E-SBC
Administration Guide
Release 4.0.5

Part Number: 010-5424-405v1.00
Release Date: November 2011

This page intentionally left blank.

E-SBC Administration Guide

Sipera Systems, Inc.
010-5424-405v1.00

Notice

The information contained in this document is subject to change without notice. This documentation is provided "as is" and Sipera Systems, Inc. disclaims any implied warranties, including the implied warranties of fitness for a particular purpose and merchantability. Sipera Systems, Inc. assumes no responsibility or obligation of any kind for errors contained herein or in connection with the furnishing, performance, or use of this document.

The Sipera software described in this documents a) is the property of Sipera Systems, Inc. or its third party licensors, b) is provided only under a license that can be requested from Sipera Systems, Inc., and c) may be copied and used only as expressly permitted under the terms of the license.

IMPORTANT:	**Before you install the appliance, we recommend that you contact Sipera Systems Support to register your appliance and to check for available upgrades.**

United States Export Control Laws Notice

Sipera Systems, Inc., products and software are subject to United States Export Control Laws. The resale, export, re-export, transfer, and/or shipment of this product and the end user of them are restricted by these U.S. laws. Any unauthorized end use, resale, export, re-export, transfer, and/or shipment of the product or software can lead to criminal and/or civil penalties, including large fines and denial of export privileges.

Trademarks or Service Marks

The following are trademarks or service marks of Sipera Systems, Inc.

Sipera Systems, Inc., Sipera, and the Sipera logo in all its forms.

All other product names and company names mentioned in this document are trademarks or registered trademarks of their respective holders.

Copyright and Confidentiality

Copyright © 2011 by Sipera Systems, Incorporated. All rights reserved. No part of this document may be reproduced, distributed, modified or translated without the prior written consent of Sipera Systems, Inc. This document is confidential information of Sipera Systems, Inc. and no third party shall be given access to this document without the written permission of Sipera Systems, Inc.

Printed in the United States of America.

Manual Name: E-SBC Administration Guide
Part Number: 010-5424-404v1.00
Release: **4.04**
Print Date: **April 2011**

Sipera Systems, Inc.
1900 Firman Drive; Ste. 600
Richardson, TX 75081

Contents

Preface

Audience xxix
Notation Conventions xxix
Notice Icons xxix
Text Conventions xxx
Revision Information xxx
Manual Organization xxxi
Related Manuals xxxii
Ordering Manuals xxxiii
How to Comment on this Manual xxxiii

Chapter 1. Introduction

E-SBC Overview 1-1
Feature Descriptions 1-3
SIP Trunking 1-3
High-Availability (EMS/E-SBC-1U) 1-4
EMS 1-4
E-SBC HA Pairs 1-5
E-SBC HA Configurations 1-6
E-SBC High Availability (HA) Configurations 1-6
Designated Active Configuration 1-7
Unified Communications (UC) Intrusion Protection 1-8
E-SBC Hardening 1-8
General Protection against Layer 3/Layer 4 Floods and Port Scans 1-8
ICMP Flood Prevention 1-8
Port Scan Blocking 1-9
Management Interface Restrictions on Ports That Can Be Opened 1-9
Data Interface Restrictions 1-9
TCP Signaling Level Flood Control 1-9
System-Wide Security Settings 1-10
Attack Protection 1-10
Monitoring 1-10
Detection 1-10
Protection 1-11
Functional Entities 1-11
Signaling 1-11
Media 1-12
E-SBC Deployment 1-12
Two-Wire 1-13
One-Wire 1-13
Managing E-SBC Security Devices 1-14
Graphical User Interface (GUI) 1-14
E-SBC Control Center 1-14
Command Line Interface (CLI) 1-15

Chapter 2. Getting Started

Prerequisites 2-1
Passwords 2-1
There are two types of passwords associated with E-SBC: 2-1
Console Password Complexity 2-1
EMS GUI Password Complexity 2-1

Password Policies 2-2
Logging-In to the E-SBC Control Center 2-2
Initial Login 2-2
E-SBC Control Center Screen Descriptions 2-4
Identification Bar 2-5
Tool Bar 2-5
Location Bar 2-6
Task Pane 2-7
Welcome 2-9
Administration 2-9
Backup/Restore 2-9
System Management 2-9
Global Parameters 2-10
Global Profiles 2-11
Domain Policies 2-12
Device Specific Settings 2-14
Troubleshooting 2-16
TLS Management 2-17
Application Pane 2-18
Content Area 2-18
General Introductory and Welcome Information 2-19
Alarms 2-19
Latest Incidents 2-20
Administrator Notes 2-21
Quick Links 2-21
Installed E-SBC Security Device List 2-21
Screen Pushbuttons and Icons 2-22

Chapter 3. Managing Administrative User Accounts

Managing Administrative User Accounts 3-1
Administrative Accounts 3-2
Creating a New Administrative Account 3-2
Setting Administrative Account Privileges 3-4
Editing an Existing Administrative Account 3-6
Deleting an Existing Administrative Account 3-7
Adding an E-SBC Device 3-7
Provisioning an E-SBC Device 3-8

Chapter 4. Device Configuration

Prerequisites 4-1
Installing an E-SBC Device 4-1
E-SBC High Availability (HA) Configurations 4-7
Updating EMS Software 4-10
Upgrade EMS from a Local File 4-10
Upgrade EMS from an Uploaded File 4-11
Upgrade EMS – Non Service Affecting 4-11
Updating VIPER Signatures 4-13

Chapter 5. Domain Policy Administration

Governing Unified Communications with Domain Policies 5-1
Purpose 5-1
How They Work 5-1
Flows 5-1
Domain Policies 5-2
Profiles 5-2
Example: Call Server with E-SBC Securing SIP Trunk 5-3
To Be Created by User 5-3
End Point Policy 5-3
Session Policy 5-3
Configuring Rules and Policies 5-4
Architecture 5-4
Rules and Policies Associations 5-5
Rules and Profiles Configuration Steps Checklists 5-7
Application Rules Checklist 5-7
Border Rules Checklist 5-7
Media Rules Checklist 5-7
Domain DoS Profiles Checklist 5-8
Security Rules Checklist 5-8
Signaling Rules Checklist 5-8
Time of Day Rules Checklist 5-8
Creating a Policy Group Checklist 5-9
Session Policies Checklist 5-9
Points to Remember 5-9
Managing Domain Policies 5-11
Application Rules 5-11
Creating a New Application Rule 5-11
Cloning an Existing Application Rule 5-13
Editing an Existing Application Rule 5-14
Renaming an Existing Application Rule 5-15
Deleting an Existing Application Rule 5-16
Border Rules 5-16
Creating a New Border Rule 5-17
Cloning a Border Rule 5-19
Editing an Existing Border Rule 5-20
Renaming an Existing Border Rule 5-21
Deleting an Existing Border Rule 5-21
Media Rules 5-22
Creating a New Media Rule 5-22
Cloning an Existing Media Rule 5-29
Editing an Existing Media Rule 5-31
Renaming an Existing Media Rule 5-33
Deleting an Existing Media Rule 5-33
Configuring a Media Rule for Reverse Turing Test 5-34
Security Rules 5-44
Creating a New Security Rule 5-44
Cloning an Existing Security Rule 5-49
Editing an Existing Security Rule 5-50
Renaming an Existing Security Rule 5-52
Deleting an Existing Security Rule 5-52
Signaling Rules 5-53
Creating a New Signaling Rule 5-53
Editing an Existing Signaling Rule 5-59
General Parameters Tab 5-59

Requests Parameters Tab 5-60
Adding Request Parameters 5-60
Editing Request Parameters 5-61
Responses Parameters Tab 5-62
Adding Response Parameters 5-62
Editing Response Parameters 5-63
Request Headers Parameters Tab 5-64
Adding Request Header Parameters 5-64
Editing Request Header Parameters 5-65
Response Headers Parameters Tab 5-66
Adding Response Header Parameters 5-66
Editing Response Header Parameters 5-68
Signaling QoS Parameters Tab 5-68
Cloning an Existing Signaling Rule 5-69
Renaming an Existing Signaling Rule 5-71
Deleting an Existing Signaling Rule 5-71
Time-of-Day (ToD) Rules 5-72
Creating a New ToD Rule 5-72
Cloning an Existing ToD Rule 5-74
Editing an Existing ToD Rule 5-75
Renaming an Existing ToD Rule 5-76
Deleting an Existing ToD Rule 5-77
End-Point Policy Groups 5-78
Creating a New Policy Group 5-78
Viewing an Existing Policy Group Summary 5-81
Editing an Existing End-Point Policy Group 5-83
Deleting an Existing End-Point Policy Group 5-88
Session Policies 5-88
Creating a New Session Policy 5-88
Cloning an Existing Session Policy 5-91
Editing an Existing Session Policy 5-91
Renaming an Existing Session Policy 5-93
Deleting an Existing Session Policy 5-94
Managing End-Point and Session Flows 5-95
End-Point Flows 5-95
Creating a New Server End-Point Flow 5-95
Cloning an Existing End-Point Flow 5-97
Editing Existing Server End-Point Flows 5-98
Reordering the Precedence of End-Point Flows 5-99
Deleting an Existing End-Point Flow 5-100
Session Flows 5-101
Creating a New Session Flow 5-101
Cloning an Existing Session Flow 5-103
Editing Existing Session Flows 5-104
Reordering the Precedence of Session Flows 5-105
Deleting an Existing Session Flow 5-106
Uniform Resource Identifier (URI) Groups 5-107
Creating a New URI Group 5-107
Emergency Group 5-109
Adding an Additional URI to an Existing URI Group 5-110
Editing an Existing URI Group 5-111
Deleting a SIP URI from an Existing URI Group 5-112
Renaming an Existing URI Group 5-113
Deleting an Existing URI Group 5-113

Chapter 6. System Configuration

Basic Configuration Overview 6-1
Architecture 6-2
Basic Configuration Quick-Start Steps Checklists 6-3
Reconfigure E-SBC Checklist 6-4
Enabling Interfaces Checklist 6-4
Configuring URI Groups Checklist 6-4
Configuring Routing Profiles Checklist 6-5
Configuring Interworking Checklist 6-5
Adding Servers Checklist 6-6
Adding TLS Certificates Checklist 6-6
Adding TLS Server Profiles Checklist 6-7
Adding Domain Policy Groups Checklist 6-7
Adding Signal Interfaces Checklist 6-8
Adding Media Interfaces Checklist 6-8
Adding Server Flows Checklist 6-8
Adding Session Flows Checklist 6-9
Backup / Restore System Information 6-9
Designating a Snapshot Server 6-9
Making a System Snapshot (Backup) 6-11
Restoring a System Snapshot (Backup) 6-12
Manual Method 6-13
Automatic Method 6-16
Deleting a System Snapshot (Backup) 6-16
Automatic Snapshot Configuration 6-17
Managing Deployed E-SBC Security Devices 6-18
Establishing a Secure Shell Session 6-18
Shutdown and Reboot an E-SBC Security Device 6-21
Shutdown 6-21
Reboot 6-22
Restarting an E-SBC Application 6-23
Managing E-SBC Device Configurations 6-24
View Configuration 6-24
Edit Configuration 6-25
Delete Configuration 6-25
System Management Updates 6-26
Configuring Advanced Options 6-26
Enabling / Disabling E-SBC Logging Level 6-26
Viewing a CDR File 6-28
Enabling / Disabling E-SBC Security Features 6-31
Managing SIP Options 6-32
Port Options 6-33
Enabling HA 6-34
Configuring HA Heartbeat Interval and Max Retries 6-35
Managing Global Parameters 6-36
Managing RADIUS Authentication Parameters 6-36
Adding a New RADIUS Server 6-36
Editing an Existing RADIUS Server Profile 6-38
Deleting an Existing RADIUS Server Profile 6-39
Signaling Forking Overview 6-41
Adding a Signaling Forking Profile 6-41
SNMP Settings 6-41
Managing SNMP v1/v2 Access 6-45
Managing SNMP v3 Access 6-47
Routing Profiles 6-49

Creating a New Routing Profile 6-49
Cloning an Existing Routing Profile 6-51
Editing an Existing Routing Profile 6-53
Renaming an Existing Routing Profile 6-56
Deleting an Existing Routing Profile 6-57
Managing Syslog Parameters 6-58
Selecting Log Levels 6-58
Managing Device-Specific Settings 6-59
Managing Signaling Interface Parameters 6-59
Viewing an Existing Signaling Interface 6-59
Adding a New Signaling Interface 6-60
Editing an Existing Signaling Interface 6-62
Deleting an Existing Signaling Interface 6-62
Managing Media Interface Parameters 6-64
Viewing an Existing Media Interface 6-64
Adding a New Media Interface 6-65
Editing an Existing Media Interface 6-66
Deleting an Existing Media Interface 6-66

Chapter 7. Security Configuration

Overview 7-1
DoS Configurations 7-1
System Wide Single Endpoint DoS Configurations 7-1
Domain DoS Configurations 7-1
SIP Server DoS Configuration 7-1
DoS Security Features 7-2
DoS/DDoS 7-2
Viewing DoS/DDoS Settings 7-2
Editing DoS/DDoS Settings 7-4
Domain DoS Profiles 7-4
Viewing an Existing Domain DoS Profile 7-4
Adding a New Domain DoS Profile 7-5
Cloning an Existing Domain DoS Profile 7-7
Renaming an Existing Domain DoS Profile 7-8
Editing an Existing Domain DoS Profile 7-9
Deleting an Existing Domain DoS Profile 7-9
Setting DoS Learning Parameters 7-10
Protocol Scrubber 7-11
Viewing Scrubber Rules 7-11
Installing a Scrubber Rules Package 7-12
Configuring Actions 7-13
Enabling / Disabling an Installed Scrubber Rules Package 7-13
Deleting an Existing Scrubber Rules Package 7-13
Topology Hiding 7-14
Creating a New Topology Hiding Profile 7-14
Adding a New Topology Hiding Header 7-17
Editing a Topology Hiding Header 7-18
Deleting a Topology Hiding Profile or Header 7-19
Delete a Topology Hiding Profile 7-19
Delete a Topology Hiding Header 7-19
Cloning an Existing Topology Hiding Profile 7-20
Renaming an Existing Topology Hiding Profile 7-21
Headers Affected By Topology Hiding 7-22
Topology Hiding Settings Examples 7-24
Topology Hiding Examples for Request-Line Header 7-24

Topology Hiding Examples for From Header 7-25
Topology Hiding Examples for To Header 7-26
Topology Hiding Examples for Record-Route Header 7-27
Topology Hiding Examples for Via Header 7-28
Topology Hiding Examples for SDP Header 7-28

Chapter 8. Network Configuration

Overview 8-1
Managing SIP Server Configuration Profiles 8-1
Viewing SIP Server Profiles 8-1
Adding a New SIP Server Profile 8-1
Editing a SIP Server Profile 8-6
Editing the DoS Whitelist Parameter Tab 8-7
Adding a URI/Domain to the DoS Whitelist 8-8
Deleting a URI/Domain from the DoS Whitelist 8-8
Editing the DoS Protection Parameter Tab 8-9
Cloning an Existing SIP Server Profile 8-10
Renaming an Existing SIP Server Profile 8-11
Deleting an Existing SIP Server Profile 8-11
Interworking 8-13
Viewing Existing Interworking Profiles 8-13
Adding a New Interworking Profile 8-14
Editing Existing Interworking Profiles 8-19
Editing the General, Timers, and Advanced Parameter Tabs 8-19
Editing the URI Manipulation and Header Manipulation Parameter Tabs 8-21
Adding a New Regex Expression 8-21
Editing an Existing Regex Expression 8-23
Deleting an Existing Regex Expression 8-24
Adding New Header Manipulation Parameters 8-24
Editing Header Manipulation Parameters 8-25
Deleting Header Manipulation Parameters 8-26
Cloning an Existing Interworking Profile 8-26
Renaming an Existing Interworking Profile 8-27
Deleting an Existing Interworking Profile 8-28
Managing E-SBC Network Interfaces 8-28
Viewing Network Interface Settings 8-29
Editing Network Management Parameters 8-29
Editing the Network Configuration Tab 8-29
Adding a New Network Interface 8-29
Editing an Existing Network Interface 8-31
Deleting an Existing Network Interface 8-32
Editing the Administrative State of the Interface Configuration 8-33
Managing TLS Parameters 8-34
Managing Certificate Signing Requests (CSRs) 8-34
Installing Certificates 8-34
Creating a Certificate Signing Request (CSR) 8-37
Managing Client Profiles 8-40
Creating a New Client Profile 8-40
Editing a Client Profile 8-43
Deleting a Client Profile 8-44
Managing Server Profiles 8-45
Creating a New Server Profile 8-45
Editing a Server Profile 8-47
Deleting a Server Profile 8-48

Chapter 9. System Monitoring

Welcome Screen 9-1
Managing System Alarms 9-2
Viewing Current System Alarms 9-2
Deleting Current System Alarms 9-4
Viewing Current System Incidents 9-4
Viewing System Statistics 9-6
Viewing System Logs 9-7
Viewing Diagnostics Results 9-8
Viewing Administrative Users 9-10
Trace Settings 9-10
Packet Trace 9-10
Adding a New Packet Trace Profile 9-11
Editing an Existing Packet Trace Profile 9-13
Deleting an Existing Packet Trace Profile 9-13
Call Trace 9-14
Adding a New Call Trace Profile 9-16
Editing an Existing Call Trace Profile 9-17
Deleting an Existing Call Trace Profile 9-18
Viewing Packet Trace and Call Trace Data 9-19
Packet Capture 9-22
Audit Logs 9-25

