEC (Local Exchange Carrier)	A Telecommunications Carrier (TC) under the state/local Public Utilities Act that provides local exchange telecommunications services. Also known as Incumbent Local Exchange Carriers (ILECs), Alternate Local Exchange Carriers (ALECs), Competitive Local Exchange Carriers (CLECs), Competitive Access Providers (CAPs), Certified Local Exchange Carriers (CLECs), and Local Service Providers (LSPs).
MAC (Media Access Control)	The MAC address is a unique identifier attached to most network adapters and is used by the EGW to uniquely identify different phone instances sharing the same number.
MSAG (Master Street Address Guide)	The MSAG is a regional database that contains the valid Address Ranges for the Streets (within the Communities, Counties, and State) in which the Addressing Authority is responsible. The MSAG database is created by the Addressing Authority for a region. An address is considered MSAG-valid if it exists in the MSAG database.
MLTS (Multi-Line Telephone System)	A phone system comprised of common control unit(s), telephone sets, and control hardware and software. This includes network and premises-based systems (i.e. Centrex and PBX, Hybrid and Key Telephone Systems).
NENA (National Emergency Number Association)	This organization sets the standards for the universal emergency telephone number system. NENA's mission is to foster the technological advancement, availability and implementation of a universal emergency telephone number system (911). In carrying out its mission, NENA promotes research, planning, training, and education.
PBX (Private Branch Exchange)	A PBX is a multi-line telephone switching system owned by a private business rather than a public Telco. PBXs interconnect the internal telephones of a private organization and allow them to terminate calls over the public switched telephone network (PSTN) via trunk lines.

Acronym	Description
IP-PBX (Private Branch Exchange)	An IP-PBX is a business telephone system designed to deliver voice over a data network and interoperate with the normal Public Switched Telephone Network (PSTN). VoIP gateways are combined with traditional PBX functionality enabling businesses to use their managed intranet to help reduce long distance expenses and enjoy the benefits of a single network for voice and data.
PSAP (Public Safety Answering Point)	A PSAP is an agency in the United States, typically county or city controlled, responsible for answering 911 calls for emergency assistance from police, fire, and ambulance services. There are roughly 6,100 primary and secondary PSAPs in the U.S.
PS-ALI (Private Switch ALI)	A private telephone system which includes network, switching, and database elements, capable of providing ANI (ELIN) and ALI (ERL). Designed to be used in emergency situations to notify Public Safety personnel of the specific location of a 911 caller utilizing a Telephone Station connected to a private telephone network.
SR (Selective Router)	The Central Office that provides the tandem switching of 911 calls. It controls delivery of the voice call with ANI to the PSAP and provides Selective Routing, Speed Calling, Selective Transfer, Fixed Transfer, and certain maintenance functions for each PSAP.
VPC (VoIP Positioning Center)	The VPC is responsible for ensuring that incoming VoIP 911 calls are routed to the correct PSAP based on the location of the caller. The VPC maintains a database of Emergency Service Zones (ESZ) which corresponds to specific PSAP boundaries. When 911 is dialed, the VPC stages the caller's location record and assigns an Emergency Service Query Key (ESQK). The ESQK is a 10 digit number which is used by the PSAP to query its regional ALI database. Based on the ESQK, the regional ALI steers this query back to the VPC to retrieve the staged location record. Intrado maintains ALI steering agreements with various carriers in order to establish the i2 data links.

22 Appendix A

22.1 Legacy batch file format for ERLs



Note: This file format is still applicable for users in US/Canada.

The batch file format is used to process multiple ERL records using the Dashboard or ftp. Each line in the file describes an ERL with its provisioning parameters. The parameters are entered as fields in a semicolon delimited file format.

Table 2: ERL Batch File Field Descriptions

Position	Field Name	Description	Req?
1	Operation	Value: 1 = Add or update 2 = Delete *For the delete operation, it is only necessary to include Position 2 (ERL ID).	Y
2	ERL ID	Unique identifier of the location. Alphanumeric between 1 and 31 characters in length. Note: The dash symbol (-) is not permitted. However, the underscore symbol (_) is permitted.	Y
3	Building Number	Building number of the location. Numerical between 1 and 10 digits in length. Also accepts 101A, 101 1/2, 101 1/4.	Y
4	Street Name	Street name of the location. Alphanumeric between 1 and 48 characters in length.	Y
5	Location	Information which specifies additional granularity for the location. e.g.: Suite 200, Floor 2, Unit 341. Alphanumeric between 1 and 20 characters.	N
6	City	City of the location. Alphanumeric between 1 and 32 characters.	Y
7	State/Province	State/Province of the location. Must be the abbreviation, not the full name. Must be 2 letters in length.	Y
8	Country	3 character representation of the country. e.g. USA, CAN.	Y
9	Zip Code/ Postal Code	US Zip Code in this format: XXXXX(-XXXX) Canadian Postal Code: X2X 2X2 *Information in parenthesis is optional.	Y
10	Local Gateway Enabled	Setting which enables or disables local trunking for the ERL. 1 = Yes 0 = No	Y