Chapter 10. Command Line Interface (CLI)

Overview 10-1
Command Structure 10-1
Console Commands 10-1
Show Flow Dynamic 10-3
Instance Commands 10-3
Accessing the CLI 10-4
Remote clipcs Access 10-4
Local clipcs Access 10-7
Connecting a Terminal Device to the E-SBC Equipment Chassis 10-8
Establishing a Communications Session 10-10
Logging in to the Command Shell 10-11

Chapter 11. Configuration Workflows for SIP Trunking

SIP Trunking Overview 11-1
E-SBC Configuration for Generic SIP Trunk 11-2
Step-1 Create Routing Profiles 11-2
Create Routing Profile for Call Server 11-2
Create Routing Profile for Trunk Server 11-4
Step-2 Create Topology Hiding Profiles 11-6
Topology Hiding Profile for Call Server 11-6
Topology Hiding Profile for Trunk Server 11-8
Step-3 Create Interworking Profiles 11-10
Step-4 Create Server Profiles 11-11
Create Server Profile for Call Server 11-11
Create Server Profile for Trunk Side Server 11-15
Step-5 Create Signaling Interfaces 11-18
Create External Signaling Interface toward Trunk Server 11-18
Create Internal Signaling Interface Toward Call Server 11-19

Step-6 Create Media Interfaces 11-21
Create External Media Interface toward Trunk Server 11-21
Create Internal Media Interface Toward Call Server 11-22
Step-7 Create Server Flows 11-23
Create Flow toward Call Server 11-23
Create Flow Toward Trunk Server 11-25
Step-8 Server-Specific Configuration for SIP Trunking 11-28
E-SBC Configuration for Avaya Trunk 11-28
E-SBC Configuration for Cisco 11-32
E-SBC Configuration for Other Trunks 11-32

Chapter 12. Signaling Manipulation

Signaling Manipulation 12-1
SigMa Scripting Language 12-1
SigMa Primer 12-2
Session Statement 12-2
Act On Statements 12-3
Code Blocks 12-4
Built-In Variables and Arrays 12-6
Built-In Functions 12-9
User-Defined Variables 12-10
Hook Points 12-10
SigMa Scripting Examples 12-12
SigMa Scripting Tutorial 12-15
Test Case 1: Manipulation of P-Asserted-Identity Header 12-15
Test Case 2: Adding a Media Attribute in SDP 12-18
Test Case 3: Changing Calling Party Presentation to Restricted 12-19
Test Case 4: Replace “From” Header For a Set of Users 12-20
Test Case 5: Editing the “Allow” Header 12-22
Test Case 6: Prefix Stripping 12-24
E-SBC GUI SigMa Editor 12-25
Sigma Design Overview 12-27
Specifying a SigMa Script in a Server Configuration 12-28

Appendix A. Acronyms and Abbreviations

..... A-1

Appendix B. Glossary

..... B-1

Appendix C. System Alarm List

..... C-1

Appendix D. GUI and Console Alarm List

..... D-1

Appendix E. UC-Sec SNMP Details

..... E-1
UC-Sec OID Descriptions E-1
Private Enterprise OIDS supported on Sipera UC-Sec Appliance E-1
ipcs stats sip calls: .1.3.6.1.4.1.25257.1.4.1 ..... E-1
ipcs stats sip protocol: .1.3.6.1.4.1.25257.1.4.3 ..... E-1
Ipcsincidenceinfo: .1.3.6.1.4.1.25257.2 ..... E-1

Ipcsalarmainfo: .1.3.6.1.4.1.25257.4 ..... E-1
MIB Tree Structure E-1
Key OIDS E-2
Ipcsstatssipcalls E-2
Classification of Requests/Responses matching a particular Domain Policy Group at the node E-3
Out of Dialog Requests Dropped E-5
Out of Dialog Responses Dropped E-5
Out of Transaction Responses Dropped E-6
Statistics Details With Examples E-6
UC-Sec MIB E-7

Appendix F. UC-Sec Error Messages

..... F-1

Figures

Chapter 1. Introduction

Figure 1-1 The E-SBC Enterprise Session Border Controller Solution. 1-1
Figure 1-2. SIP Trunking. 1-3
Figure 1-3. EMS High-Availability (HA). 1-5
Figure 1-4. Typical E-SBC HA – Parallel Mode Topology (co-located) 1-6
Figure 1-5. System Management Screen 1-6
Figure 1-6. Install Device Icon 1-7
Figure 1-7. E-SBC Deployment – Two-Wire. 1-13
Figure 1-8. E-SBC Deployment – One-Wire. 1-14
Figure 1-9. E-SBC Control Center – Welcome Screen. 1-15

Chapter 2. Getting Started

Figure 2-1. E-SBC Control Center – Login Screen. 2-3
Figure 2-2. E-SBC Control Center – Welcome Screen Description 2-3
Figure 2-3. E-SBC Control Center – Functional Screen Description 2-4
Figure 2-4. E-SBC Control Center – Welcome Screen 2-5
Figure 2-5. Identification Bar. 2-5
Figure 2-6. Tool Bar. 2-5
Figure 2-7. Example of Location Bar Information. 2-6
Figure 2-8. E-SBC Control Center Task Pane. 2-7
Figure 2-9. Task Pane Elements 2-8
Figure 2-10. Administration Function. 2-9
Figure 2-11. Backup / Restore Function. 2-9
Figure 2-12. System Management. 2-9
Figure 2-13. Global Parameters Feature (Expanded View). 2-10
Figure 2-14 Global Profiles Feature 2-11
Figure 2-15. Domain Policy Feature (Expanded View). 2-13
Figure 2-16. Device Specific Settings Feature (Expanded View) 2-15
Figure 2-17. Troubleshooting Feature (Expanded View). 2-16
Figure 2-18. TLS Management Feature (Expanded View). 2-17
Figure 2-19. E-SBC Control Center – Application Pane. 2-18
Figure 2-20. E-SBC Control Center – Content Area. 2-18

Figure 2-21. E-SBC Control Center – Content Area (Welcome Screen). 2-19
Figure 2-22. Welcome Screen Content Area Descriptions. 2-19
Figure 2-23. Current System Alarms List. 2-19
Figure 2-24. Alarms Window. 2-20
Figure 2-25. Current System Incidents List. 2-20
Figure 2-26. Incidents Window. 2-20
Figure 2-27. Administrator Notes. 2-21
Figure 2-28. Quick Links. 2-21
Figure 2-29. Installed E-SBC Security Device List. 2-21

Chapter 3. Managing Administrative User Account

Figure 3-1. Available Administrative Functions by Access Level 3-1
Figure 3-2. Default Administration Display. 3-2
Figure 3-3. Add New Administrative User Pop-up Window. 3-2
Figure 3-4. Updated Administration Display. 3-3
Figure 3-5. Administration Parameters Tab Display. 3-4
Figure 3-6. Administration Parameters Confirmation Display. 3-5
Figure 3-7. Edit Administrative User Pop-up Window 3-6
Figure 3-8. Delete Confirmation Pop-up Window. 3-7
Figure 3-9. Updated Administration Display. 3-7
Figure 3-10. System Management Screen 3-8
Figure 3-11. Add Device Pop-Up Window 3-8
Figure 3-12. Installation Pop-Up Window 3-9

Chapter 4. Device Configuration

Figure 4-1. Installation Pop-up Window. 4-2
Figure 4-2. Selecting a Network Type. 4-4
Figure 4-3. Selecting a Network Topology. 4-4
Figure 4-4. Network Settings Pop-up Window 4-5
Figure 4-5. Final Installation Window 4-7
Figure 4-6. System Management Screen 4-7
Figure 4-7. Installation Wizard Screen 1 4-8
Figure 4-8. Installation Wizard Screen 2 4-8
Figure 4-9. System Information Screen Part 1 4-9
Figure 4-10. System Information Screen Part 2 4-9
Figure 4-11. System Management Screen - Updates Tab Display. 4-10
Figure 4-12. Upgrading the EMS from a Local File. 4-11
Figure 4-13. Upgrading the EMS from an Uploaded File. 4-11

Chapter 5. Domain Policy Administration

Figure 5-1 UC Policy Process 5-1
Figure 5-2 Securing a SIP Trunk 5-4
Figure 5-3 E-SBC Architecture 5-5
Figure 5-4 Rules and Policies Associations 1 5-5
Figure 5-5 Rules and Policies Associations 2 5-6
Figure 5-6 Rules and Policies Associations 3 5-6
Figure 5-7 End-Point Policy Groups Assigned to Server Flows 5-10
Figure 5-8 Session Policies Assigned to Session Flows 5-10
Figure 5-9 Application Rules Screen. 5-11
Figure 5-10 Add Application Rule Pop-up Window. 5-11
Figure 5-11 Add Application Rule Pop-up Window. 5-12

Figure 5-12 New Application Rule Display..... 5-13
Figure 5-13 Selecting an Existing Application Rule..... 5-14
Figure 5-14. Clone Application Rule Pop-up Window..... 5-14
Figure 5-15 Updated Application Rules Screen..... 5-14
Figure 5-16. Edit Application Rule Pop-up Window..... 5-15
Figure 5-17. Rename Application Rule Pop-up Window. 5-16
Figure 5-18. Delete Confirmation Pop-up Window..... 5-16
Figure 5-19 Border Rules Screen..... 5-17
Figure 5-20. Add Border Rule Pop-up Window. 5-17
Figure 5-21. Add Borer Rule Pop-up Window. 5-18
Figure 5-22 Updated Border Rules Screen. 5-19
Figure 5-23. Clone Border Rule Pop-up Window..... 5-20
Figure 5-24 Updated Border Rule Screen..... 5-20
Figure 5-25 NAT Traversal Pop-up Window. 5-21
Figure 5-26. Rename Border Rule Pop-up Window..... 5-21
Figure 5-27. Delete Confirmation Pop-up Window..... 5-22
Figure 5-28. Media Rules Information Screen..... 5-22
Figure 5-29. Add Media Rule Pop-up Window 1. 5-23
Figure 5-30. Add Media Rule Pop-up Window 2. 5-23
Figure 5-31. Add Media Rule Pop-up Window 3. 5-24
Figure 5-32. Add Media Rule Pop-up Window 4. 5-25
Figure 5-33. Add Media Rule Pop-up Window 5. 5-26
Figure 5-34. Add Media Rule Pop-up Window 6. 5-26
Figure 5-35. Add Media Rule Pop-up Window 7. 5-27
Figure 5-36. Add Media Rule Pop-up Window 8. 5-28
Figure 5-37. Add Media Rule Pop-up Window 9. 5-29
Figure 5-38. Updated Media Rule Screen..... 5-29
Figure 5-39. Media Rules Screen..... 5-30
Figure 5-40. Selecting an Existing Media Rule Set. 5-30
Figure 5-41 Clone Rule Pop-up Window..... 5-30
Figure 5-42. Updated Media Rule Screen..... 5-31
Figure 5-43 Selecting Media Rule Parameter Tabs. 5-31
Figure 5-44 Media Encryption Pop-up Window..... 5-32
Figure 5-45. Rename Rule Pop-up Window..... 5-33
Figure 5-46. Delete Confirmation Pop-up Window..... 5-33
Figure 5-47 Selecting Media Rules..... 5-35
Figure 5-48 Add Media Rule Screen 1 5-35
Figure 5-49 Add Media Rule Screen 2 5-35
Figure 5-50 Add Media Rule Screen 3 5-36
Figure 5-51 Add Media Rule Screen 4 5-36
Figure 5-52 Add Media Rule Screen 5 5-36
Figure 5-53 Add Media Rule Screen 6 37
Figure 5-54 Add Media Rule Screen 7 5-37
Figure 5-55 Add Media Rule Screen 8 5-38
Figure 5-56 Add Media Rule Screen 8 5-39
Figure 5-57 Policy Groups Screen..... 5-39
Figure 5-58 Add Policy Group Screen 1..... 5-39
Figure 5-59 Add Policy Group Screen 2..... 5-40
Figure 5-60 Updated Policy Groups Screen..... 5-40
Figure 5-61 Subscriber and Server Flows Screen 5-41
Figure 5-62 Server Flows Screen..... 5-41
Figure 5-63 Editing the Trunk Server Flow..... 5-42
Figure 5-64 Edit Flow Screen..... 5-42
Figure 5-65 Selecting Media Rules Turing Tab..... 5-43
Figure 5-66 Turing Tab Edit Screen 5-43
Figure 5-67 Security Rules Display Screen. v44

Figure 5-68 Add Security Rule Pop-up Window. 5-45
Figure 5-69 Add Security Rule: Authentication Pop-up Window. 5-45
Figure 5-70 Add Security Rule: Compliance Pop-up Window. 5-45
Figure 5-71 Add Security Rule: Fingerprint Profile Pop-up Window. 5-46
Figure 5-72 Add Security Rule: Scrubber Profile Pop-Up Window. 5-46
Figure 5-73 Scrubbers Feature of Global Parameters 5-47
Figure 5-74 Add Security Rule: Domain DoS Pop-up Window. 5-47
Figure 5-75 Domain DoS Feature of Global Profiles 5-48
Figure 5-76 Updated Security Rule Screen. 5-49
Figure 5-77 Selecting an Existing Security Rule Set. 5-49
Figure 5-78 Clone Rule Pop-up Window 5-49
Figure 5-79 Updated Security Rule Display Screen. 5-50
Figure 5-80 Selecting an Existing Security Rule Set. 5-50
Figure 5-81 Security Rule Set Parameter Tabs. 5-51
Figure 5-82 Edit Security Rule: Authentication Pop-up Window. 5-51
Figure 5-83 Edit Domain DoS Pop-up Window. 5-52
Figure 5-84 Rename Security Rule Pop-up Window. 5-52
Figure 5-85 Delete Confirmation Pop-up Window. 5-53
Figure 5-86 Signaling Rules Display Screen. 5-54
Figure 5-87 Add Signaling Rule Pop-up Window. 5-54
Figure 5-88 Add Signaling Rule Pop-up Window. 5-54
Figure 5-89 Add Signaling Rule: QoS Pop-up Window. 5-58
Figure 5-90 Updated Signaling Rule Screen. 5-58
Figure 5-91 Signaling Rule Parameter Tabs. 5-59
Figure 5-92 General Control Pop-up Window. 5-60
Figure 5-93 Add Request Control Pop-up Window. 5-60
Figure 5-94 Updated Requests Parameters Tab. 5-61
Figure 5-95 Edit Request Control Pop-up Window. 5-62
Figure 5-96 Add Response Control Pop-up Window. 5-62
Figure 5-97 Updated Responses Parameters Tab. 5-63
Figure 5-98 Edit Response Control Pop-up Window 5-64
Figure 5-99 Add Header Control Pop-up Window. 5-64
Figure 5-100 Edit Header Control Pop-up Window. 5-66
Figure 5-101 Add Header Control Pop-up Window. 5-66
Figure 5-102 Updated Responses Headers Parameters Tab. 5-67
Figure 5-103 Edit Response Header Control Pop-up Window. 5-68
Figure 5-104 Signaling QoS Pop-up Window. 5-68
Figure 5-105 Selecting an Existing Signaling Rule. 5-69
Figure 5-106 Clone Rule Pop-up Window 5-70
Figure 5-107 Updated Signaling Rules Display 5-70
Figure 5-108 Rename Rule Pop-up Window. 5-71
Figure 5-109 Delete Confirmation Pop-up Window. 5-71
Figure 5-110 Time-of-Day Rules Display Screen 5-72
Figure 5-111 Add Rule Pop-up Window. 5-72
Figure 5-112 Add ToD Parameters Pop-up Window. 5-73
Figure 5-113 New ToD Rule. 5-74
Figure 5-114 Selecting an Existing ToD Rule. 5-75
Figure 5-115 Clone Rule Pop-up Window 5-75
Figure 5-116 Selecting an Existing Time-of-Day Rule. 5-76
Figure 5-117 Edit Time-of-Day Rule Pop-up Window. 5-76
Figure 5-118 Rename Rule Pop-up Window. 5-77
Figure 5-119 Delete Confirmation Pop-up Window. 5-77
Figure 5-120 Policy Groups Display Screen. 5-79
Figure 5-121 Add Policy Group Name Pop-up Window. 5-79
Figure 5-122 Add Policy Group Screen. 5-80
Figure 5-123 New End-Point Policy Group Display. 5-80

Figure 5-124 Selecting an Existing Policy Group..... 5-81
Figure 5-125 End-Point Policy Group Summary Report. 5-82
Figure 5-126 Add Policy Set Pop-up Window. 5-83
Figure 5-127 Updated End-Point Policy Set Display..... 5-84
Figure 5-128 Policy Group Display Screen. 5-85
Figure 5-129 Selecting a Policy Group. 5-85
Figure 5-130 Selecting a New Order of Precedence for Existing Policy Sets. 5-86
Figure 5-131 Reordered Policy Set Display..... 5-86
Figure 5-132 Edit Policy Set Pop-up Window..... 5-87
Figure 5-133 Delete Confirmation Pop-up Window. 5-87
Figure 5-134 Delete Confirmation Pop-up Window. 5-88
Figure 5-135 Session Policies Display..... 5-89
Figure 5-136 Add Session Policy Pop-up Window. 5-89
Figure 5-137 Codec Prioritization Pop-up Window. 5-89
Figure 5-138 Media Anchoring Pop-up Window. 5-90
Figure 5-139 Media Forking Pop-up Window..... 5-91
Figure 5-140 Clone Policy Pop-up Window. 5-91
Figure 5-141 Codec Prioritization Pop-up Window. 5-92
Figure 5-142 Media Anchoring Pop-up Window. 5-93
Figure 5-143 Selecting an Existing Session Policy. 5-94
Figure 5-144 Rename Policy Pop-up Window. 5-94
Figure 5-145 Add Flow Pop-Up Window..... 5-96
Figure 5-146 Updated Server End-Point Flow Display. 5-97
Figure 5-147 Clone Flow: Criteria Pop-up Window..... 5-98
Figure 5-148 Updated Server End-Point Flow Display. 5-98
Figure 5-149 Edit Flow: Criteria Pop-up Window..... 5-99
Figure 5-150 Selecting a New Order of Precedence for Existing End-Point Flows. 5-100
Figure 5-151 Reordered End-Point Flows. 5-100
Figure 5-152 Delete Confirmation Pop-up Window. 5-100
Figure 5-153 Session Flow Display. 5-101
Figure 5-154 Selecting an E-SBC Device..... 5-101
Figure 5-155 Add Flow Pop-up Window..... 5-102
Figure 5-156 Updated Session Flow Display..... 5-102
Figure 5-157 Clone Flow Pop-up Window. 5-103
Figure 5-158 Updated Session Flow Display..... 5-104
Figure 5-159 Edit Flow Pop-up Window. 5-104
Figure 5-160 Selecting a New Order of Precedence for Existing Session Flows. 5-105
Figure 5-161 Reordered Session Flows. 5-105
Figure 5-162 Selecting an E-SBC Device..... 5-106
Figure 5-163 Delete Confirmation Pop-up Window. 5-106
Figure 5-164 URI Groups Feature of Global Profiles..... 5-107
Figure 5-165 URI Group Display. 5-107
Figure 5-166 Add URI Group Pop-up Window. 5-108
Figure 5-167 Subsequent Add URI Pop-up Window..... 5-108
Figure 5-168 New URI Group Display. 5-109
Figure 5-169 Emergency Group 5-110
Figure 5-170 Selected URI Group Display. 5-110
Figure 5-171 Add URI Pop-up Window. 5-111
Figure 5-172 New URI Group Display. 5-111
Figure 5-173 Edit URI Pop-up Window. 5-111
Figure 5-174 Delete Confirmation Pop-up Window. 5-112
Figure 5-175 Rename URI Group Pop-up Window..... 5-113
Figure 5-176 Association Notification Pop-up Window..... 5-113
Figure 5-177 Delete Confirmation Pop-up Window. 5-114

Chapter 6. System Configuration

Figure 6-1 E-SBC Architecture 6-2
Figure 6-2 Basic Overall Configuration Steps 6-3
Figure 6 - 1 Typical Backup/Restore Screen 6-9
Figure 6-2 Backup/Restore Screen - Snapshot Servers Tab Display 6-10
Figure 6-3 Add Snapshot Server Pop-up Window 6-10
Figure 6-4 Updated Backup/Restore Screen - Snapshot Servers Tab Display 6-11
Figure 6-5. Create Snapshot Pop-up Window 6-12
Figure 6-6. Snapshot Notification Banner. 6-12
Figure 6-7. Updated Backup/Restore Screen - Snapshots Tab Display. 6-12
Figure 6-8. Selecting a Snapshot Server. 6-13
Figure 6-9. Designating a Snapshot File Action. 6-14
Figure 6-10. Directory Dialog Pop-up Window 6-14
Figure 6-11. Restore by File Pop-up Window. 6-15
Figure 6-12. File Upload Dialog Pop-up Window. 6-15
Figure 6-13. Updated Restore by File Pop-up Window. 6-15
Figure 6-14. Restoration Warning Pop-up Window. 6-16
Figure 6-15. Restoration Warning Pop-up Window. 6-16
Figure 6-16. Delete Confirmation Pop-up Window. 6-17
Figure 6-17. Automatic Snapshot Configuration Screen. 6-17
Figure 6-18. Automatic Snapshot Configuration Screen (cont). 6-18
Figure 6-19. System Management Screen Selection 6-19
Figure 6-20. System Management Screen - Installed Tab Display. 6-19
Figure 6-21. System Management Screen HA Status Information 6-20
Figure 6-22. SSH Connection Profile Pop-up Window. 6-20
Figure 6-23. SSH Password Authentication Pop-up Window. 6-21
Figure 6-24. Active SSH Communications Session. 6-21
Figure 6-25. Shutdown Confirmation Pop-up Window. 6-22
Figure 6-26. Successful Shutdown Notification Pop-up Window. 6-22
Figure 6-27. Reboot Confirmation Pop-up Window. 6-22
Figure 6-28. Successful Reboot Notification Pop-up Window. 6-23
Figure 6-29. Restart Application Confirmation Pop-up Window. 6-23
Figure 6-30. Successful Restart Notification Pop-up Window. 6-23
Figure 6-31. System Management Display. 6-24
Figure 6-32. E-SBC Device Configuration Window 6-24
Figure 6-33. Edit Device Pop-up Window 6-25
Figure 6-34. Delete Confirmation Pop-up Window. 6-26
Figure 6-35. System Management Updates Screen 6-26
Figure 6-36. Advanced Options Function 6-27
Figure 6-37. Advanced Options: Subsystem Logs Display (E-SBC View). 6-27
Figure 6-38. Advanced Options: Subsystem Logs Display (EMS View). 6-27
Figure 6-39. Selecting an E-SBC Security Device. 6-28
Figure 6-40. CDR Listing Tab Display. 6-28
Figure 6-41. CDR Support Definition in Application Rules 6-29
Figure 6-42. Open CDR Dialog Pop-up Window. 6-29
Figure 6-43. Selecting a Program to View the CDR File. 6-29
Figure 6-44. CDR File Display Example 6-30
Figure 6-45. Feature Control Tab Display. 6-31
Figure 6-46. SIP Options Tab Display. 6-32
Figure 6-47. Port Ranges Tab Display 6-33
Figure 6-48. System Management Installed Tab 6-34
Figure 6-49. Edit Device Configuration Pop-up Window 6-35
Figure 6-50. HA Pairs Tab 6-35
Figure 6-51. Selecting the RADIUS Authentication Function 6-36
Figure 6-52. RADIUS Tab Display. 6-37

Figure 6-53. Add RADIUS Server Pop-up Window..... 6-37
Figure 6-54. Updated RADIUS Tab Display..... 6-38
Figure 6-55. Edit RADIUS Server Pop-up Window..... 6-39
Figure 6-56. Delete Confirmation Pop-up Window..... 6-39
Figure 6-57. Updated RADIUS Server Tab Display..... 6-40
Figure 6-58 Interface Configuration Screen..... 6-42
Figure 6-59 Selecting the Signaling Forking Function..... 6-42
Figure 6-60 Selecting Signaling Forking Screen..... 6-42
Figure 6-61 Add Forking Profile Screen..... 6-43
Figure 6-62 Signaling Forking Profile Information Screen..... 6-44
Figure 6-63. SNMP v1/v2 Tab Display..... 6-44
Figure 6-64. Add SNMP Community Pop-up Window..... 6-45
Figure 6-65. Updated SNMP v1/v2 Display..... 6-45
Figure 6-66. Edit SNMP Community Pop-up Window..... 6-46
Figure 6-67. Updated SNMP v1/v2 Tab Display..... 6-46
Figure 6-68. Delete Confirmation Pop-up Window..... 6-46
Figure 6-69. Add SNMP User Pop-up Window..... 6-47
Figure 6-70. Updated SNMP v3 Display..... 6-48
Figure 6-71. Edit SNMP User Pop-up Window..... 6-48
Figure 6-72. Delete Confirmation Pop-up Window..... 6-49
Figure 6-73. Routing Profile Screen..... 6-50
Figure 6-74. Add Routing Profile Pop-up Window..... 6-50
Figure 6-75. Add Routing Profile: Next Hop Routing Pop-up Window..... 6-50
Figure 6-76. Updated Routing Profile Screen..... 6-51
Figure 6-77. Selecting an Existing Routing Profile..... 6-52
Figure 6-78. Clone Profile Pop-up Window..... 6-52
Figure 6-79. Updated Routing Profile Screen..... 6-52
Figure 6-80. Selecting the Routing Function..... 6-53
Figure 6-81. Updated Routing Profile Display..... 6-54
Figure 6-82. Edit Routing Rule Pop-up Window..... 6-54
Figure 6-83. Delete Confirmation Pop-up Window..... 6-55
Figure 6-84. Selecting a New Order of Precedence for Existing Routing Rules..... 6-55
Figure 6-85. Reordered Routing Rules..... 6-56
Figure 6-86. Selecting a Routing Profile..... 6-56
Figure 6-87. Rename Profile Pop-up Window..... 6-57
Figure 6-88. Selecting the Routing Function..... 6-57
Figure 6-89. Delete Confirmation Pop-up Window..... 6-57
Figure 6-90. Selecting the Syslog Management Function..... 6-58
Figure 6-91. Syslog Management Display..... 6-59
Figure 6-92. Selecting Log Collection Parameters..... 6-59
Figure 6-93. Selecting the Signaling Interface Function..... 6-60
Figure 6-94. Signaling Interface Display..... 6-60
Figure 6-95. Selecting an E-SBC Device..... 6-60
Figure 6-96. Signaling Interface Display..... 6-60
Figure 6-97. Add Signaling Interface Pop-up Window..... 6-61
Figure 6-98. Updated Signaling Interface Display..... 6-62
Figure 6-99. Edit Signaling Interface Pop-up Window..... 6-62
Figure 6-100. Delete Confirmation Pop-up Window..... 6-62
Figure 6-101. Selecting the Media Interface Function..... 6-64
Figure 6-102. Media Interface Display..... 6-64
Figure 6-103. Selecting an E-SBC Device..... 6-64
Figure 6-104. Media Interface Display..... 6-65
Figure 6-105. Add Media Interface Pop-up Window..... 6-65
Figure 6-106. Updated Media Interface Display..... 6-66
Figure 6-107. Edit Media Interface Pop-up Window..... 6-66
Figure 6-108. Delete Confirmation Pop-up Window..... 6-66

Chapter 7. Security Configuration

Figure 7 - 1. Selecting the DoS/DDoS Function 7-2
Figure 7 - 2. DoS Settings Display. 7-3
Figure 7-3. Edit Call Walk DoS Pop-up Window. 7-4
Figure 7-4. Domain DoS Display. 7-5
Figure 7-5. Selecting a Domain DoS Profile. 7-5
Figure 7-6. Add Domain DoS Pop-up Window. 7-6
Figure 7-7. Add Server Configuration Profile - Advanced Pop-up Window. 7-6
Figure 7-8. Updated Domain DoS Display. 7-6
Figure 7-9. Clone Domain DoS Profile. 7-7
Figure 7-10. Updated Domain DoS Display. 7-7
Figure 7-11. Rename Domain DoS Profile. 7-8
Figure 7-12. Updated Domain DoS Display. 7-8
Figure 7-13. Edit Domain DoS Pop-up Window. 7-9
Figure 7-14. Delete Confirmation Pop-up Window. 7-9
Figure 7-15. Selecting an E-SBC Device. 7-10
Figure 7-16. Selecting DoS Learning Time Parameters. 7-10
Figure 7-17. Selecting the Scrubber Function 7-11
Figure 7-18. Scrubber Display. 7-12
Figure 7-19. Install Scrubber Package Pop-up Window. 7-12
Figure 7-20. Delete Confirmation Pop-up Window. 7-13
Figure 7-21. Selecting the Topology Hiding Function 7-14
Figure 7-22. Topology Hiding Display. 7-14
Figure 7-23. Topology Hiding Profile Screen 1 7-15
Figure 7-24. Topology Hiding Profile Screen 2 7-15
Figure 7-25. Topology Hiding Profile Header Parameters 7-15
Figure 7-26. Topology Hiding Profile Screen 2 Criteria Parameters 7-16
Figure 7-27. Topology Hiding Profile Screen 2 Replace Action 7-16
Figure 7-28. Topology Hiding Profile Screen 7-16
Figure 7-29. Edit Topology Hiding Profile Screen 1 7-17
Figure 7-30. Edit Topology Hiding Profile Screen 2 7-17
Figure 7-31. Edit Topology Hiding Profile Screen 3 7-18
Figure 7-32. Updated Topology Hiding Profile Display 7-18
Figure 7-33. Edit Topology Hiding Profile Screen 7-19
Figure 7-34. Clone Profile Pop-up Window. 7-20
Figure 7-35. Updated Topology Hiding Display. 7-20
Figure 7-36. Rename Profile Pop-up Window 7-21
Figure 7-37. Updated Topology Hiding Display. 7-21
Figure 7-38. Topology Hiding Headers. 7-22
Figure 7-39. Topology Hiding Examples for Request-Line Header 7-24
Figure 7-40. Topology Hiding Examples for From Header 7-25
Figure 7-41. Topology Hiding Examples for To Header 7-26
Figure 7-42. Topology Hiding Examples for Record-Route Header 7-27
Figure 7-43. Topology Hiding Examples for Via Header 7-28
Figure 7-44. Topology Hiding Examples for SDP Header 7-28

Chapter 8. Network Configuration

Figure 8 - 1. Server Configuration Display. 8-1
Figure 8-2. Add Server Configuration Pop-up Window. 8-2
Figure 8-3. Add Server Configuration Profile - General Pop-up Window. 8-2
Figure 8-4. Add Server Configuration Profile - Authentication Pop-up Window. 8-3
Figure 8-5. Add Server Configuration Profile - Heartbeat Pop-up Window. 8-4

Figure 8-6. Add Server Configuration Profile - Advanced Pop-up Screen 8-5
Figure 8-7. Updated Server Configuration Display. 8-6
Figure 8-8. Server Configuration Parameter Tabs. 8-6
Figure 8-9. Server Configuration Profile – Advanced Edit Pop-up Window. 8-7
Figure 8-10. Enabling DoS Protection. 8-7
Figure 8-11. Add Whitelist URI Pop-up Window. 8-8
Figure 8-12. Updated DoS Whitelist Display. 8-8
Figure 8-13. Delete Confirmation Pop-up Window. 8-8
Figure 8-14. Updated DoS Whitelist Display. 8-9
Figure 8-15. Selecting the DoS Protection Parameters Tab. 8-9
Figure 8-16. Edit Server DoS Pop-up Window. 8-10
Figure 8-17. Selecting a SIP Configuration Profile. 8-10
Figure 8-18. Add Server Configuration Profile Pop-up Window. 8-10
Figure 8-19. Updated Server Configuration Display. 8-11
Figure 8-20. Rename Server Configuration Profile Pop-up Window. 8-11
Figure 8-21. Updated Server Configuration Display. 8-11
Figure 8-22. Delete Confirmation Pop-up Window. 8-12
Figure 8-23. Updated Server Configuration Display. 8-12
Figure 8-24. Interworking Display 8-13
Figure 8-25. Add Interworking Profile Pop-up Window. 8-14
Figure 8-26. Add Interworking Profile - General Pop-up Window. 8-15
Figure 8-27. Add Interworking Profile - Privacy Pop-up Window. 8-16
Figure 8-28. Add Interworking Profile – SIP Timers Pop-up Window. 8-17
Figure 8-29. Add Interworking Profile – Advanced Settings Pop-up Window. 8-18
Figure 8-30. Updated Server Configuration Display. 8-19
Figure 8-31. Selecting an Interworking Profile. 8-20
Figure 8-32. Edit Profile Pop-up Window. 8-20
Figure 8-33. Editing Profile Pop-up Window. 8-21
Figure 8-34. Add Regex Expression Pop-up Window. 8-22
Figure 8-35. Updated URI Manipulation Display 8-23
Figure 8-36. Edit Regex Pop-up Window. 8-23
Figure 8-37. Delete Confirmation Pop-up Window. 8-24
Figure 8-38. Add Parameter Pop-up Window 8-24
Figure 8-39. Updated Header Manipulation Display. 8-25
Figure 8-40. Edit Parameter Pop-up Window. 8-25
Figure 8-41. Updated Header Manipulation Parameters Display. 8-25
Figure 8-42. Delete Confirmation Pop-up Window. 8-26
Figure 8-43. Clone Profile Pop-up Window. 8-26
Figure 8-44. Updated interworking Display. 8-27
Figure 8-45. Rename Profile Pop-up Window. 8-27
Figure 8-46. Updated Interworking Display. 8-27
Figure 8-47. Delete Confirmation Pop-up Window. 8-28
Figure 8-48. Device Specific Settings - Network Management Selection 8-29
Figure 8-49. Network Management Display 8-29
Figure 8-50. Add IP Information Line 8-30
Figure 8-51. Information Fields Completed 8-30
Figure 8-52. Confirmation Pop-up Window. 8-30
Figure 8-53. Delete Confirmation Pop-up Window. 8-32
Figure 8-54. Toggling the Administrative State of an Interface Configuration. 8-33
Figure 8-55. TLS Management Certificates Screen. 8-34
Figure 8-56. Install Certificate Pop-up screen. 8-35
Figure 8-57. Install CA Certificate Pop-up screen. 8-36
Figure 8-58. Install Certificate Revocation List Pop-up screen. 8-37
Figure 8-59. TLS Management Certificates Screen. 8-37
Figure 8-60. TLS Management Generate CSR Screen. 8-38
Figure 8-61. Sample Completed TLS Management Generate CSR Screen. 8-39