Position	Field Name	Description	Req?
11	Security Desk Call Route Setting	<p>Setting which determines call routing for the security desk route.</p> <p>0 = Call Monitoring 1 = Direct Call Delivery 2 = Security Desk Dial Plan Only</p> <p>When set to 0, default setting of Call Monitoring will be used, if a Security Desk is configured at the Dashboard. The security desk is referenced by the Security Desk Name (Position 14) specified for the ERL record.</p> <p>When set to 1, security desk call routing feature will use Direct Delivery.</p> <p>If 2 is set, the security desk feature will only apply to calls made to a security desk dial plan number (e.g. 511, 888). If the ERL setting is 2, and a security desk number is dialed, the call will route as a direct delivery call to the on-site security desk. With this configuration, a call from the same ERL to the emergency number (e.g. 911) will not route to the security desk.</p>	Y
12	Customer Name	<p>The name of the customer. This field will appear on the PSAP screen as the "Name."</p> <p>Between 1 and 60 characters.</p>	N
13	ELINs	<p>ELINs for the ERL. May be defined statically or dynamically.</p> <p>Static assignment To statically assign ELINs, enter the ELIN numbers (must be 10 digit numbers and comma delimited).</p> <p>e.g. 1000000000,3333333333,2323232323.</p> <p>Dynamic assignment (ERS call delivery only) Add the amount of ELINs, enclosed in parentheses, which you would like the EGW to assign to this ERL. The EGW will select available ELINs from the ELIN pool based on this number. For example, [1],[2],[3]</p> <p>An error will be generated if the ELIN pool has been exhausted.</p> <p> Note: Dynamic ELIN management should be reserved for enterprises with on-site security P-ALI databases, or for enterprises that use local trunking to route all 911 calls within a single PSAP jurisdiction.</p> <p>Multiple ERLs per ELIN It is possible to assign multiple ERLs to the same ELIN number. However, you are not able to assign a dynamic ELIN from the ELIN pool to more than one ERL. A dynamic ELIN can only be assigned to one ERL at a time. If you attempt this operation an error is returned.</p>	N
14	Security Desk Name	Name identifier of the security desk. Letters and underscores.	N

Position	Field Name	Description	Req?
15	Crisis Email List	Distribution list which will receive an email when 911 is dialed from the ERL. Comma delimited for multiple entries. e.g. john@enterpriseabc.com, jane@enterpriseabc.com.	N
16	URL Data	Information that will appear in the Crisis Alert Email. e.g. URL or database query. All characters accepted except semicolons.	N

Example Batch Files

Example # 1: 1;LOC_X;211;MAIN ST;;NEW YORK;NY;USA;10044;0;0;;;;

- The batch file is performing the “Add” operation.
- The ERL ID is LOC002.
- Local trunking is disabled for the parameter.
- Direct delivery is disabled for the parameter.
- Position 12-16 are void.

Example # 2: 1;CID003;800;MAIN ST;SUITE 200;NEW YORK;NY;USA;10044;0;0;NITRO

INSURANCE;5147775555,4221554141;;jean@bob.ca,mike@gene.ca;http://corp.company.com/?remoteURL=910z
3

- The batch file is performing the “Add” operation.
- The ERL ID is CID003.
- Local trunking is disabled.
- Direct delivery is disabled.
- The Customer Name is Nitro Insurance.
- Statically defined ELINs are included.
- Crisis Alert emails are included.
- A URL link is included.

Example # 3: 1;LOC_X;355;Main st;;New York;NY;USA;10044;0;0;[2];;;

- Batch file is performing the “Add” operation.
- ERL ID is FCERT55.
- Local gateway is disabled.
- Direct call delivery is disabled.
- The batch file instructs the EGW to assign 2 ELINs from the dynamic ELIN pool.

22.1.1 Dynamic ELIN Management

The ERL batch file format can be used to dynamically assign ELINs to ERL records. There are a variety of operations that can be performed to add and remove ELINs from the ERL configuration.



Note: Dynamic ELIN management should be reserved for enterprises with on-site security P-ALI databases, or for enterprises that use local trunking to route all 911 calls within a single PSAP jurisdiction. This feature is not applicable for call delivery via the ERS. You are not permitted to provision a dynamic ELIN pool number to more than one ERL at a time.

The following sequences illustrate all possible ELIN management operations:

1;LOC_X;355;Main st;;New York;NY;USA;10044;0;0;[1];;;

- The EGW dynamically assigns one free ELIN to the ERL record.

1;LOC_X;355;Main st;;New York;NY;USA;10044;0;0;[2];;;

- One ELIN is already assigned to this ERL. An additional ELIN is assigned, for a total of two ELINs.

1;LOC_X;355;Main st;;New York;NY;USA;10044;0;0;[1];;;

- Two ELINs were previously assigned to the ERL. This operation releases one ELIN.

1;LOC_X;355;Main st;;New York;NY;USA;10044;0;0;5146661111;;;

- The dynamic ELIN is released from the ERL. The specified ELIN is statically assigned to the ERL.

1;LOC_X;355;Main st;;New York;NY;USA;10044;0;0;;;;

- All ELINs are removed from the ERL record.

1;LOC_X;355;Main st;;New York;NY;USA;10044;0;0;3333333333;;;

- The number specified is a dynamic ELIN. It is bound to the ERL record, but remains dynamic.

22.1.2 ERL Batch Logs

Batch log files report on the success or failure of each entry in a submitted batch file. The batch logs are generated in response to the following actions:

- Validate
- Batch Process

To view the batch logs

- Click on **Provisioning > ERLs > Batch Logs**

The columns of the log display the following information:

- Original File Name
- Log file
- Log date
- Status
- Actions (Validate, Delete, Batch Process)*

*These actions apply to uploading an ERL batch file using the Dashboard interface. For more information, see section 11.2.2 “Dashboard Interface.”

Viewing a Batch Log File

To view a log file, click on **View Log File** under **Log File**.

The log file provides a status report for each line of the processed batch file. A line will contain an error code followed by a description, and then the original line in the batch file. If the operation was executed successfully, the error code will be set to 00. If the operation failed to complete successfully, the error code will be larger than 00.

The following table details each possible outcome resulting from a single operation.

Table 3: ERL Batch Log Error Codes

Error #	Description	Add / Update	Delete
00	Entry is successful.	X	X
01	Entry does not include the correct number of fields.	X	X
02	Operation entered is invalid.	X	X
03	Format of the ERL ID is invalid.	X	X
04	Format of the building number is invalid.	X	
05	Format of the street name is invalid.	X	
06	Format of the location is invalid.	X	
07	Format of the city is invalid.	X	
08	Format of the state/province is invalid.	X	
09	Format of the country is invalid.	X	