Figure 8-62. Sample CSR Display 8-40
Figure 8-63. TLS Client Profiles Screen. 8-40
Figure 8-64. New TLS Client Profile Pop-up Screen. 8-41
Figure 8-65. Updated Client Profiles Screen. 8-43
Figure 8-66. Edit TLS Client Profile Pop-up Window. 8-44
Figure 8-67. Delete Confirmation Pop-up Window. 8-45
Figure 8-68. Server Profiles Screen. 8-45
Figure 8-69. TLS Server Profile Pop-up Window. 8-46
Figure 8-70. Edit TLS Server Profile Pop-up Window. 8-48
Figure 8-71. Delete Confirmation Pop-up Window. 8-49

Chapter 9. System Monitoring

Figure 9 - 1. E-SBC Control Center - Welcome Screen. 9-1
Figure 9-2. Current System Alarms Notifications. 9-2
Figure 9-3. Alarms Screen. 9-3
Figure 9-4. E-SBC Device-specific Alarms Screen. 9-3
Figure 9-5. Alarms Screen Navigation Buttons. 9-4
Figure 9-6. Delete Confirmation Pop-up Window. 9-4
Figure 9-7. Incidents Screen. 9-5
Figure 9-8. Statistics Screen: Summary Tab Display. 9-6
Figure 9-9. Syslog Viewer. 9-7
Figure 9-10. Example of Syslog Report Output. 9-8
Figure 9-11. Diagnostics Display 9-9
Figure 9-12. Terminated Diagnostic Display. 9-9
Figure 9-13. Users Screen 9-10
Figure 9-14. Selecting the Trace Settings Function 9-11
Figure 9-15. Selecting a E-SBC Device and Packet Trace Tab. 9-11
Figure 9-16. Add Packet Trace Pop-up Window 9-11
Figure 9-17. Sample Updated Packet Trace Display. 9-12
Figure 9-18. Edit Trace Pop-up Window. 9-13
Figure 9-19. Deleting an Existing Packet Trace Profile 9-14
Figure 9-20. Delete Confirmation Pop-up Window. 9-14
Figure 9-21. Logs Button. 9-14
Figure 9-22. Logs Viewer Screen. 9-15
Figure 9-23. Call Trace Logs Viewer Display Example. 9-15
Figure 9-24. Call Trace – More Information. 9-16
Figure 9-25. Call Trace – Details Pop-Up Screen. 9-16
Figure 9-26. Add Capture Profile Pop-up Window. 9-17
Figure 9-27. Edit Trace Pop-up Window. 9-18
Figure 9-28. Delete Confirmation Pop-up Window. 9-18
Figure 9-29. SSH Command String Example 9-19
Figure 9-30. System Configuration Screen 9-19
Figure 9-31. E-SBC Welcome Screen 9-20
Figure 9-32. Navigating to the syslog/ipcs Directory 9-20
Figure 9-33. VI Editor Screen Display of an octeon.log Log File 9-21
Figure 9-34. Packet Capture Configuration Pop-Up Screen 9-22
Figure 9-35. Packet Capture Information Pop-Up Screen 9-22
Figure 9-36. File Download Pop-Up Screen 9-23
Figure 9-37. Save As Pop-Up Screen 9-23
Figure 9-38. Opening the Capture File 9-24
Figure 9-39. Sample Capture File Display 9-24
Figure 9-40. Audit Logs Menu Option 9-25
Figure 9-41. Audit Log Viewer 9-25
Figure 9-42. Selecting a Log Line 9-26

Figure 9-43. Audit Log Details 9-26

Chapter 10. Command Line Interface (CLI)

Figure 10-1 Instance Commands Example 10-4
Figure 10-2 SSH Login to clipcs 10-5
Figure 10-3. clipcs Password Prompt. 10-5
Figure 10-4. Top-level clipcs Prompt. 10-6
Figure 10-5. Super User Password Prompt. 10-6
Figure 10-6. Super User Command Line Prompt. 10-7
Figure 10-7. clipcs Command Line 10-7
Figure 10-8. Connecting a Terminal Device to the Sipera E-SBC EMS. 10-8
Figure 10-9. Connecting a Terminal Device to the E-SBC 1U. 10-9
Figure 10-10. Console Screen. 10-10

Chapter 11. Configuration Workflows for SIP Trunking

Figure 11- 1 SIP Trunking Diagram 11-1
Figure 11-2 Selecting the Routing Function 11-3
Figure 11-3 Add Routing Profile Pop-up Screen 1 11-3
Figure 11-4 Add Routing Profile Pop-up Screen 2 11-3
Figure 11-5 Routing Profile Screen 11-4
Figure 11-6 Add Routing Profile Pop-up Screen 1 11-4
Figure 11-7 Add Routing Profile Pop-up Screen 2 11-5
Figure 11-8 Routing Profile Screen 11-5
Figure 11-9 Selecting the Topology Hiding Function 11-6
Figure 11-10 Add Topology Hiding Profile Pop-up Screen 1 11-6
Figure 11-11 Add Topology Hiding Profile Pop-up Screen 2 11-7
Figure 11-12. Topology Hiding Profile Header Parameters 11-7
Figure 11-13. Topology Hiding Profile Screen 2 Criteria Parameters 11-7
Figure 11-14. Topology Hiding Profile Screen 2 Replace Action 11-8
Figure 11-15 Selecting the Topology Hiding Function 11-8
Figure 11-16 Add Topology Hiding Profile Pop-up Screen 1 11-8
Figure 11-17 Add Topology Hiding Profile Pop-up Screen 2 11-9
Figure 11-18. Topology Hiding Profile Header Parameters 11-9
Figure 11-19. Topology Hiding Profile Screen 2 Criteria Parameters 11-9
Figure 11-20. Topology Hiding Profile Screen 2 Replace Action 11-10
Figure 11-21 Selecting the Server Interworking Function 11-11
Figure 11-22. Global Profiles Server Interworking Screen 11-11
Figure 11-23 Selecting the Server Configuration Function 11-12
Figure 11-24 Add Server Configuration Profile Pop-up Screen 1 11-12
Figure 11-25 Add Server Configuration Profile Pop-up Screen 2 11-12
Figure 11-26 Add Server Configuration Profile – Authentication Pop-up Screen 11-13
Figure 11-27 Add Server Configuration Profile – Heartbeat Pop-up Screen 11-13
Figure 11-28 Add Server Configuration Profile – Advanced Pop-up Screen 11-14
Figure 11-29 Add Server Configuration Profile – Advanced Pop-up Screen (cont) 11-14
Figure 11-30 Server Configuration Profile Screen 11-15
Figure 11-31 Add Server Configuration Profile Pop-up Screen 1 11-15
Figure 11-32 Add Server Configuration Profile Pop-up Screen 2 11-16
Figure 11-33 Add Server Configuration Profile Authentication Pop-up Screen 11-16
Figure 11-34 Add Server Configuration Profile Heartbeat Pop-up Screen 11-17
Figure 11-35 Add Server Configuration Profile Advanced Pop-up Screen 11-17
Figure 11-36 Add Server Configuration Profile Screen 11-18
Figure 11-37 Selecting the Signaling Interface Function 11-18

Figure 11-38 Add Signaling Interface Pop-up Screen 1 11-19
Figure 11-39 Add Signaling Interface Pop-up Screen 2 11-20
Figure 11-40 Signaling Interface Screen..... 11-20
Figure 11-41 Selecting the Media Interface Function..... 11-21
Figure 11-42 Add Media Interface Pop-up Screen 1 11-21
Figure 11-43 Add Media Interface Pop-up Screen 2 11-22
Figure 11-44 Media Interface Screen..... 11-22
Figure 11-45 Selecting the End Point Flows Function 11-23
Figure 11-46 End Point Server Flows Information Screen 11-23
Figure 11-47 Add Flow Pop-up Screen 11-24
Figure 11-48 Updated Add Flow Pop-up Screen..... 11-25
Figure 11-49 Add Flow Pop-up Screen 11-26
Figure 11-50 Server Flows Information Screen..... 11-27
Figure 11-51. Selecting the Server Configuration Function 11-28
Figure 11-52 Server Configuration Advanced Tab Screen..... 11-28
Figure 11-53 Server Configuration Advanced Edit Pop-up Screen 11-29
Figure 11-54. Selecting the Server Interworking Function..... 11-29
Figure 11-55. Server Interworking Advanced Tab 11-30
Figure 11-56. Server Interworking Advanced Edit Window 11-30
Figure 11-57. Server Interworking General Tab..... 11-31
Figure 11-58. Server Interworking General Edit Window..... 11-31

Chapter 12. Signaling Manipulation

Figure 12- 1 Built-In Variables and Arrays - %HEADERS[] Variable 12-7
Figure 12-2 Built-In Variables and Arrays - %SDP[] Variable 12-8
Figure 12-3 Packet Path..... 12-11
Figure 12-4 SigMa Editor Screen for Signaling Manipulation 12-26
Figure 12-5 SigMa Process Flowchart..... 12-27
Figure 12-6 Server Configuration Screen 12-28
Figure 12-7 Add Server Configuration Profile Screen 1..... 12-28
Figure 12-8 Add Server Configuration Profile General Screen 2 12-29
Figure 12-9 Add Server Configuration Profile Authentication Screen 3 12-30
Figure 12-10 Add Server Configuration Profile Heartbeat Screen 4 12-30
Figure 12-11 Add Server Configuration Profile Advanced Screen 5..... 12-31
Figure 12-12 Updated Server Configuration Screen..... 12-31
Figure 12-13 Sever Configuration Advanced Tab Button 12-32
Figure 12-14 Server Configuration Advanced Tab Screen..... 12-32
Figure 12-15 Server Configuration Advanced Tab Edit Screen 12-32

Appendix E. UC-Sec SNMP Details

Figure E - 1 MIB Tree Structure.....E-2

Tables

Chapter 2. Getting Started

Table 2-1. Toolbar Item Descriptions. 2-6
Table 2-2. Global Parameters Feature Descriptions..... 2-10
Table 2-3. Global Profiles Feature Descriptions 2-11
Table 2-4. Domain Policy Feature Descriptions. 2-13
Table 2-5. Device Specific Settings Feature Descriptions. 2-15
Table 2-6. Troubleshooting Feature Descriptions. 2-16
Table 2-7. TLS Management Feature Descriptions. 2-17
Table 2-8. Screen Icon Descriptions. 2-22

Chapter 3. Managing Administrative User Account

Table 3-1. Add New Administrative User Pop-up Window Field Descriptions. 3-3
Table 3-2. Administration Parameters Tab Display Field Descriptions..... 3-4
Table 3-3. Installation Wizard Field Descriptions – Installation Pop-Up Window 3-9

Chapter 4. Device Configuration

Table 4-1. Installation Wizard Field Descriptions - Window 1. 4-3
Table 4-2. Network Settings Pop-up Window Field Descriptions. 4-5
Table 4- 3. EMS Upgrade – Non Service Affecting 4-11

Chapter 5. Domain Policy Administration

Table 5-1 Add Application Rule Pop-up Window Field Descriptions..... 5-12
Table 5-2 Add Border Rule – Topology Hiding and Learning Mode Pop-up Window Field Descriptions. 5-18
Table 5-3 Add Media Rule – Media NAT Pop-up Window Field Descriptions. 5-23
Table 5-4 Add Media Rule - Codec Prioritization Pop-up Window Field Descriptions. 5-24
Table 5-5 Add Media Rule – Media Silencing Pop-up Window Field Descriptions. 5-27
Table 5-6 Add Media Rule – QoS Reporting and Marking Pop-up Window Field Descriptions. 5-28
Table 5-7 Turing Test Parameter Descriptions. 5-38
Table 5-8 Add Security Rule: Fingerprint Profile Pop-up Window Field Descriptions. 5-46
Table 5-9 Add Security Rule: Scrubber Profile Pop-up Window Field Descriptions. 5-47
Table 5-10 Add Security Rule: Domain DoS Pop-up Window Field Descriptions. 5-48
Table 5-11 Add Signaling Rule Pop-up Window Field Descriptions. 5-55
Table 5-12 Add Signaling Rule: QoS Pop-up Window Field Descriptions. 5-58
Table 5-13 Add Request Control Pop-up Window Field Descriptions. 5-61
Table 5-14 Add Response Control Pop-up Window Field Descriptions. 5-63
Table 5-15. Add Header Control Pop-up Window Field Descriptions. 5-65
Table 5-16 Add Header Control Pop-up Window Field Descriptions. 5-67
Table 5-17 Add Time of Day Rule Pop-Up Window Field Descriptions. 5-73
Table 5-18 Add Policy Group Parameters Screen Field Descriptions. 5-80
Table 5-19 Add Policy Set Pop-up Window Field Descriptions..... 5-84
Table 5-20 Codec Prioritization Pop-up Window Field Descriptions..... 5-90
Table 5-21 Add Flow: Criteria Pop-up Window Field Descriptions. 5-96
Table 5-22 Add Flow Pop-up Window Field Descriptions..... 5-102
Table 5-23 Add URI Group Pop-up Window Field Descriptions. 5-109

Chapter 6. System Configuration

Table 6-1. Add Snapshot Server Pop-up Window Field Descriptions. 6-11
Table 6-2. SIP Options Tab Display Field Descriptions. 6-32
Table 6-3. Add RADIUS Server Pop-up Window Field Descriptions. 6-37
Table 6-4 Add Forking Profile Screen Field Descriptions. 6-44
Table 6-5. SNMP v3 Configuration: Add User Pop-up Window Field Descriptions. 6-48
Table 6-6. Add Routing Profile: Next Hop Routing Pop-up Window Field Descriptions. 6-52
Table 6-7. Add Signaling Interface Pop-up Window Field Descriptions. 6-61
Table 6-8. Add Media Interface Pop-up Window Field Descriptions 6-65

Chapter 7. Security Configuration

Table 7-1. DoS/DDoS Attack Type Descriptions. 7-3
Table 7-2. Topology Hiding Headers. 7-23

Chapter 8. Network Configuration

Table 8-1. Add Server Configuration Profile – General Pop-up Window Field Descriptions. ... 8-2
Table 8-2. Add Server Configuration Profile – Authentication Pop-up Window Field Descriptions. 8-3
Table 8-3. Add Server Configuration Profile – Heartbeat Pop-up Window Field Descriptions. 8-4
Table 8-4. Add Server Configuration Profile – Heartbeat Pop-up Window Field Descriptions. 8-5
Table 8-5. Add Interworking Profile – General Pop-up Window Field Descriptions. 8-16
Table 8-6. Add Interworking Profile – Privacy Pop-up Window Field Descriptions. 8-17
Table 8-7. Add Interworking Profile – SIP Timers Pop-up Window Field Descriptions. 8-18
Table 8-8. Add Interworking Profile – Advanced Settings Pop-up Window Field Descriptions. 8-18
Table 8-9. Add Regex Expression Pop-up Window Field Descriptions. 8-22
Table 8-10. Add Parameter Pop-up Window Field Descriptions. 8-24
Table 8-11. E-SBC Interface Addressing Field Descriptions. 8-31
Table 8-12. TLS Certificates Screen Field Descriptions. 8-34
Table 8-13. Install Certificate Pop-up Screen Field Descriptions. 8-35
Table 8-14. CA Certificate Screen Field Descriptions. 8-36
Table 8-15. Install CRL Screen Field Descriptions. 8-37
Table 8-16. TLS Management Generate CSR Screen Field Descriptions. 8-38
Table 8-17. TLS Client Profile Pop-up Screen Field Descriptions. 8-41
Table 8-18. New TLS Server Profile Pop-up Window Field Descriptions. 8-46

Chapter 9. System Monitoring

Table 9-1. Dashboard Alarm and Event Reporting Component Descriptions. 9-1
Table 9-2. Current Alarms Screen Field Descriptions. 9-3
Table 9-18. Add Packet Trace Pop-up Window Field Descriptions. 9-12
Table 9-19. Add Capture Profile Pop-up Window Field Descriptions. 9-17

Chapter 10. Command Line Interface (CLI)

Table 10-1. clipcs Commands Available at the Console Prompt. 10-1
Table 10-2. CLI (Top) Commands Available from the Instance Mode. 10-4

Chapter 12. Signaling Manipulation

Table 12-1 Where Clause Variables 12-2
Table 12-2 Session Variables..... 12-3
Table 12-3 Built-In Variables and Arrays - %HEADERS[] Variable 12-6
Table 12-4 Built-In Variables and Arrays - %SDP[] Variable 12-7
Table 12-5 Built-In Variables and Arrays - Other Variables 12-9
Table 12-6 Built-In Functions..... 12-9
Table 12-7 Hook Points 12-11
Table 12-8 SigMa Scripting Examples 12-12

Preface

The *E-SBC Administration Guide* describes how to use the E-SBC Control Center as an Element Management System (EMS) to configure, monitor, and control the security features provided by E-SBC security products deployed throughout Session Initiation Protocol (SIP) enterprise VoIP networks. It contains the information necessary to configure, provision, monitor, and administer E-SBC-specific security features, including unified communication policies, using the GUI interface. In addition, this manual describes how to access and use the EMS using the Command Line Interface (CLI).

Audience

This document is intended for network or VoIP administrators and other personnel who will administer and monitor the operation of the E-SBC security devices within their network. It is assumed that these individuals have an excellent working knowledge of IP network and telephony concepts and SIP protocol, as well as more specific expertise in VoIP-related security issues and call routing techniques. This guide will provide the information necessary to:

- Log-in to the E-SBC Control Center and provision administrator, group, and user accounts and permissions
- Configure device, system, security, and network parameters
- Configure and apply unified communication policies (also referred to as domain policies) to control inbound/outbound voice and media communications sessions
- Monitor the security status of the entire SIP-based VoIP network
- Manage the detection and prevention activities of all E-SBC security products deployed throughout the network
- Run various summary and detail security reports.

Notation Conventions

Certain notation conventions are used in this manual and described below:

Notice Icons

This manual uses the following notice icons.

Icon	Alerts you to…
Note	Important features, instructions, or additional relevant information.
Caution!	Risk of system damage, service and/or security interruption, or data loss.

Text Conventions

This manual uses the following notation conventions.

- **Boldface** emphasizes words in text such as screen names or commands that you type.
- *Italics* introduce or define new terms.
- `Monospace` represents information as it appears on a display screen or command syntax.

Revision Information

This manual describes how to use Revision 4.0.5 of the E-SBC Control Center security software and incorporates the following updates and additions that were made to the functionality of Release 4.0:

- **Office Communications Server (OCS) R2 / UC Security Support**
    - Instant Messaging (IM) Support
    - SIP Trunking Support

- **SIP 2-Factor (2-FA) Authentication Support**

    - Native SIP 2-FA Authentication ─ The user authenticates using a VoIP phone.
    - Web-Based SIP 2-FA Authentication ─ The user authenticates using a Web browser on a separate PC.

- **Secure Live Communications (SLiC)**
  (Sipera's secure mobile client solution)
    - Fingerprint Matching ─ Using SLiC's Fingerprint Matching feature, every message is checked for a client-specific signature to ensure that the user receives only messages from E-SBC.
    - Blacklisting ─ Using SLiC's Blacklisting feature, mobile users can maintain a list, cached on their mobile phone, of numbers that the user does not want to receive calls from.
    - TLS/Smart Card ─ SLiC's TLS/Smart Card feature enables mutual authentication by reading certificates present on a microSD memory card inserted in the user's mobile phone's microSD slot.
- **Security Enhancements**
    - RTP Injection Attack Detection/Prevention
- **Miscellaneous Feature Enhancements**
    - Statistical Enhancements
    - Packet Capture and CLI Troubleshooting Enhancements
    - Automatic Backup/Restore Snapshot Configuration

Manual Organization

This manual is divided into the following chapters and appendixes.

- Chapter 1, *Introduction*, provides a general overview of the Control Center, which is the GUI-accessible provisioning, monitoring, and control platform for all E-SBC security products.
- Chapter 2, *Getting Started*, explains how to log-in to the Control Center and navigate through its different screens and windows.
- Chapter 3, *Managing Administrative User Accounts*, explains how to create and manage Administrative user accounts (**Admin**, **Manager**, and **Supervisor**).
- Chapter 4, *Device Configuration,* explains how to provision E-SBC security devices which have been physically installed into the network.
- Chapter 5, *Domain Policy Administration*, describes how to define and configure unified communication (domain) policies to manage call flows (end-point and session) from and to the protected VoIP network.
- Chapter 6, *System Configuration*, explains how to configure various system-related E-SBC security features, such as RADIUS authentication, SNMP access, trace settings, and debugging options.
- Chapter 7, *Security Configuration*, explains how to configure specific security features such as protocol scrubbing, Denial-of-Service (DoS) attack responses, and Transport Layer Security (TLS).
- Chapter 8, *Network Configuration*, contains the procedures necessary to manage protected network elements as well as how to configure firewall network address translation traversal (FW/NATT) and virtual IP (VIP) addressing parameters.
- Chapter 9, *System Monitoring*, describes how to monitor the security of the VoIP network using the various Alarm, Incidents, Statistics, and Users screens.
- Chapter 10, *Command Line Interface*, describes how to directly access E-SBC security devices system using the Command Line Interface (CLI).
- Chapter 11, *Configuration Workflows for SIP Trunking,* provides detailed step-by-step procedures for installing E-SBC in various SIP trunking configurations.
- Chapter 12, Signaling Manipulation, provides an overview of Sipera's SIP signaling header manipulation feature and proprietary scripting language for the E-SBC product. This feature adds the ability to configure, add, change, and delete any of the headers and other information in a SIP message.
- Appendix A, *Acronyms and Abbreviations*, contains a list of all acronyms and abbreviations used throughout this document.
- Appendix B, *Glossary*, contains definitions for the industry and technology specific terms used throughout this document.
- Appendix C, *System Alarm List*, contains a description of system-generated events which trigger alarms.
- Appendix D, *GUI and Console Alarm List*, contains a description of the GUI and CLI-generated events which trigger alarms.

- Appendix E, *SNMP Details*, contains a description of the E-SBC Management Information Base (MIB) tree structure and content, which can be read by the Simple Network Management Protocol (SNMP).
- Appendix F, *Error Messages*, contains a list of E-SBC error messages to aid in troubleshooting.

Related Manuals

See the following Sipera manuals for more information.

- *UC-Sec 1U Installation Guide* (101-5224-405) contains instructions for physically installing the UC-Sec 1U security product and connecting it to a VoIP network.
- *UC-Sec™ 1U Maintenance Guide* (101-5303-405) describes how to maintain the UC-Sec™ 1U equipment chassis.
- *UC-Sec EMS Installation Guide* (100-5224-405) contains instructions for physically installing the Sipera EMS security product and connecting it to a VoIP network.
- *UC-Sec Release Notes* (010-5524-405) contains the final changes, additions, and deletions to the UC-Sec product release that were not available at the time of printing.

Ordering Manuals

To order manuals, contact Sipera Customer Support.

Main Phone:	(214) 206-3210
FAX:	(214) 206-3215
Support Phone:	(866) 861-3113
Support E-mail:	support@sipera.com
Address:	Sipera Systems, Inc. 1900 Firman Drive; Ste. 600 Richardson, TX 75081

You should also direct any questions about the ordering process to Sipera Customer Support.

How to Comment on this Manual

Sipera welcomes any corrections and suggestions for improving this manual. Please send any comments or trouble reports on this manual to Sipera Customer Support.

Phone:	(214) 206-3210
FAX:	(214) 206-3215
E-mail:	support@sipera.com
Address:	Sipera Systems, Inc. Customer Support 1900 Firman Drive; Ste. 600 Richardson, TX 75081

This page intentionally left blank.

Introduction 1

This document provides an overview of the E-SBC Enterprise Session Border Controller UC network security solution and how it can be administered using the ***E-SBC Control Center***. It primarily describes how to use the *Unified Communications Policies* (also referred to as *Domain Policies*) feature of the E-SBC to configure, apply, and manage security rule sets based upon the source and destination end-point and session call flows entering or exiting the enterprise. In addition, this document provides the information necessary to allow you to effectively monitor a SIP-based UC network security using the E-SBC Control Center and various incident and historical reports.

Note:	**Throughout this document, when referring to E-SBC devices, the terms *Primary* and *Secondary* are used interchangeably with the terms *Active* and *Stand-by*, respectively.**

E-SBC Overview

E-SBC security products (E-SBC 1U, E-SBC 2U, E-SBC 1UA, and E-SBC EMS) are true enterprise session border controllers (SBCs) not repackaged carrier SBCs that provide SIP trunk termination for 20 sessions to 10,000 sessions. Figure 1-1 illustrates the E-SBC solution.

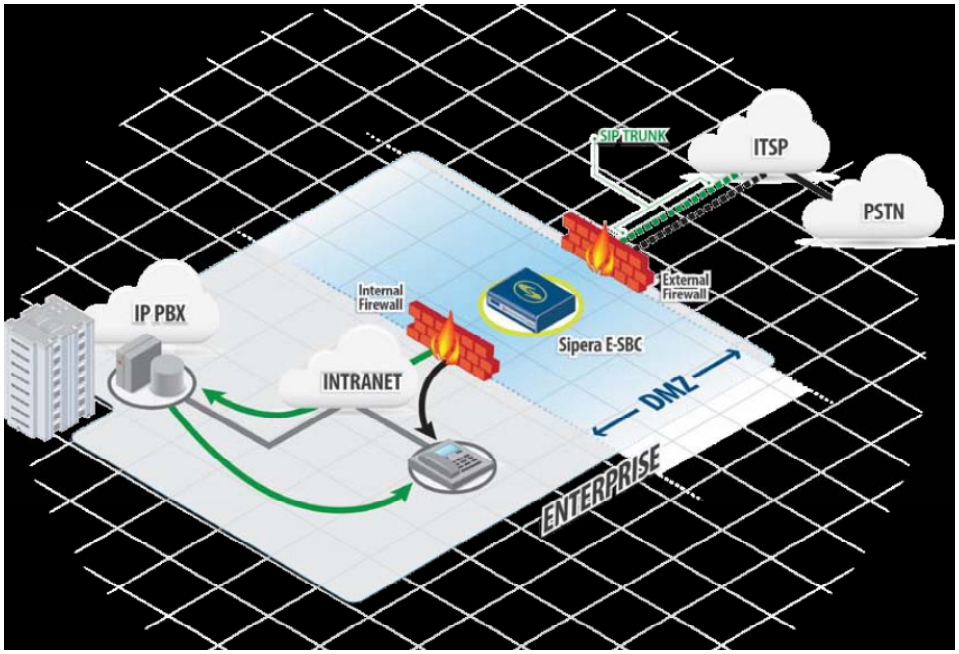


Figure 1-1 The E-SBC Enterprise Session Border Controller Solution.

E-SBC Overview

E-SBC products provide a lower-cost alternative to the more expensive Carrier SBCs, while at the same time providing an Enterprise SBC that is affordable, highly scalable, easy to install and manage plug-and-play solution for Enterprises and SMBs (Small to Medium Businesses).

Based on Sipera's extensive experience in SIP trunk deployments supporting hundreds of thousands of enterprise users, Sipera's E-SBC is the industry's first SBC to feature the unique SIP Trunk Integration Module (SIM), which dramatically simplifies the deployment of SIP trunks for any enterprise.

The STIM streamlines integration of SIP trunks into any of thousands of variations of enterprise SIP telephony environments, greatly reducing implementation timeframes. As a result, SIP trunk deployment in many standard configurations can occur in two hours or less.

The industry's only safe SIP trunk choice, Sipera's E-SBC offers:

- Industry standard SBC functionality with Sipera's industy-leading VoIP, SIP, and Unified Communications security expertise
- Capacity ranging from 20 to 10,000 concurrent sessions, including High-Availability configurations
- Upgrade options to comprehensive application-layer communications security; UC firewalling, archiving compliance, VoIP and UC proxying, teleworkers, Borderless UC, advanced endpoint security, and the industry's best protection against VoIP toll fraud and UC intrusion

Feature Descriptions

The following sections briefly describe the security features offered by E-SBC Rel. 4.0.5.

SIP Trunking

The *SIP Trunking* feature of E-SBC security devices allow SIP trunk-enabled enterprises to completely secure SIP connectivity over the Internet via SIP Trunking services obtained through an Internet Telephony Service Provider (ITSP).

SIP trunking ensures the privacy of all calls traversing the enterprise network, while maintaining a well defined demarcation point between the core and access network. In addition, the SIP trunking feature in E-SBC allows an enterprise to maintain granular control through well-defined domain policies securing customers' SIP implementations/servers from known SIP and Media vulnerabilities.

Because the E-SBC security device is deployed in the enterprise DMZ as a trusted host, all SIP signaling traffic destined for the enterprise is received by the external firewall and sent to the E-SBC device for processing, as shown in Figure 1-2 below.

If the signaling traffic is encrypted, the E-SBC device decrypts all TLS encrypted traffic and looks for anomalous behavior before forwarding the packets through the internal firewall to the appropriate IP PBX in the enterprise core to establish the requested call session.

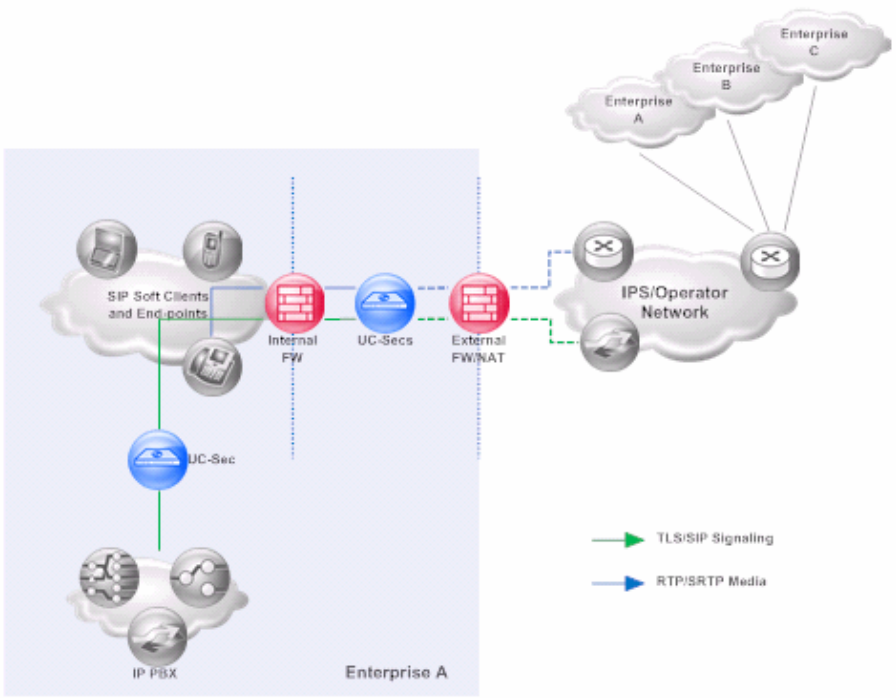


Figure 1-2. SIP Trunking.

Once a valid call session has been set-up, Real-Time Transport Protocol (RTP) or Secure Real-Time Transport Protocol (SRTP) media packets are allowed to flow through the external firewall to the E-SBC device in the DMZ. The E-SBC device then looks for anomalous behavior in the media before passing the RTP/SRTP stream on to the intended end-point.

High-Availability (EMS/E-SBC-1U/E-SBC-2U)

High-Availability (HA) support for both media and signaling ensures E-SBC security functionality is provided continuously, regardless of any hardware or software failures which may occur. Two E-SBC security devices are logically deployed as an 'HA pair', either in the enterprise DMZ or core, wherein one E-SBC device functions as an Active security device with the other functioning as a hot-standby back-up. HA pairs (EMS and E-SBC) can also be geographically dispersed, wherein each EMS or E-SBC device resides in a separate, physical facility.

Note: **HA Functionality requires GARP support on the connected network elements. In cases like Avaya Medpro and certain Cisco endpoints, which do not support GARP, it is necessary to introduce a GARP aware router/Switch between these elements and E-SBC for it to handle GARP packets sent from E-SBC.**

EMS

The *EMS Replication* feature gives an enterprise the option of deploying two Sipera EMS servers (*Active* and *Stand-by*) to ensure EMS high availability for uninterrupted network monitoring and control (Figure 1-3). These servers can only be co-located in the same facility (Figure 1-4).

EMS data is replicated on an iterative basis, determined by user-defined fields accessed from the EMS GUI interface.

Note: ***EMS Replication*** **does not support automatic takeover as it requires manual intervention by the operator.**

When an operator detects that the Active EMS is down, to effect a switch-over to the Stand-by, the operator must perform the following steps:

1. Login as root on the appropriate EMS.
2. Run the script **switchover.py** (on the *Active*) to effect a graceful switchover.
3. Run the script **takeover.py** (on the *Stand-by*) to allow the *Stand-by* to become the *Active*.

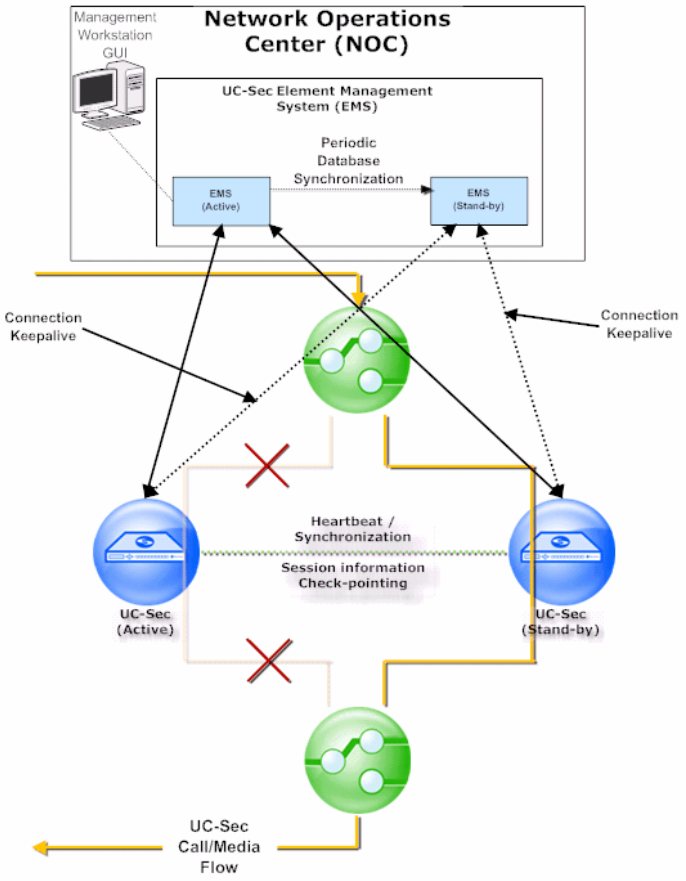


Figure 1-3. EMS High-Availability (HA).