Error #	Description	Add / Update	Delete
10	Format of the zip code/postal code is invalid.	X	
11	a) Local gateway enabled setting is invalid. b) An ELIN must be present in order to use this setting.	X	
12	a) Direct call delivery setting is invalid. b) A valid security desk name is required in order to use this setting.	X	
13	Format of the customer name is invalid.	X	
14	One of the ELIN numbers entered is invalid.	X	
15	Security desk name entered does not exist.	X	
17	One of the crisis emails is invalid.	X	
18	Address entered already exists.	X	
19	ERL ID entered is invalid.		X
21	Address failed validation.	X	
22	One of the subnets entered is already assigned to another ERL ID.	X	
23	Endpoints assigned to the ERL ID entered.		X
24	One of the ELIN numbers is already set to another ERL ID, or is an existing Extension-Bind number.	X	
25	Direct call delivery and local gateway cannot be enabled at the same time.	X	
26	An error occurred during the SOAP call.	X	X
27	Account is invalid for local trunking.	X	
28	Account is only valid for local trunking.	X	
29	Cannot delete ERL because a switch is assigned.		X
30	Cannot delete ERL because a switch port is assigned.		X
31	URL data contains invalid characters.	X	
32	You do not have support for Canadian addresses enabled.	X	
33	At least one ELIN must be assigned to each Canadian address.	X	
34	Invalid license key. Either the license key is not defined or it is in the wrong format.	X	
35	ELIN pool is exhausted or dynamic ELIN pool is empty.	X	
36	One of the ELINs that you tried to assign to the ERL is in the dynamic ELIN pool. Dynamic ELINs cannot be assigned to more than one ERL at a time.		
37	Cannot delete ERL because a WLAN controller is assigned.		X
38	Cannot delete ERL because an access point is assigned.		X

Batch File Example

00;success;1;CID020;577;MAIN ST;SUITE 111;NEW YORK;NY;USA;10044;0;1;NITRO
INSURANCEB;5142132501,4651214545;SECURITYDESK1;;;

- The ERL batch upload was successful.

View Peer

If **Log File** displays **View Peer**, you must login to the Peer in order to view the log file. This scenario occurs when a batch file is processed by the Peer machine.

23 Appendix B

23.1 All Supported Countries for WWE EGW

Country	ISO ALPHA-2 Code
Afghanistan	AF
Albania	AL
Algeria	AG
Andorra	AN
Angola	AO
Antigua and Barbuda	AC
Argentina	AR
Armenia	AM
Australia	AS
Austria	AU
Azerbaijan	AJ
Bahamas, The	BF
Bahrain	BA
Bangladesh	BG
Barbados	BB
Belarus	BO
Belgium	BE
Belize	BH
Benin	BN
Bhutan	BT
Bolivia	BL
Bosnia and Herzegovina	BK
Botswana	BC
Brazil	BR
Brunei	BX
Bulgaria	BU
Burkina Faso	UV
Burma	BM

Country	ISO ALPHA-2 Code
Burundi	BY
Cabo Verde	CV
Cambodia	CB
Cameroon	CM
Canada	CA
Central African Republic	CT
Chad	CD
Chile	CI
China	CH
Colombia	CO
Comoros	CN
Costa Rica	CS
Côte d'Ivoire	IV
Croatia	HR
Cuba	CU
Cyprus	CY
Czech Republic	EZ
Denmark	DA
Djibouti	DJ
Dominica	DO
Dominican Republic	DR
Ecuador	EC
Egypt	EG
El Salvador	ES
Equatorial Guinea	EK
Eritrea	ER
Estonia	EN
Ethiopia	ET
Fiji	FJ
Finland	FI
France	FR
Gabon	GB
Gambia, The	GA
Georgia	GG
Germany	GM
Ghana	GH

Country	ISO ALPHA-2 Code
Greece	GR
Grenada	GJ
Guatemala	GT
Guinea	GV
Guinea-Bissau	PU
Guyana	GY
Haiti	HA
Holy See	VT
Honduras	HO
Honk Kong	HK
Hungary	HU
Iceland	IC
India	IN
Indonesia	ID
Iran	IR
Iraq	IZ
Ireland	EI
Israel	IS
Italy	IT
Jamaica	JM
Japan	JA
Jordan	JO
Kazakhstan	KZ
Kenya	KE
Kiribati	KR
Korea, South	KS
Kosovo	KV
Kuwait	KU
Kyrgyzstan	KG
Laos	LA
Latvia	LG
Lebanon	LE
Lesotho	LT
Liberia	LI
Libya	LY
Liechtenstein	LS
Lithuania	LH

Country	ISO ALPHA-2 Code
Luxembourg	LU
Macedonia	MK
Madagascar	MA
Malawi	MI
Malaysia	MY
Maldives	MV
Mali	ML
Malta	MT
Marshall Islands	RM
Mauritania	MR
Mauritius	MP
Mexico	MX
Micronesia, Federated States of	FM
Moldova	MD
Monaco	MN
Mongolia	MG
Montenegro	MJ
Morocco	MO
Mozambique	MZ
Namibia	WA
Nauru	NR
Nepal	NP
Netherlands	NL
New Zealand	NZ
Nicaragua	NU
Niger	NG
Nigeria	NI
Norway	NO
Oman	MU
Pakistan	PK
Palau	PS
Panama	PM
Papua New Guinea	PP

Country	ISO ALPHA-2 Code
Paraguay	PA
Peru	PE
Philippines	RP
Poland	PL
Portugal	PO
Qatar	QA
Romania	RO
Russia	RS
Rwanda	RW
Saint Kitts and Nevis	SC
Saint Lucia	ST
Saint Vincent and the Grenadines	VC
Samoa	WS
San Marino	SM
Sao Tome and Principe	TP
Saudi Arabia	SA
Senegal	SG
Serbia	RI
Seychelles	SE
Sierra Leone	SL
Singapore	SN
Slovakia	LO
Slovenia	SI
Solomon Islands	BP
Somalia	SO
South Africa	SF
South Korea	KR
South Sudan	OD
Spain	SP
Sri Lanka	CE
Sudan	SU
Suriname	NS

Country	ISO ALPHA-2 Code
Swaziland	WZ
Sweden	SW
Switzerland	SZ
Syria	SY
Taiwan	TW
Tajikistan	TI
Tanzania	TZ
Thailand	TH
Timor-Leste	TT
Togo	TO
Tonga	TN
Trinidad and Tobago	TD
Trinidad and Tobago	TD
Tunisia	TS
Turkey	TU
Turkmenistan	TX
Tuvalu	TV
Uganda	UG
Ukraine	UP
United Arab Emirates	AE
United Kingdom	UK
United States	US
Uruguay	UY
Uzbekistan	UZ
Vanuatu	NH
Venezuela	VE
Vietnam	VM
Yemen	YM
Zambia	ZA
Zimbabwe	ZI

23.2 Country Specific Validation Requirements

The following table describes the PIDF-LO fields that are required for specific countries. Fields are included in this table are required for a country, or their validation behavior varies from the Global batch file behavior.

Country Code	PIDF-LO	Field validation	Required	Accepted Characters/Validation Behavior
3 Austria	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÂÃÄÅÆÇÈÉÊËÌÍÐÑÒÓÔÔØÙÚÛÜÝàáâãäåæçèéêëìíðñòóôôøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
3	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
3	Country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
3	PC	'zip_code'	yes	4 digits (1234)
4 Belgium	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÂÃÄÅÆÇÈÉÊËÌÍÐÑÒÓÔÔØÙÚÛÜÝàáâãäåæçèéêëìíðñòóôôøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
4	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
4	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
4	PC	'zip_code'	yes	4 digits (1234)
5 Denmark	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÂÃÄÅÆÇÈÉÊËÌÍÐÑÒÓÔÔØÙÚÛÜÝàáâãäåæçèéêëìíðñòóôôøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
5	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
5	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)

Country Code	PIDF-LO	Field validation	Required	Accepted Characters/Validation Behavior
5	PC	'zip_code'	yes	4 digits (1234)
6 France	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÂÃÄÅÆÇÈÉÊËÌÍÐÑÒÓÔÔØÙÚÛÜÝàáâãäåæçèéêëìíðñòóôôøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
6	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
6	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
6	PC	'zip_code'	yes	5 digits (12345)
7 Germany	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÂÃÄÅÆÇÈÉÊËÌÍÐÑÒÓÔÔØÙÚÛÜÝàáâãäåæçèéêëìíðñòóôôøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
7	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
7	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
7	PC	'zip_code'	yes	5 digits (12345)
8 Ireland	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÂÃÄÅÆÇÈÉÊËÌÍÐÑÒÓÔÔØÙÚÛÜÝàáâãäåæçèéêëìíðñòóôôøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
8	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)

Country Code	PIDF-LO	Field validation	Required	Accepted Characters/Validation Behavior
8	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
8	PC	'zip_code'	no	5 digits (12345)
9 Italy	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÂÃÄÅÆÇÈÉÊÏÏÐÑÒÓÔÕØÙÚÛÜÝàáâãäåæçèéêïïðñòóôõøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
9	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
9	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
9	PC	'zip_code'	yes	5 digits (12345)
9	A1	'state'	yes	Any combination of 2 letters (a-z, A-Z)
10 Luxembourg	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÂÃÄÅÆÇÈÉÊÏÏÐÑÒÓÔÕØÙÚÛÜÝàáâãäåæçèéêïïðñòóôõøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
10	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
10	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
10	PC	'zip_code'	yes	4 digits (1234)
11 Portugal	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÂÃÄÅÆÇÈÉÊÏÏÐÑÒÓÔÕØÙÚÛÜÝàáâãäåæçèéêïïðñòóôõøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)

Country Code	PIDF-LO	Field validation	Required	Accepted Characters/Validation Behavior
11	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
11	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
11	PC	'zip_code'	yes	4 digits followed by a dash and 3 digits (1234-567)
12 Spain	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÂÃÄÅÆÇÈÉÊÏÍÐÑÒÓÔÔØÙÚÛÜÝàáâãäåæçèéêïíðñòóôôøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
12	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
12	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
12	PC	'zip_code'	yes	5 digits (12345)
13 sweden	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÂÃÄÅÆÇÈÉÊÏÍÐÑÒÓÔÔØÙÚÛÜÝàáâãäåæçèéêïíðñòóôôøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
13	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
13	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
13	PC	'zip_code'	yes	3 digits followed by a space and 2 digit (123 45)
14 UK	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÂÃÄÅÆÇÈÉÊÏÍÐÑÒÓÔÔØÙÚÛÜÝàáâãäåæçèéêïíðñòóôôøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.)

Country Code	PIDF-LO	Field validation	Required	Accepted Characters/Validation Behavior
				parenthesis(()), slash(/), pound(#), dash(-)
14	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
14	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
14	PC	'zip_code'	yes	(any length series of a-z or A-Z)
15 Netherlands	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÃÄÅÆÇÈÉÊÏÐÑÒÓÔÖØÙÚÛÜÝàáâãâæçèéêïðñòóôöøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
15	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
15	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
15	PC	'zip_code'	yes	(\d\d\d\d\s\w\w) 4 digits followed by a space and then 2 letters (e.g. 2585 GJ).
16 Norway	RD	'street_name'	yes	Any combination of 1 to 60 of the following : ÀÁÃÄÅÆÇÈÉÊÏÐÑÒÓÔÖØÙÚÛÜÝàáâãâæçèéêïðñòóôöøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
16	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
16	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
16	PC	'zip_code'	yes	4 digits (1234)
17 Switzerland	RD	'street_name'	yes	Any combination of 1 to 60 of the following :

Country Code	PIDF-LO	Field validation	Required	Accepted Characters/Validation Behavior
				ÀÁÂÃÄÅÆÇÈÉÊËÏÍÐÑÒÓÔÔØØÙÚÛÜÝàáâãâæçèéêëïíðñòóôôøøùúûüý, letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
17	HNO	'street_number'	yes	Any combination of 1 to 10 letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
17	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
17	PC	'zip_code'	yes	4 digits (1234)
17	A1	state	no	([a-zA-Z]{2})
18 Oman	country	'country'	yes	Any combination of 2 to 3 Upper Case letters (A-Z)
18	PC	'zip_code'	yes	3 digits (123)
18	RD	'street_name'	no	Any combination of 0 to 60 of the following: letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)
18	A3	City, township	yes	Any combination of 1 to 64 of the following: letters (a-z, A-Z), space (), digit (0-9), period (.), parenthesis(()), slash(/), pound(#), dash(-)