E-SBC HA Pairs

E-SBC HA pairs can be deployed in an enterprise in a parallel mode configuration. In the parallel configuration (Figure 1-4), the signaling packets are routed only to the Active (primary) E-SBC security device which performs all data processing: the interface ports on the stand-by E-SBC device do not process any traffic. The Management interfaces on the E-SBC appliances have different IP addresses, but the signaling/media interfaces have the same IP address. Upon failover, the standby E-SBC advertises its new MAC as the L2 address for the common IP address. The E-SBC devices are synchronized together via the heart-beat on the dedicated interfaces, and both E-SBC devices are in continuous communication with the Sipera EMS.

When a failure is detected on the Active E-SBC device by the Sipera EMS, its network interface ports are automatically disabled while those of the stand-by E-SBC device are enabled. Failure detection and operational transfer occur without dropping packets or adding any significant amount of latency into the data paths. The EMS reports the change in status to the E-SBC Control Center for action by the system administrator.

E-SBC HA Configurations

There is one standard E-SBC HA configurations, illustrated in Figure 1-4 below, where the Active (primary) and Stand-by (secondary) E-SBC devices are co-located in the same general area.

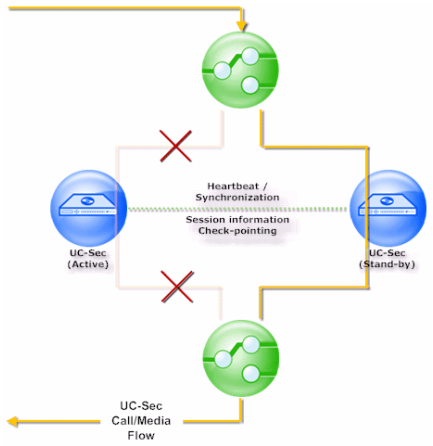


Figure 1-4. Typical E-SBC HA – Parallel Mode Topology (co-located).

E-SBC High Availability (HA) Configurations

The Standard High Availability (HA) configuration (devices co-located) is performed from the System Management screen on two devices that have already been added using the **Add Device** function (described in the section in Chapter 3 titled, "***Adding a E-SBC Device***") and listed with a ***Registered*** status in the management screen, as shown in Figure 1-5.

Note:	When a device is first added, its status is ***New*** and this status eventually changes to ***Registered*** once it is becomes known to the network.

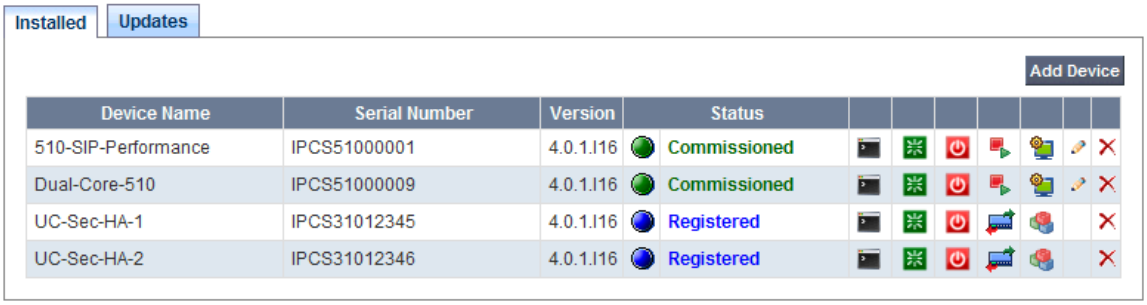


Figure 1-5. System Management Screen

The HA configuration procedure is done using the **Install Wizard** which is started by clicking on the **Install Device** icon located on the right-hand portion of the device information line in the System Management screen, as shown in Figure 1-6 below.

Note:	You must select the device information line for the device that will be configured as the "***Active***" (primary) device in the HA configuration.

Using the **Install Wizard** procedure (described in the section in Chapter 4 titled, "***Installing a E-SBC Device***") you will open a configuration screen for the "***Active***" (primary) device and select the "***Stand-By***" (secondary) device from a drop-down list in the screen to associate the two devices.

Note:	The device you choose for the ***Stand-By*** device must be listed in the System Management screen to be available in the drop-down selection list. If not listed, use the **Add Device** button (see the section in Chapter 3 titled, "**Adding a E-SBC Device**") to add it.

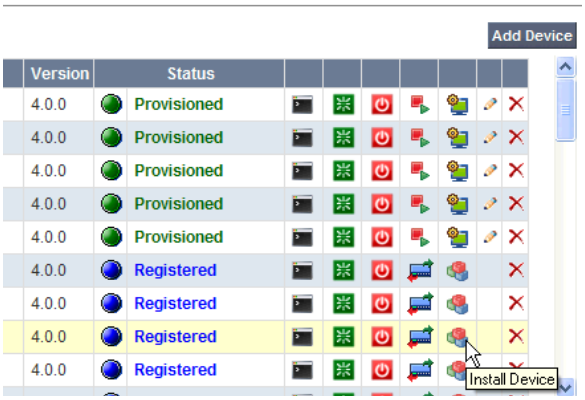


Figure 1-6. Install Device Icon

Note:	Refer to Chapter 4, "***Device Configuration***," for instructions on using the **Install Wizard** to perform Standard E-SBC configurations as well as Standard HA configurations and Geographically-Dispersed HA configurations and deployments.

Designated Active Configuration

One of the nodes in the HA pair can be configured to be the designated "***Active***" (primary) node. In the configuration screens, this is done by selecting the "**Is Active**" checkbox or "**Designate Active**" checkbox. This is an additional configuration on top of the Parallel HA configuration, which can be configured in the HA-related screens at the time of installation. When a node is designated ***Active***, it means that when there is no link between the HA nodes, the designated ***Active*** node will automatically become ***Active*** irrespective of its previous status.

When a node is a Designated Primary, it means that when there is no link between the HA nodes, the Designated Primary node will automatically become Primary irrespective of its previous status.

Unified Communications (UC) Intrusion Protection

Unlike traditional intrusion prevention systems (IPS), which monitor network traffic to gather and analyze information from various parts of that network to identify possible security breaches for subsequent prevention or mitigation, E-SBC security products are uniquely engineered not only to detect any anomalous event – including day zero attacks – but also prevent virtually any type of intrusion (attack from outside the enterprise) and misuse (attack from within the enterprise). This is due to the unparalleled flexibility and fine-grain tuning allowed when establishing Unified Communications rule sets by the network security administrator. The functionality provided by the E-SBC IPS security feature includes:

- **Flood and Fuzzing Protection** – Unequalled protection from volume-based Denial-of-Service (DoS) and malformed message ('fuzzed') attacks. Customized protocol scrubbing rules detect and remove malformed messages which may crash call servers or other critical network components, or make other portions of the communications infrastructure vulnerable because of degraded performance of critical Unified Communications systems components (such as servers and end-points).
- **Media Anomaly Prevention** – Selectively enables the media traffic and enforces rules on the type of traffic carried, based on the negotiated signaling and other configured policies (for example prevent video or prevent modem/FAX).
- **Spoofing Prevention** – Various validation techniques are applied to detect and prevent spoofing, including the use of end-point 'fingerprints' for different message fields to trigger other validations and verifications.
- **Stealth Attack Prevention** – Based on the learned call behavior patterns of subscriber end-points, E-SBC security products can detect any nuisance and annoying calls to a particular destination or user and selectively block only those subscribers from whom those calls originate.
- **Reconnaissance Prevention** – E-SBC security products detect and block application layer scan reports and block the attackers which originate them.

E-SBC Hardening

System level Layer 3/Layer 4 security features include IPTable firewall rules to provide restrictions on INBOUND traffic (effective after content filtering processing for data traffic) to protect E-SBC from IP/ICMP/TCP level attacks.

Note:	OUTBOUND traffic is not restricted.

General Protection against Layer 3/Layer 4 Floods and Port Scans

ICMP Flood Prevention

Once an ICMP flood from a host is detected, all further requests from that host are blocked for a specified period of time.

Port Scan Blocking

Once a port scan from a host is detected, all further requests from that host are blocked for a specified period of time.

Management Interface Restrictions on Ports That Can Be Opened

Only selected ports are allowed on the management interface:

- SSH TCP-222
- HTTPS TCP-443
- DNS TCP/UDP-53
- OpenVPN UDP-1194
- Syslog TCP/UDP-514
- NTP UDP-123
- SNMP UDP-161/162

All other TCP/UDP traffic is blocked on the management interface.

Only a specified number of TCP packets are allowed from a host within a specified time frame, irrespective of TCP ports. Regarding the SSH port, the following rules are defined:

- Only a specified number of connections from a host are allowed within a specified time frame.
- Only a specified number of connection requests are responded with ICMP-unreachable
- Further connection requests are dropped until new connection requests stop for a specified period of time.

For other TCP ports, TCP signaling level flooding control is applied.

Data Interface Restrictions

- General protection is provided on all data interfaces
- TCP signaling level flooding control rules are applied dynamically on application-specified listening IP and listening port.

TCP Signaling Level Flood Control

Only a specified number of requests are allowed in a specified time period for each of the following request types:

- TCP SYN
- FIN
- RST

System-Wide Security Settings

System-wide security settings are supported across the entire Sipera product line. Each product (i.e., E-SBC 1U, E-SBC 2U, and E-SBC 1UA) has the following protection types:

General Protection
Management Interface Restrictions
Data Interface Restrictions

Note:	For all products, the management interface is dynamically detected from the system configuration. For E-SBC 2U, there are no restrictions on the internal Ethernet interface (**ethint**) and external Ethernet M1 interface (**ethext**) on the (**Com Express**) co-processor board in the E-SBC box. To enable E-SBC 1U HA, TCP 1950 ports are allowed bi-directionally on the data interface. E-SBC 2U HA does not require any extra rules to enable HA traffic.

Attack Protection

To ensure the integrity of all real-time IP applications, not just UC, E-SBC security products comprehensively perform each of the three functions that are critical to maintaining the highest level of communications network security, reliability, and availability; these are *monitoring*, *detection*, and *protection.*

Monitoring

Each E-SBC security product provides complete network security monitoring and management capabilities that encompass each aspect of the UC network; including all media gateways, call servers, voice mail (VM) and applications servers. In addition, its monitoring and management capabilities provide a cascaded, multi-layered detection, mitigation, and reporting system that provides real-time information based upon user-definable event thresholds. This system supports a detailed graphical user interface (GUI) called the *E-SBC Control Center*, and others. The E-SBC Control Center can be installed on and run from any E-SBC security device or it can be installed on a separate server platform and used as a stand-alone Element Management System (EMS) that monitors and coordinates the security activities of all E-SBC security devices installed in a network.

Note:	Both the EMS and E-SBC can be installed in one box. However, as your network grows and you require more than one E-SBC, at that time it recommended that your EMS be installed on a dedicated platform.

Detection

First, the detection capability of the E-SBC solution utilizes a host of dynamic and adaptive algorithms to detect any anomalies in the learned caller behavior that are based upon user-definable Time-of-Day (ToD) and Day-of-Week (DoW) criteria. These are

flexible enough to accommodate special circumstances such as weekends, holidays, and other user-specified time periods.
The detection capability is also able to collect and correlate multiple events and activities from different nodes and end-points in the network to accurately detect attacks which otherwise might have escaped unnoticed if reported only by a single point in the network. Finally, the detection capability of the E-SBC solution can validate the source of a suspected malicious call or attack by implementing a unique detection technique that is based upon learned caller fingerprints.

This ability of E-SBC security products to continuously learn call patterns in addition to being able to constantly analyze raw event data based upon specific user-definable criteria and take automatic action, gives them the unique characteristic of being the only products able to evolve and adapt on their own to effectively counter any new or existing threat.

Protection

The third crucial security function that the E-SBC security solution provides is complete network protection by blocking attacks while at the same time allowing legitimate calls to pass through unimpeded. This exceptional level of protection can be extended either to an individual end-point, a specific group of end-points, or to all the assets in the network based upon highly flexible user-defined rule sets called Unified Communications Policies. These policies can be implemented to precisely discriminate or normalize (aggregate) any incoming or outgoing signaling or multimedia traffic.

Functional Entities

E-SBC security products perform their security functions using three inter-related and complimentary functional entities (*signaling*, *media*, and *intelligence*), all of which are highly scaleable and can support UC call signaling and media activity for up to 10,000 users at 500 Mbps throughput. These functional entities can either be packaged in the same physical unit, or deployed separately throughout the enterprise network.

Signaling

The Signaling element is the primary call signaling protection subsystem and is typically deployed at the edge of the network, in the DMZ. Functioning as a proxy, the Signaling element accounts for less than 2 ms of the entire end-to-end latency budget. .

The Signaling element provides the following features:

- Inline signaling decryption and secure key management (TCP and TLS support)
- Hardware-accelerated SIP decoding
- Enhanced SIP validation (source limiting, policy enforcement, and DDoS detection)
    - NAT/FW traversal
    - Protocol anomaly detection and prevention
    - SIP source limiting

- DoS and DDoS attack detection and prevention
- Message sequence anomaly detection and prevention
- Continuous user behavior learning
- By-pass for all non-SIP traffic (ARP, DNS, ICMP, STUN, and TURN)
- Domain-based policy filtering based upon user definable call source and destination criteria
- Behavior anomaly detection
- Alarm generation and incident reporting to the E-SBC intelligence functional element

Media

The media element is the primary RTP media protection subsystem and is typically deployed in the network in conjunction with the Signaling element. The Media element can be deployed as a separate physical entity within a network in a distributed manner to facilitate various types of network topologies. In this arrangement, the Media element will be 'slaved' to a particular Signaling element to provide seamless RTP security and NAT traversal. In either deployment, the Media element accounts for less than 100 µs of the end-to-end latency budget.

The Media element provides the following features:

- Media policy enforcement
- RTP anomaly detection
- Timing and bandwidth validation
- Codec validation
- FAX and modem pass through

The Intelligence element is the primary UC security information management subsystem of the E-SBC solution. Its primary purpose is to receive the variously formatted event and alarm reports from the different security components in the network and to store and normalize that information into a comprehensive format that allows distributed attacks to be effectively detected and mitigated.

The E-SBC Intelligence function provides the following features:

- Event log collection
- Propagate alarms to network management systems
- Maintain per-user, per-caller, and per-network element behavior models on a ToD and DoW basis

E-SBC Deployment

E-SBC security products can be deployed in either of two basic modes depending upon organizational security needs and requirements: *In-line Mode* and *Screened Subnet Mode.*

E-SBC devices can be deployed in these modes with or without Transport Layer Security (TLS) / Secure Real-Time Transport Protocol (SRTP) encryption.

Two-Wire

The two-wire in-line topology (also referred to as *in-line*) is the simplest and most basic E-SBC security device deployment. Positioned at the edge of the network in the DMZ, directly in-line with the call servers, The E-SBC device can effectively protect the enterprise network against all types of inadvertent and malicious intrusions and attacks (Figure 1-7).

In this configuration, the E-SBC security device performs border access control functionality such as Firewall / Network Address Translation (FW/NAT) traversal (both internal and external), access management and control based on user-configurable domain policies, and intrusion functionality to protect against DoS, spoofing, and stealth attacks, along with voice SPAM.

In this deployment, E-SBC security products can enable UC Virtual Private Network (VPN) TLS encryption of the signaling traffic and SRTP encryption of the media traffic.

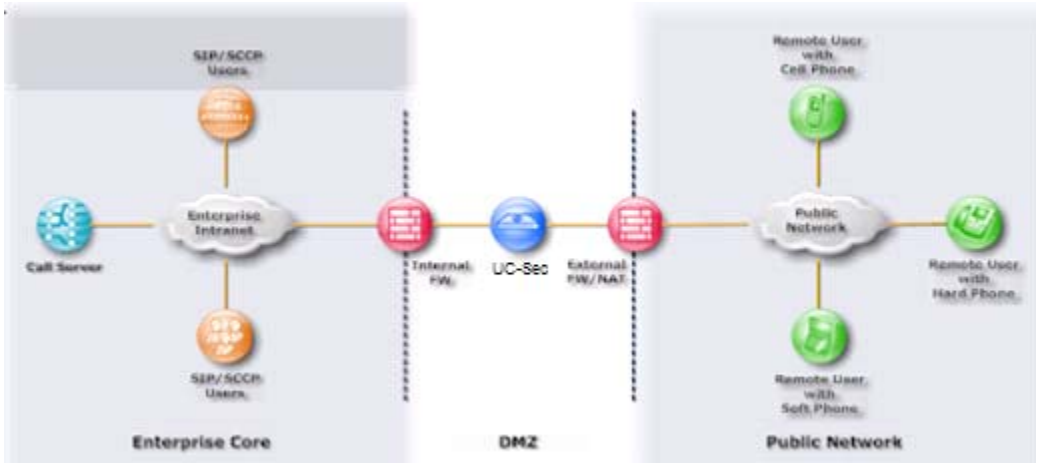


Figure 1-7. E-SBC Deployment – Two-Wire.

One-Wire

Similar to the two-wire deployment, is the *one-wire* deployment (also referred to as the *screened subnet*), wherein the E-SBC security device is deployed in the enterprise DMZ, but not directly in-line with the enterprise call servers (Figure 1-8). The E-SBC is in the direct signaling path, has an IP address, and is the next hop for SIP traffic. The E-SBC provides a high level of security functionality characteristic of in-line deployment without adding any latency to such time critical multimedia applications such as videoconferencing or music-on-demand.