23.2.1 Regular Expressions for Country-Specific Validations

Country_id	Field_name	Regular_Expression
3	street_name	([\w\s\d\.\.\(\)\)\,\#\-\-]{1,60})
3	street_number	([\w\s\d\.\.\(\)\)\,\#\-\-]{1,10})
3	country	([A-Z]{2,3})
3	zip_code	([0-9]{4})
4	street_name	([\w\s\d\.\.\(\)\)\,\#\-\-]{1,60})
4	street_number	([\w\s\d\.\.\(\)\)\,\#\-\-]{1,10})
4	country	([A-Z]{2,3})
4	zip_code	([0-9]{4})
5	street_name	([\w\s\d\.\.\(\)\)\,\#\-\-]{1,60})
5	street_number	([\w\s\d\.\.\(\)\)\,\#\-\-]{1,10})
5	country	([A-Z]{2,3})
5	zip_code	([0-9]{4})

6	street_number	([\w\ s\d\.\.\(\),\/#-]{1,10})
6	street_name	([\w\ s\d\.\.\(\),\/#-]{1,60})
6	country	([A-Z]{2,3})
6	zip_code	([0-9]{5})
7	street_name	([\w\ s\d\.\.\(\),\/#-]{1,60})
7	street_number	([\w\ s\d\.\.\(\),\/#-]{1,10})
7	country	([A-Z]{2,3})
7	zip_code	([0-9]{5})
8	street_number	([\w\ s\d\.\.\(\),\/#-]{1,10})
8	street_name	([\w\ s\d\.\.\(\),\/#-]{1,60})
8	country	([A-Z]{2,3})
9	street_name	([\w\ s\d\.\.\(\),\/#-]{1,60})
9	street_number	([\w\ s\d\.\.\(\),\/#-]{1,10})
9	zip_code	([0-9]{5})
9	state	([a-zA-Z]{2})
9	country	([A-Z]{2,3})
10	street_number	([\w\ s\d\.\.\(\),\/#-]{1,10})
10	street_name	([\w\ s\d\.\.\(\),\/#-]{1,60})
10	country	([A-Z]{2,3})
10	zip_code	([0-9]{4})
11	street_name	([\w\ s\d\.\.\(\),\/#-]{1,60})
11	street_number	([\w\ s\d\.\.\(\),\/#-]{1,10})
11	country	([A-Z]{2,3})
11	zip_code	(\d\d\d\d\d)
12	street_name	([\w\ s\d\.\.\(\),\/#-]{1,60})
12	street_number	([\w\ s\d\.\.\(\),\/#-]{1,10})
12	country	([A-Z]{2,3})
12	zip_code	([0-9]{5})
13	street_name	([\w\ s\d\.\.\(\),\/#-]{1,60})
13	street_number	([\w\ s\d\.\.\(\),\/#-]{1,10})
13	country	([A-Z]{2,3})
13	zip_code	(\d\d\d\d\d)
14	street_number	([\w\ s\d\.\.\(\),\/#-]{1,10})
14	street_name	([\w\ s\d\.\.\(\),\/#-]{1,60})
14	zip_code	((\w\d\s\d\w\w) (\w\d\d\s\d\w\w) (\w\w\d\s\d\w\w) (\w\w\d\s\d\w\w) (\w\w\d\s\d\w\w) (GIR OAA))
14	country	([A-Z]{2,3})
15	street_name	([\w\ s\d\.\.\(\),\/#-]{1,60})
15	street_number	([\w\ s\d\.\.\(\),\/#-]{1,10})
15	country	([A-Z]{2,3})
15	zip_code	(\d\d\d\d\s\w\w)
16	street_name	([\w\ s\d\.\.\(\),\/#-]{1,60})
16	street_number	([\w\ s\d\.\.\(\),\/#-]{1,10})
16	country	([A-Z]{2,3})
16	zip_code	([0-9]{4})
17	street_name	([\w\ s\d\.\.\(\),\/#-]{1,60})
17	street_number	([\w\ s\d\.\.\(\),\/#-]{1,10})
17	country	([A-Z]{2,3})
17	zip_code	([0-9]{4})
17	state	([a-zA-Z]{2})

24 Appendix C: EGW Proprietary MIB Reference

```

-- ****
-- WEST-EGW-MIB.my: West Emergency Gateway MIB file
--
-- Copyright (c) 2019 by West Safety Services.
-- All rights reserved.
-- ****
--
WEST-EGW-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    NOTIFICATION-TYPE,
    enterprises
        FROM SNMPv2-SMI
    OBJECT-GROUP,
    NOTIFICATION-GROUP
        FROM SNMPv2-CONF;

-- ****
-- * MODULE IDENTITY
-- ****

emergencyGatewayMIB MODULE-IDENTITY
    LAST-UPDATED      "201902190000Z"
    ORGANIZATION      "West Safety Services"
    CONTACT-INFO
        "
            West Safety Services
            Customer Service

        Postal: 7150 Rue Alexander Fleming
        Montreal, Quebec, Canada
        H4S 2C8

        Tel: 1-877-862-2835

        E-mail: support@911.west.com"
DESCRIPTION
    "This MIB module provides management and alerts
     for the West Safety Services Emergency Gateway (EGW) .

ACRONYMS
ERL
    Emergency Response Location

SIP
    Session Initiation Protocol

GLOSSARY
"

REVISION      "201902190000Z"
DESCRIPTION

```

```

"-- Removed alarms MON-03, MON-04"

REVISION      "201805280000Z"
DESCRIPTION
    "- Removed egwAlarmType"

REVISION      "201609160000Z"
DESCRIPTION
    "- Added trap for EGW alarms."

REVISION      "201112190000Z"
DESCRIPTION
    "This is the initial version of this MIB module.

 ::= { emergencyGateway 1 }

-- Object Identifiers

west OBJECT IDENTIFIER
 ::= { enterprises 38995 }

products OBJECT IDENTIFIER
 ::= { west 1 }

emergencyGateway OBJECT IDENTIFIER
 ::= { products 1 }

egwMIBNotifications OBJECT IDENTIFIER
 ::= { emergencyGatewayMIB 0 }

egwMIBNotifObjects OBJECT IDENTIFIER
 ::= { egwMIBNotifications 0 }

egwMIBGroups OBJECT IDENTIFIER
 ::= { emergencyGatewayMIB 1 }

-- Objects

egwMIBObjectGroup OBJECT-GROUP
    OBJECTS {
        egwAlarmLevel,
        egwAlarmText,
        egwAlertCallback,
        egwAlertEndpoint,
        egwAlertCallingPartyName,
        egwAlertIpPbxName,
        egwAlertTimestamp,
        egwAlertUrlData,
        egwAlertLocation,
        egwServerType,
        egwAlertCallType,
        egwAlarmID,
        egwAlarmName,
        egwAlarmOccurrences,
        egwAlarmUUID
    }
    STATUS current

```

```

DESCRIPTION
    "A collection of objects providing remote configuration of
    management target translation parameters for use by
    proxy forwarder applications."
 ::= { egwMIBGroups 1 }

egwAlarmLevel OBJECT-TYPE
    SYNTAX      INTEGER {
                    critical(1),
                    warning(2),
                    info(3),
                    rac(4)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Alarm Levels:
         critical(1) - Critical,
         warning(2)  - Warning,
         info(3)     - Informational,
         rac(4)       - Remote Access Controller."
 ::= { egwMIBNotifObjects 2 }

egwAlarmText OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..1024))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Text describing the nature of the alarm and providing
more details"
 ::= { egwMIBNotifObjects 3 }

egwAlertCallback OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..64))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Callback number for the alert"
 ::= { egwMIBNotifObjects 4 }

egwAlertEndpoint OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..64))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The endpoint (extension) for the alert"
 ::= { egwMIBNotifObjects 5 }

egwAlertCallingPartyName OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..64))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Calling party name of the alert"
 ::= { egwMIBNotifObjects 6 }

egwAlertIpPbxName OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..70))
    MAX-ACCESS  read-only
    STATUS      current

```

```

DESCRIPTION "Corresponding EGW IP-PBX name for the alert"
 ::= { egwMIBNotifObjects 7 }

egwAlertTimestamp OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..70))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Timestamp (unix epoch format) of the alert when raised"
    ::= { egwMIBNotifObjects 8 }

egwAlertUrlData OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..1024))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The URL data set for the ERL corresponding to the alert"
    ::= { egwMIBNotifObjects 9 }

egwAlertLocation OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..1024))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The location (formatted according to the multiline
template as set in
                           the EGW configuration) for the alert"
    ::= { egwMIBNotifObjects 10 }

egwServerType OBJECT-TYPE
    SYNTAX      INTEGER {
        primary(1),
        secondary(2),
        standalone(3)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Server type:
         primary(1)      - Primary,
         secondary(2)    - Secondary,
         standalone(3)  - Standalone"
    ::= { egwMIBNotifObjects 11 }

egwAlertCallType OBJECT-TYPE
    SYNTAX      INTEGER {
        emergency(1),
        test(2)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Call type:
         emergency(1)    - Emergency call,
         test(2)         - Test call"
    ::= { egwMIBNotifObjects 12 }

egwAlarmID OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..10))
    MAX-ACCESS  read-only

```

STATUS current

DESCRIPTION "The Alarm ID for each alarm.

egwAlarmID : egwAlarmName

AXL-01 : AXL - Failed to complete for the PBX

AXL-02 : AXL - Failed to retrieve IP Addresses

from CUCM

AXL-03 : AXL - Failed to retrieve phones from the CUCM

AXL-04 : AXL - Peer Check Failed

AXL-05 : AXL - Failed to retrieve Device Names

from CUCM

AXL-06 : Spark client could not be provisioned.

CFG-01 : LDAP Directory is not available

CFG-02 : LDAP server unreachable.

CFG-03 : Location Server Misconfiguration

CFG-04 : Location Server Time Out

CTI-01 : CTI could not create Routepoint

CTI-02 : CTI server login failure

CTI-03 : RLM Notifier CTI Login failed

CTI-04 : RLM Notifier push to phone failed

CTI-05 : The CTI Service is flapping

DSH-01 : Dashboard login failed.

DSH-02 : Sending test SNMP trap

DIS-01 : Layer 2 Discovery - Could Not Scan

Switch

DIS-02 : Layer 2 Discovery - Duplicate MAC Found

DIS-03 : Layer 2 Discovery - Invalid Scan

DIS-04 : Layer 2 Discovery - MAC Location Has

Changed

DIS-05 : Layer 2 Discovery - MAC Location Has

Changed To ECRC

DIS-06 : Layer 2 Discovery - Peer Check Failed

DIS-07 : WLAN Controller is unreachable

DIS-08 : Wlan Discovery - Multiple Access Points

found for a BSSID

MON-01 : All routes are down

MON-05 : EGW license successfully activated

MON-06 : EGW licensing problem: Entering Grace

Period

MON-07 : EGW licensing problem: Grace period over

MON-08 : EGW licensing problem: Reminder EGW

currently in grace period

MON-09 : Unreachable ERS server.

MON-10 : Unreachable PBX Server

MON-11 : Connectivity to RLM Proxy server was lost.

main call leg.

RTE-01 : Call detail records request failed on

RTE-02 : Call detail records request failed on

security desk call leg.

RTE-03 : Call leg to ERS SBC failed.

RTE-04 : Call route to ECRC via ERS unavailable.

RTE-05 : Call route to ERS SBC unavailable.

RTE-06 : Call to ECRC via ERS failed.

RTE-07 : Callback call leg failed.

RTE-08 : Callback call route unavailable.

RTE-10 : ECRC call leg failed.