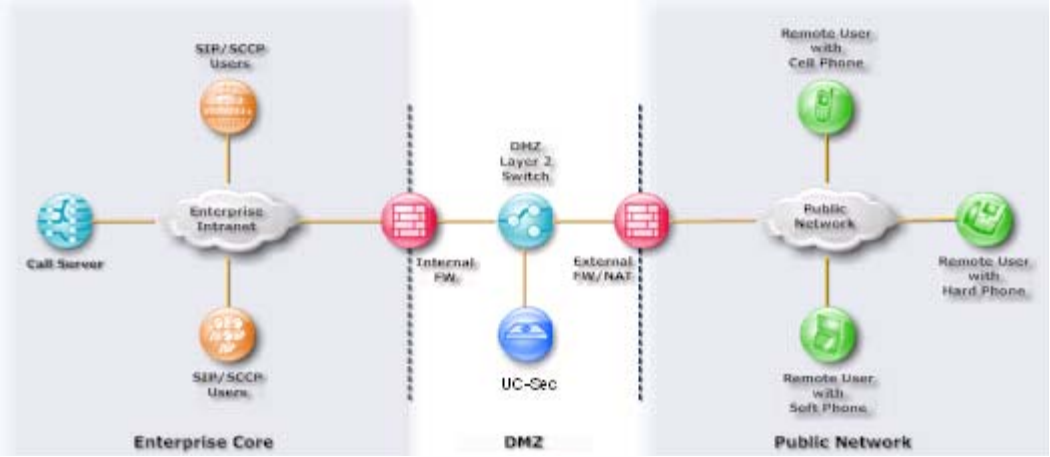


Figure 1-8. E-SBC Deployment – One-Wire.

Managing E-SBC Security Devices

E-SBC security devices can be monitored and controlled in one of two ways: either remotely via a graphical user interface (GUI) or locally via a command line interface (CLI). GUI access is provided by Ethernet management interface ports located on each E-SBC equipment chassis, which allow up to 10 simultaneous log-onto the E-SBC Control Center. Equally high-speed serial CLI access is provided by the console ports also located on the E-SBC equipment chassis, which allow administrators to establish direct, physical connections to the devices using any commonly available terminal device for provisioning, management, troubleshooting, maintenance, and repair. Both the GUI and CLI interfaces can be accessed any time an E-SBC security device is operational.

Graphical User Interface (GUI)

E-SBC security devices support a GUI interface through the EMS that can be accessed from any remote physical location using the web browsers Mozilla Firefox (2.0 or later), Microsoft Internet Explorer (7.0 or later), or the Google Chrome stable channel version. This provides administrators and maintenance personnel the ability to view concise, real-time, graphical representations of the security activities and operational condition of the network being monitored in addition to providing access to all the screens and windows necessary to properly configure and maintain each security aspect of a particular E-SBC device.

E-SBC Control Center

The **E-SBC Control Center** is the fully integrated, web-accessible operations and administration platform for the E-SBC UC security products. It is a graphical user interface (GUI) that centralizes and simplifies the provisioning, administration, control, and monitoring of the E-SBC signaling, media, and intelligence elements to reduce the overall operational burden and eliminate unnecessary system management complexity.

The E-SBC Control Center contains a redundant Solid® database to store configuration and subscriber information which is continually updated by each of the deployed E-SBC security elements.

The following functions can be performed using the E-SBC Control Center:

- Configuration Management
- Alarm and Fault Management
- Performance Management
- Administration and Maintenance

Refer to **Figure 1-9** for an example of the E-SBC Control Center Welcome Screen.

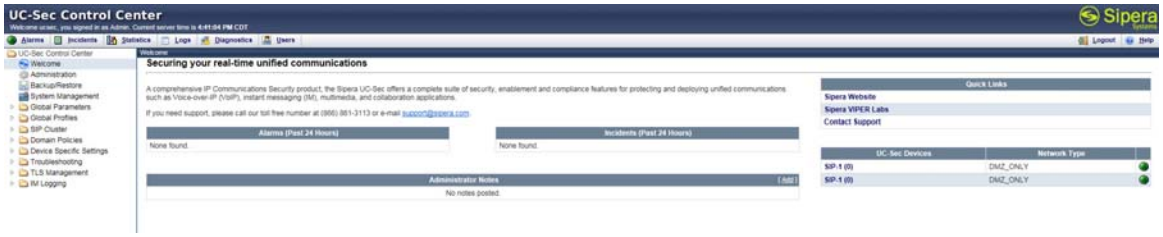


Figure 1-9. E-SBC Control Center – Welcome Screen.

Command Line Interface (CLI)

The Command Line Interface (CLI) is a management interface that provides local access to a particular E-SBC security device for performing administrative and operational tasks. These tasks are executed using various commands entered via a terminal emulator such as Telnet or another commonly available serial application like HyperTerminal. The CLI interface is available whenever an E-SBC equipment chassis is running. Security is provided through a combination of account login and user access privileges.

Note:	It is recommended that the Command Line Interface should only be used under the direction of authorized Sipera support personnel. Refer to Chapter 10, ***Command Line Interface*** for information on using the CLI.

This page intentionally left blank.

Getting Started 2

This chapter explains how to log into the E-SBC Control Center using a web browser. It also describes the general layout and function of the E-SBC Control Center interface and its various components.

Prerequisites

To ensure proper operation, the most recent versions of the following software programs are required to be installed on the workstation to be used for accessing the E-SBC Control Center:

- Mozilla Firefox™ (2.0 or later)
- Windows® Internet Explorer (7.0 or later)
- Google Chrome (stable channel)

Passwords

There are two types of passwords associated with E-SBC:

- Console Password
- EMS GUI Password

Console Password Complexity

The Console Password

- must be at least eight (8) characters long
- must contain at least two (2) uppercase characters, not including the first character of the password
- must contain at least one (1) lowercase character
- must contain at least one (1) special character
- must contain at least two (2) digits, not including the last character of the password
- Password Authentication Module (PAM) enforces password security, and hashes are stored in: **/etc/shadow**
- maximum length is not limited
- is hashed by MD5 hash algorithm

EMS GUI Password Complexity

The EMS GUI Password

- must be at least eight (8) characters long
- must contained mixed uppercase and lowercase characters
- must contain at least one (1) special character
- must contain at least one (1) number
- maximum length is not limited

- is hashed by SHA-256 hash algorithm

Password Policies

- Upon first-time power-up of the E-SBC, user is allowed immediate access to the E-SBC system via console.
- When user is configuring the box (this is where the Text-based User Interface (TUI) comes up), the system asks for root and ipcs account passwords.
- Before configuration, the default root password is: "sipera"

- The root password "sipera" is overwritten by the root password assigned during configuration. The default root password is not known by the customer user-end but by Sipera customer support personnel.
- All of the above policy statements apply to the EMS system as well.
- The EMS GUI has a separate password.
- The EMS GUI default password is "ucsec" for the account "ucsec."

Note

The Console Admin **Login ID** and **Password** are determined by the customer's network administrator during the installation procedure. Two of the installation steps prompt the installer to enter a chosen login and password.

The EMS GUI Admin **Login ID** and **Password** were assigned by Sipera when the E-SBC security was initially configured prior to shipment. Older installations may still use the previous default login / password: **ipcs / ipcs**

Logging-In to the E-SBC Control Center

- The E-SBC Control Center is used to provision, monitor and control the E-SBC functional entities and is accessed via a web browser (either Mozilla Firefox or Windows® Internet Explorer).

Initial Login

Logging-in to the E-SBC Control Center using the **Admin** account login ID and password provides unrestricted top-level access to all the features and parameters supported by the E-SBC security products.

Use the following procedure to login to the E-SBC Control Center for the first time:

Caution!

Great care should be taken by the Admin **when configuring or altering domain policies or network, system or security parameters as these actions will have an immediate and direct affect on the level of security provided to the enterprise. In addition, changing any of these parameters may also impact application or network availability.**

1. Open a new browser tab or window.

2. Enter the following URL:
   `https://<Control_Center_IP_Address>`
   where `<Control_Center_IP_Address>` is the IP address of the E-SBC Control Center you want to access.
3. Press `<Enter>`.
   The **E-SBC Control Center** (EMS) sign-in screen is displayed (Figure 2-1).

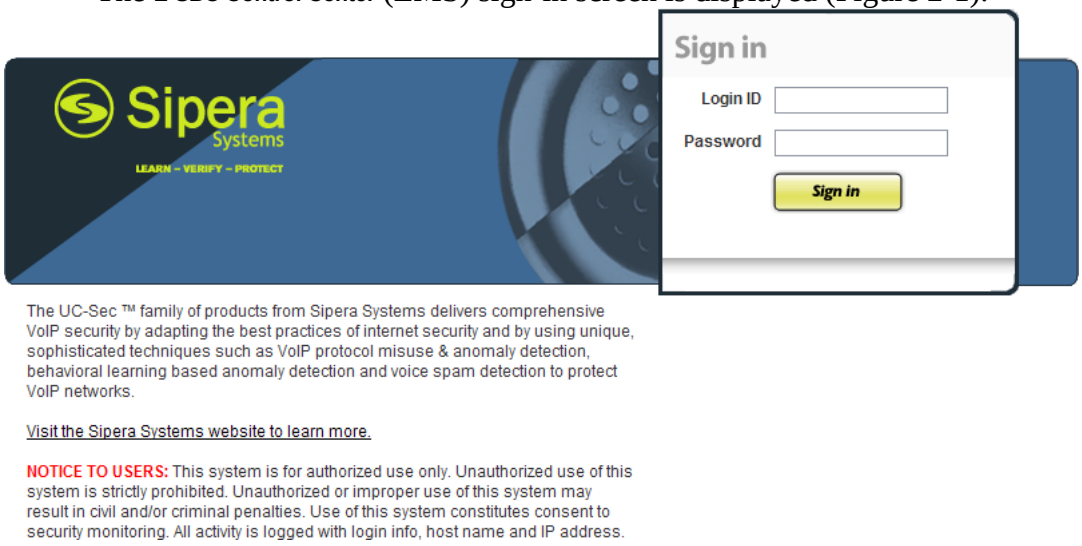


Figure 2-1. E-SBC Control Center – Login Screen.

4. Enter your assigned **Login ID** and **Password** and click the **Sign In** pushbutton.

> **Note** The EMS GUI Admin **Login ID** and **Password** were assigned by Sipera when the E-SBC security was initially configured prior to shipment and should have been provided to you when the equipment was delivered and installed.

The **E-SBC Control Center – Welcome Screen** is displayed, similar to the screen shown in Figure 2-2.

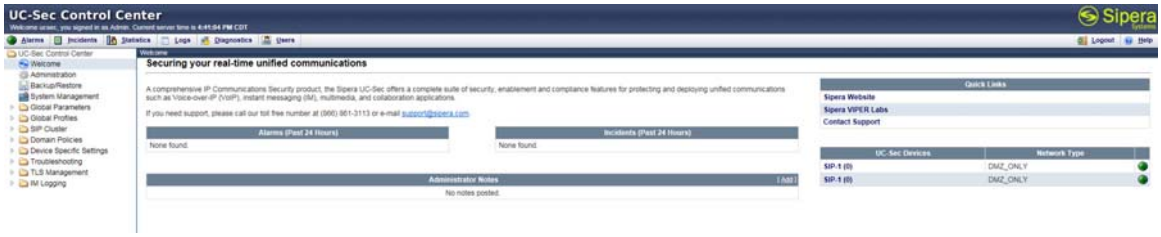


Figure 2-2. E-SBC Control Center – Welcome Screen Description

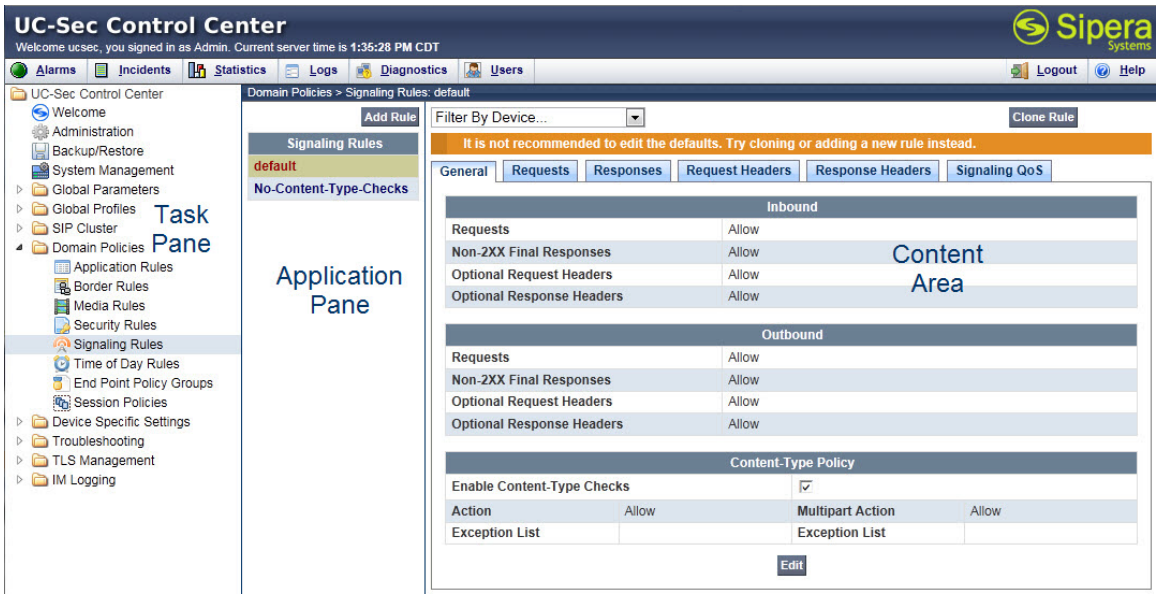


Figure 2-3. E-SBC Control Center – Functional Screen Description

The **E-SBC Control Center – Welcome Screen** is the top-level display screen which provides direct access to all the features, functions, and information available on the current release of the E-SBC security system. From this screen you can display additional, separate summary windows which contain active, up-to-the-minute alarm, incident, and statistical information as well as review and exchange textual messages with other administrative accounts. In addition, you can select wizards to either provision additional E-SBC security devices into the network or define new destination-source call flows. Finally, you can select specific E-SBC security features and functions from the **Task Pane** for administration and maintenance.

The various parts of the **E-SBC Control Center** screen are described in the section *E-SBC Control Center Screen Descriptions*.

E-SBC Control Center Screen Descriptions

The **E-SBC Control Center– Welcome Screen** is the main administrative and configuration display screen for the E-SBC security system (Figure 2-4). It is the screen that the E-SBC displays upon a successful logon and is comprised of five main sections – *Identification Bar*, *Tool Bar*, *Location Bar*, *Task Pane*, and *Content Area*. Together they provide an ordered, top-level textual and/or visual representation of the security status of the monitored IP network in real-time, as well as all the user-selectable options and controls that are necessary to facilitate administration.

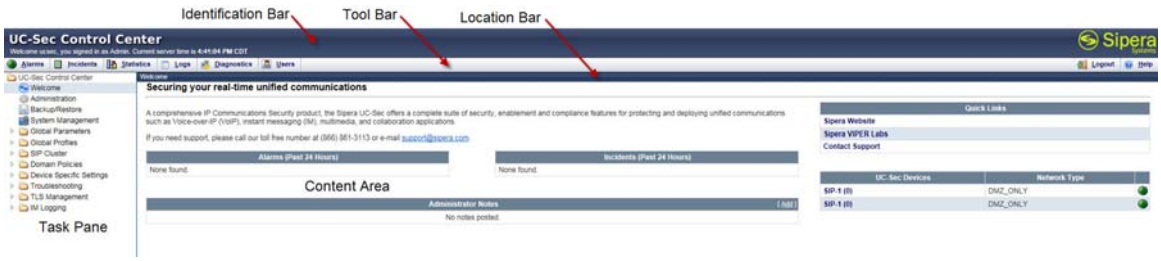


Figure 2-4. E-SBC Control Center – Welcome Screen

Identification Bar

The **Identification Bar** appears at the top of the E-SBC Control Center window. It provides certain basic identifying information such as which E-SBC software module is currently being viewed (**E-SBC Control Center** or **IM Log Viewer**) being run, the **user name** of the user currently logged in to the system, the user's assigned **administrative role**, and the current **time of day**.

Figure 2-5. Identification Bar.

Tool Bar

The **Tool Bar** (Figure 2-6) appears directly beneath the Identification Bar at the top of each E-SBC Control Center screen and contains several user-selectable icons (**Alarms**, **Incidents**, **Statistics**, **Users**, **Logout**, **Help**, and **About**) and a constantly-blinking alarm status indicator (**Alarms**).

Figure 2-6. Tool Bar.

Table 2-1. Toolbar Item Descriptions.

Icon	Name	Description
Alarms	**Alarm Status Indicator**	Indicates the current alarm status: **Green** – No active alarms **Red** – One or more alarms are active. When selected, opens the Alarm Status window.
Incidents	**Incident Viewer**	Opens the Incident Viewer window in the Content Area.
Statistics	**Display Statistics Screen**	Opens the E-SBC Statistics screen in a new window.
Logs	**SysLog Viewer Screen**	Opens the SysLog Viewer in a new window.
Diagnostics	**Diagnostic Test Selection Window**	Opens the Diagnostic Test Selection window. Test selections which can then be made are: **Full Diagnostic**, **Ping Test**, **Octeon PFC**, **Octeon TCP**, **Octeon TLS**, **Octeon Memory**, and **Octeon Ethernet**.
Users	**Display System Users**	Open the E-SBC Active User Account window.
Logout	**Logout**	Logs you out of the E-SBC Control Center and redisplays the main login screen.
Help	**Help**	Activates system help.
About	**About**	Displays the software version, build number, and copyright information for the E-SBC software running on your system.