RTE-11 : ECRC call route unavailable.
 RTE-12 : Extension Missing
 RTE-13 : Fallback call failed.
 RTE-14 : IP-PBX not found
 RTE-15 : Local Trunking call leg failed.
 RTE-16 : Local trunking call route unavailable.
 RTE-17 : SBC unable to retrieve routing
 instructions from CPM.
 RTE-18 : Security desk call leg failed.
 RTE-19 : Security desk call route unavailable.
 RTE-20 : Caller location from location server
 could not be retrieved
 Domain/IP
 SCH-02 : CDR Export Scheduled Task Failed
 SCH-03 : Unresolved configured pbx server
 SYS-01 : Database Connection Failure
 SYS-02 : EGW Status Error
 SYS-03 : Mail Server Down
 SYS-04 : Max Endpoints Exceeded
 SYS-05 : CPM at Primary EGW timed out
 SYS-06 : SOAP call failure
 MON-12 : Number of currently logged in users
 reached the warning level (Nagios currently has 20 should probably be 1)
 MON-13 : Number of currently logged in users
 reached the critical level (Maybe we should just have one alarm that triggers
 as soon as someone logs in.)
 SYS-07 : Number of running process has reached
 the warning level (800)
 SYS-08 : Number of running process has reached
 the critical level (1000)
 SYS-09 : CPU average load has reached warning
 level (5.0,4.0,3.0)
 SYS-10 : CPU average load has reached warning
 level (10.0,6.0,4.0)
 SYS-11 : Swap usage has reached warning level
 (only 20% free sapce remaining)
 SYS-12 : Swap usage has reached critical level
 (only 10% free sapce remaining)
 MON-14 : Local SSH service is unavailable
 MON-15 : Local HTTPD service is unreachable
 MON-16 : Peer HTTPD servive is unreachable
 MON-17 : Local EGW database cannot be accessed
 MON-18 : Peer EGW database cannot be accessed
 MON-19 : Local MySQL server is unreachable
 MON-20 : Peer MySQL server is unreachable
 MON-21 : Local Mail Server is unreachable
 MON-22 : Local SBC is unreachable
 MON-23 : Peer SBC is unreachable
 MON-25 : /boot file system Disk Space Warning.
 MON-26 : /boot file system Disk Space Critical.
 MON-27 : Root file system disk space warning
 MON-28 : Root file system disk space critical
 MON-29 : /var/spool file system disk space
 warning
 MON-30 : /var/spool file system disk space
 critical
 MON-31 : /var/log file system disk space warning

```

MON-32      : /var/log file system disk space critical
MON-33      : /home file system disk space warning
MON-34      : /home file system disk space critical
MON-35      : /opt/911Gateway/core file system disk
space warning
MON-36      : /opt/911Gateway/core file system disk
space critical
SYS-13      : Local system IP address is unreachable
SYS-14      : Peer system IP address is unreachable
"
 ::= { egwMIBNotifObjects 13 }

egwAlarmName OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..100))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The Alarm Name for each alarm."
    ::= { egwMIBNotifObjects 14 }

egwAlarmOccurrences OBJECT-TYPE
    SYNTAX      INTEGER
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "A numeric value indicating the number of times the alarm
instance has been raised."
    ::= { egwMIBNotifObjects 15 }

egwAlarmUUID   OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..100))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "A unique alphanumeric ID that binds all the instances of
an alarm (raised or cleared) together"
    ::= { egwMIBNotifObjects 16 }

-- **** Notifications ****
-- **** Notifications ****

egwAlarms NOTIFICATION-GROUP
    NOTIFICATIONS { egwApplicationRaiseNotification,
egwCTILinkUpNotification, egwCTILinkDownNotification,
egwERSLinkUpNotification, egwERSLinkDownNotification,
egwPBXLinkUpNotification, egwPBXLinkDownNotification,
egwAllRoutesDownNotification, egwRoutesUpNotification,
egwApplicationClearNotification, egwCTILinkUnstableNotification  }
    STATUS      current
    DESCRIPTION "Emergency Gateway Alarms"
    ::= { egwMIBGroups 2 }

egwAlerts NOTIFICATION-GROUP
    NOTIFICATIONS { egwCrisisAlert, egwUnprovisionedAlert,
egwOffCampusAlert }
    STATUS      current
    DESCRIPTION "Emergency Gateway Alerts"
    ::= { egwMIBGroups 3 }

```

```

egwApplicationRaiseNotification NOTIFICATION-TYPE
    OBJECTS {
        egwAlarmID,
        egwAlarmName,
        egwAlarmText,
        egwAlarmLevel,
        egwAlertTimestamp,
        egwServerType,
        egwAlarmOccurrences,
        egwAlarmUUID
    }
    STATUS current
    DESCRIPTION
        "This notification will be sent when any alarm other than
        'The CTI service on EGW could not create terminal on the PBX', 'Unreachable
        ERS server' 'Unreachable PBX server', or 'All routes are down' is raised on
        the West Safety Services Emergency Gateway (EGW)."
        ::= { egwMIBNotifications 1 }

egwCrisisAlert NOTIFICATION-TYPE
    OBJECTS {
        egwAlertCallback,
        egwAlertEndpoint,
        egwAlertCallingPartyName,
        egwAlertIpPbxName,
        egwAlertTimestamp,
        egwAlertUrlData,
        egwAlertLocation,
        egwServerType,
        egwAlertCallType
    }
    STATUS current
    DESCRIPTION
        "This notification will be sent when an emergency call
        is handled on the West Safety Services Emergency Gateway
        (EGW)."
        ::= { egwMIBNotifications 2 }

egwUnprovisionedAlert NOTIFICATION-TYPE
    OBJECTS {
        egwAlertCallback,
        egwAlertEndpoint,
        egwAlertCallingPartyName,
        egwAlertIpPbxName,
        egwAlertTimestamp,
        egwServerType,
        egwAlertCallType
    }
    STATUS current
    DESCRIPTION
        "This notification will be sent when an emergency call
        is handled on the West Safety Services Emergency Gateway
        (EGW) but the
            EGW is unable to determine the location of the caller."
        ::= { egwMIBNotifications 3 }

```

```

egwOffCampusAlert NOTIFICATION-TYPE
    OBJECTS {
        egwAlertCallback,
        egwAlertEndpoint,
        egwAlertCallingPartyName,
        egwAlertIpPbxName,
        egwAlertTimestamp,
        egwAlertLocation,
        egwServerType,
        egwAlertCallType
    }
    STATUS current
    DESCRIPTION
        "This notification will be sent when an emergency call
        is handled on the West Safety Services Emergency Gateway
        (EGW) and the
            caller has been identified as being off-campus."
    ::= { egwMIBNotifications 4 }

egwCTILinkUpNotification NOTIFICATION-TYPE
    OBJECTS {
        egwAlarmID,
        egwAlarmName,
        egwAlarmText,
        egwAlarmLevel,
        egwAlertTimestamp,
        egwServerType,
        egwAlarmOccurrences,
        egwAlarmUUID
    }
    STATUS current
    DESCRIPTION
        "This notification will be sent when 'The CTI service on EGW
        could not create terminal on the PBX' alarm
            is cleared on the West Safety Services Emergency Gateway
        (EGW) .
            egwAlarmID contains CTI-01."
    ::= { egwMIBNotifications 5 }

egwCTILinkDownNotification NOTIFICATION-TYPE
    OBJECTS {
        egwAlarmID,
        egwAlarmName,
        egwAlarmText,
        egwAlarmLevel,
        egwAlertTimestamp,
        egwServerType,
        egwAlarmOccurrences,
        egwAlarmUUID
    }
    STATUS current
    DESCRIPTION
        "This notification will be sent when 'The CTI service on EGW
        could not create terminal on the PBX' alarm
            is raised on the West Safety Services Emergency Gateway
        (EGW) .
            egwAlarmID contains CTI-01."

```

```

 ::= { egwMIBNotifications 6 }

egwERSLinkUpNotification NOTIFICATION-TYPE
    OBJECTS {
        egwAlarmID,
        egwAlarmName,
        egwAlarmText,
        egwAlarmLevel,
        egwAlertTimestamp,
        egwServerType,
        egwAlarmOccurrences,
        egwAlarmUUID
    }
    STATUS current
    DESCRIPTION
        "This notification will be sent when 'Unreachable ERS server' alarm is cleared on the West Safety Services Emergency Gateway (EGW). egwAlarmID contains MON-09."
    ::= { egwMIBNotifications 7 }

egwERSLinkDownNotification NOTIFICATION-TYPE
    OBJECTS {
        egwAlarmID,
        egwAlarmName,
        egwAlarmText,
        egwAlarmLevel,
        egwAlertTimestamp,
        egwServerType,
        egwAlarmOccurrences,
        egwAlarmUUID
    }
    STATUS current
    DESCRIPTION
        "This notification will be sent when 'Unreachable ERS server' alarm is raised on the West Safety Services Emergency Gateway (EGW). egwAlarmID contains MON-09."
    ::= { egwMIBNotifications 8 }

egwPBXLinkUpNotification NOTIFICATION-TYPE
    OBJECTS {
        egwAlarmID,
        egwAlarmName,
        egwAlarmText,
        egwAlarmLevel,
        egwAlertTimestamp,
        egwServerType,
        egwAlarmOccurrences,
        egwAlarmUUID
    }
    STATUS current
    DESCRIPTION
        "This notification will be sent when 'Unreachable PBX server' alarm is cleared on the West Safety Services Emergency Gateway (EGW). egwAlarmID contains MON-10."
    ::= { egwMIBNotifications 9 }

egwPBXLinkDownNotification NOTIFICATION-TYPE

```

```

OBJECTS {
    egwAlarmID,
    egwAlarmName,
    egwAlarmText,
    egwAlarmLevel,
    egwAlertTimestamp,
    egwServerType,
    egwAlarmOccurrences,
    egwAlarmUUID
}
STATUS current
DESCRIPTION
    "This notification will be sent when 'Unreachable PBX server' alarm is raised on the West Safety Services Emergency Gateway (EGW). egwAlarmID contains MON-10."
    ::= { egwMIBNotifications 10 }

egwAllRoutesDownNotification NOTIFICATION-TYPE
OBJECTS {
    egwAlarmID,
    egwAlarmName,
    egwAlarmText,
    egwAlarmLevel,
    egwAlertTimestamp,
    egwServerType,
    egwAlarmOccurrences,
    egwAlarmUUID
}
STATUS current
DESCRIPTION
    "This notification will be sent when 'All routes are down' alarm is raised on the West Safety Services Emergency Gateway (EGW). egwAlarmID contains MON-01."
    ::= { egwMIBNotifications 11 }

egwRoutesUpNotification NOTIFICATION-TYPE
OBJECTS {
    egwAlarmID,
    egwAlarmName,
    egwAlarmText,
    egwAlarmLevel,
    egwAlertTimestamp,
    egwServerType,
    egwAlarmOccurrences,
    egwAlarmUUID
}
STATUS current
DESCRIPTION
    "This notification will be sent when 'All routes are down' alarm is cleared on the West Safety Services Emergency Gateway (EGW). egwAlarmID contains MON-01."
    ::= { egwMIBNotifications 12 }

egwApplicationClearNotification NOTIFICATION-TYPE
OBJECTS {
    egwAlarmID,

```

```

egwAlarmName,
egwAlarmText,
egwAlarmLevel,
egwAlertTimestamp,
egwServerType,
egwAlarmOccurrences,
egwAlarmUUID
}
STATUS current
DESCRIPTION
    "This notification will be sent when any alarm other than
'The CTI service on EGW could not create terminal on the PBX', 'Unreachable
ERS server' 'Unreachable PBX server', or 'All routes are down' is cleared on
the West Safety Services Emergency Gateway (EGW)."
 ::= { egwMIBNotifications 13 }

egwCTILinkUnstableNotification NOTIFICATION-TYPE
OBJECTS {
    egwAlarmID,
    egwAlarmName,
    egwAlarmText,
    egwAlarmLevel,
    egwAlertTimestamp,
    egwServerType,
    egwAlarmOccurrences,
    egwAlarmUUID
}
STATUS current
DESCRIPTION
    "This notification will be sent when 'The CTI Service is
flapping' alarm is raised on the West Safety Services Emergency Gateway
(EGW). egwAlarmID contains CTI-05."
 ::= { egwMIBNotifications 14 }

```

END