Location Bar

The **Location Bar** (Figure 2-7) identifies your current location within the E-SBC Control Center feature and function structure.

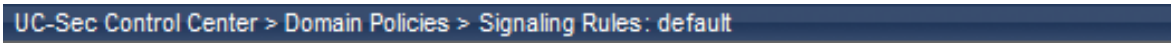


Figure 2-7. Example of Location Bar Information.

Task Pane

The **Task Pane** (Figure 2-8) is always displayed on the left side of the E-SBC Control Center and provides access to each of the functional areas of the E-SBC Control Center. The functional areas to which a user is granted access is determined by the administrative privileges assigned to them by the System Administrator (*Administrator*, *Manager*, or *Supervisor*).

The functions available to a particular administrative role are shown in Figure 2-9.

A general description of these functions and features is provided in the following sections.

Figure 2-8. E-SBC Control Center Task Pane.

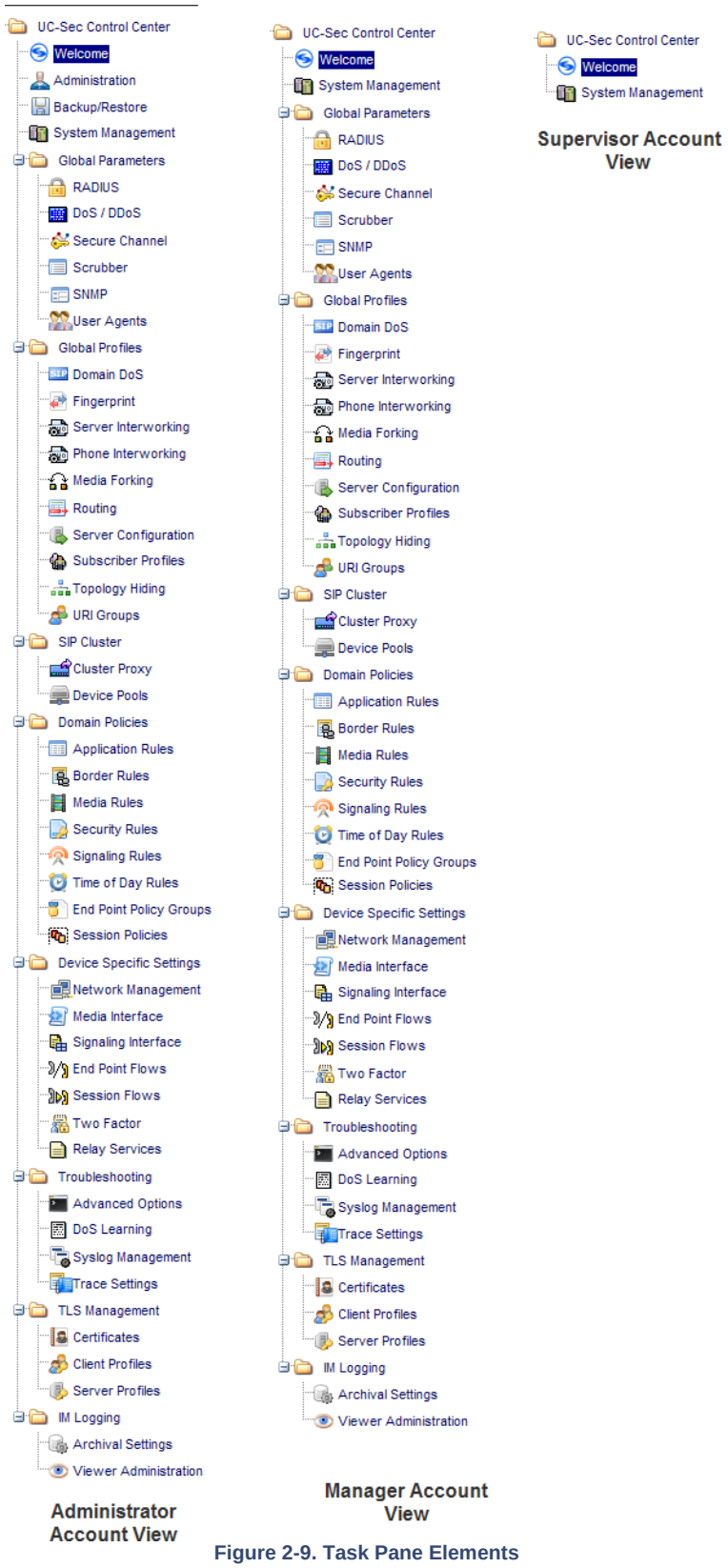


Figure 2-9. Task Pane Elements

Welcome

The **Welcome** feature causes the **E-SBC Control Center – Welcome Screen** to be displayed (Figure 2-2) from which you can view and access all the features, functions, and information available of the current release of the ICPS security system. Using this screen you can display additional, separate summary windows which contain active, up-to-the-minute alarm, incident, and statistical information as well as review and exchange textual messages with other administrative accounts. Finally, you can select specific E-SBC security features and functions from the Task Pane for administration and maintenance.

Notes

Depending upon which administrative user account you long in with (Administrator, Manager, or Supervisor) will determine which specific features will be displayed in the Task Pane. Refer to Figure 2-9.

Administration

The **Administration** function (Figure 2-10) displays the **User Administration** screen in the content area of the E-SBC Control Center which displays a comprehensive list of all users having **Admin**, **Manager**, and **Supervisor** privileges. In addition, this feature screen allows you add new user accounts, edit existing user accounts, and delete existing user accounts.

Figure 2-10. Administration Function.

Backup/Restore

The **Backup / Restore** function (Figure 2-11) displays the **Backup / Restore** window which allows you to create a back-up file containing a snapshot of the entire E-SBC system configuration. In addition, the **Backup / Restore** window allows you to restore system files when necessary.

Figure 2-11. Backup / Restore Function.

System Management

The **System Management** function (Figure 2-12) displays the **System Management** window which contains two tabs (**Installed** and **Updates**) that allow you to either view, configure, shut-down, or re-start E-SBC security devices or update the EMS software.

Figure 2-12. System Management.

Global Parameters

Refer to Figure 2-13. When selected, it allows for configuration of parameters across all E-SBC appliances (see Table 2-2).

Figure 2-13. Global Parameters Feature (Expanded View).

Table 2-2. Global Parameters Feature Descriptions.

Feature	Description
RADIUS	Displays the **Radius** tab allowing you to provision RADIUS server parameters, such as IP address, retry timeout, etc.
DoS / DDoS	Displays the **DoS Settings** screen containing four tabs: **Single Source DoS**, **Phone DoS/DDoS**, **Stealth DoS/DDoS**, and **Call Walking**. These tabs allow you to configure which actions the E-SBC security system will perform when certain types of **DoS**, **DDoS**, and **Call Walking** attacks have been detected.
Secure Channel	Not Applicable for E-SBC deployments.
Scrubber	Displays the **Scrubber** screen containing two tabs: **Packages** and **Rules** which allow you to determine which scrubber rule sets (packages) the E-SBC system will use when analyzing SIP signaling messages for anomalies.
Device Pools	Not Applicable for E-SBC deployments.
SNMP Settings	Displays the SNMP Settings screen which contains tabs (**SNMP v1/v2** and **SNMP v3**) that allow you to configure Simple Network Management Protocol (SNMP) parameters to enhance alarm reporting.
User Agents	Not Applicable for E-SBC deployments.

Global Profiles

Refer to Figure 2-14. When selected, Global Profiles allows for configuration of parameters across all E-SBC appliances (see Table 2-3).

Note:	These profiles are used in security rules. Refer to the section titled, "Security Rules," in Chapter 5.

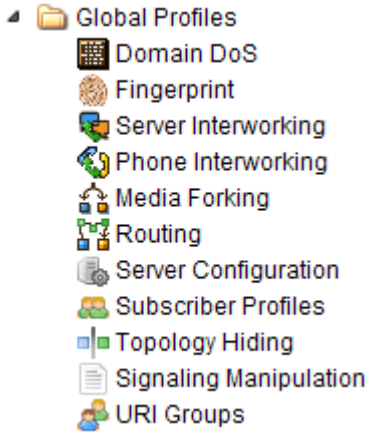


Figure 2-14 Global Profiles Feature

Table 2-3. Global Profiles Feature Descriptions

Feature	Description
Domain DoS	Displays the **Rate Limit** screen that allows you to determine how the E-SBC security solution will respond to suspected DoS attacks. Responses include **Alert Only**, **Enforce Limit**, **Sender Intention Verification**, and **White List**.
Fingerprint	Not Applicable for E-SBC deployments.
Interworking	Displays the **interworking** screen containing five tabs: **General**, **Timers**, **URI Manipulation**, **Header Manipulation**, and **Advanced**. These tabs allow you to edit specific SIP signaling message parameters to facilitate interoperability between SIP implementations within the enterprise. Two interworking features: • Phone Interworking (Not Applicable for E-SBC deployments.) • Server Interworking
Routing	Displays the **Routing Profile** which allows you to manage parameters related to routing SIP signaling messages.

Server Configuration	Displays the **Server Configuration** screen containing six tabs: **General**, **Authentication**, **Heartbeat**, **Advanced**, **DoS White List**, and **DoS Protection**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters (for HA deployments), DoS security statistics, and trusted domains. **Note:** DoS White List and DoS Protection are only activated once the ***DoS Protection*** check box is selected under the Advanced Tab.
Subscriber Profiles	Not Applicable for E-SBC deployments.
Topology Hiding	Displays the **Topology Hiding** screen which allows you to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. Hides the topology of the enterprise network from external networks.
Signaling Manipulation	Signaling Manipulation adds the ability to add, change, and delete any of the headers and other information in a SIP message. This feature will add the ability to configure such manipulation at each flow level in a highly flexible manner using a proprietary scripting language.
URI Groups	Displays the **URI Group** screen. The domain(s) comprising the URI Group is/are displayed in the Content Area. A URI Group is a logical group of SIP users that is referenced by call flows that are identified by various End Point and Session policies. URI Groups can be added, deleted, viewed, edited cloned, and deleted using the corresponding buttons in the Application Pane and Content Area.

Domain Policies

The **Domain Policies** feature (Figure 2-15), also referred to as *Unified Communication Policies*, allows you to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the E-SBC security device to aggregate, monitor, control, and normalize call flows.

When selected, these items perform the actions described in Table 2-4.

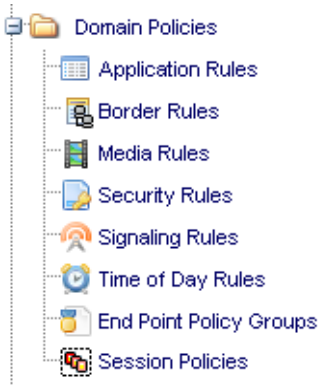


Figure 2-15. Domain Policy Feature (Expanded View).

Table 2-4. Domain Policy Feature Descriptions.

Feature	Description
Application Rules	Displays a list of existing **Application Rule** sets in the Application Pane. **Voice**, **Video**, and **IM** application states (**IN** / **OUT**) are displayed, along with the number of maximum concurrent sessions. These parameters can be changed in a pop-up window accessible from the Content Area. Application rules can be added, viewed, edited, cloned, or deleted using the corresponding buttons in the Application Pane and Content Area.
Border Rules	Displays the **NAT Traversal** tab which allows you to manage the way in which the E-SBC security device operates when deployed at the edge of the network (secure border access).
Media Rules	Displays a list of existing **Media Rule** sets in the Application Pane. The **Media Encryption**, **Media Anomaly**, **Media Silencing,** and **Media QoS** parameters for an existing Media Rule set are displayed in the Content Area. These values can be viewed or changed by selected the tab corresponding to the parameters group you want to see or change. Media rules can be added, viewed, edited, cloned, or deleted using the corresponding buttons in the Application Pane and Content Area.
Security Rules	Displays a list of existing **Security Rule** sets in the Application Pane. The **Authentication**, **Compliance**, **Fingerprint**, **Scrubber**, and **Domain DoS** parameters for an existing Security Rule set are displayed in the Content Area. These values can be viewed or changed by selected the tab corresponding to the group of parameters you want to see or change. Security Rule sets can be added, viewed, edited, cloned, or deleted using the corresponding buttons in the Application Pane and Content Area.

	Displays a list of existing **Signaling Rule** sets in the Application Pane. The **General**, **Requests**, **Responses**, **Request Headers**, **Response Headers** , and **Signaling QoS** parameters for an existing Signaling Rule set are displayed in the Content Area. These values can be viewed or changed by selected the tab corresponding to the control parameters group you want to see or change. Signaling rules can be added, viewed, edited, cloned, or deleted using the corresponding buttons in the Application Pane and Content Area.
	Displays a list of existing **Time-of-Day (ToD) Rule** sets in the Application Pane. The parameters of a ToD Rule set are displayed in the Content Area. These parameters can be viewed, edited, or deleted. In addition, new ToD Rule sets can be added as needed.
	Displays a list of existing end-point **Policy Groups** in the Application Pane. The Policy Sets comprising the Policy Group are displayed in the Content Area. A Policy Group is a completely user-definable combination of previously configured **Application**, **Border**, **Media**, **Security**, **Signaling**, and **ToD** rule sets that are applied to call flows traversing the enterprise as identified by **Sessions** feature. Policy Groups rules can be added, viewed, edited, cloned, or deleted using the corresponding buttons in the Application Pane and Content Area. **Caution!** The default parameters should only be changed after consulting Sipera's technical support staff.
	Displays two tabs which control how media streams are processed by the E-SBC: **Codec Prioritization** and **Media Anchoring**. Session Policies added, viewed, edited, cloned, or deleted using the corresponding buttons in the Application Pane and Content Area. **Caution!** These parameters should only be changed after consulting Sipera's technical support staff.

Device Specific Settings

Refer to Figure 2-16 and see descriptions of the menu selections in Table 2-5.

The **Device Specific Settings** feature for SIP allows you to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, you have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, and session call flows, as well as the ability to manage system logs and control security features.

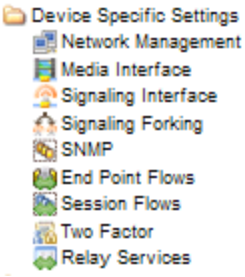


Figure 2-16. Device Specific Settings Feature (Expanded View).

Table 2-5. Device Specific Settings Feature Descriptions.

Feature	Description
Network Management	Displays the Network Management screen containing two tabs: **Network Configuration** and **Interface Configuration**. The **Network Configuration** tab allows you to manage the internal and external IP addresses assigned to a particular E-SBC security device while the **Interface Configuration** tab allows you to enable or disable E-SBC Ethernet interfaces (**A1**, **A2**, **B1**, and **B2**).
Media Interface	Displays the **Media Interface** screen which allows you to designate which server and port range will be used for media traffic.
Signaling Interface	Displays the **Signaling Interface** screen which allows you to designate which server and port range will be used for SIP signaling traffic (TCP, UDP, and TLS).
End Point Flows	Displays two tabs (**Subscriber Flows** and **Server Flows**) in the Content Area which allow you to determine how calls will be handled. Note that Subscriber Flows are not applicable for E-SBC deployments, therefore only the **Server Flows** tab will be applicable. Together, these flow descriptions determine which security actions will be applied to the message packets identified by these combined policies. The End Point Flows determine the End Point Policy Group, which includes a security rule set (domain policy).
Session Flows	Displays the **Session Flows** screen, which contains a prioritized list of all currently defined media Session Flows. The Session Flow dictates what session policy to use.
Relay Services	Not Applicable for E-SBC deployments.

Troubleshooting

Refer to Figure 2-17 and see descriptions of the menu selections in Table 2-6.

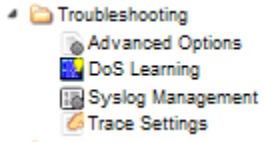


Figure 2-17. Troubleshooting Feature (Expanded View).

The Troubleshooting Feature provides options that are useful for troubleshooting problems.

Table 2-6. Troubleshooting Feature Descriptions.

<table>
<tr><th>Feature Item</th><th>Description</th></tr>
<tr><td>Advanced Options</td><td>The following tabs options may be displayed:

<table>
<tr><th>Tabs</th><th>EMS</th><th>E-SBC</th></tr>
<tr><td>Subsystem Logs</td><td>√</td><td>√</td></tr>
<tr><td>Port Ranges</td><td></td><td>√</td></tr>
<tr><td>CDR listing</td><td></td><td>√</td></tr>
<tr><td>Feature Control</td><td></td><td>√</td></tr>
<tr><td>SIP Options</td><td></td><td>√</td></tr>
</table></td></tr>
<tr><td>DoS Learning</td><td>Displays the Learned Info screen which allows you to select a time slot (i.e., weekday/weekend and morning/afternoon, evening/night) for which DoS-related information will be learned and displayed, providing a snap-shot of potential threats and anomalies which may be targeting the network. DoS information learned will be the DoS Protection parameters that were configured under the DoS Protection tab of the Server Configuration feature. An Update button updates a displayed list with the current information.

Note: This learns “Server DoS/DDoS” only, and the learning applies to : Global Profiles → Server Configuration → Profile → DoS Protection Tab</td></tr>
<tr><td>Syslog Management</td><td>Displays a Log Level tab where Syslog information specifications can be selected for Class (i.e., Platform, Trace, Security, Protocol, and Registrations) for a specified Facility. Log Level specifictions (i.e., All, Info, Notice, Warning, Error, Critical, Alert, and Emergency) determine the types of information reported.

A Collectors tab allows you to view, edit, or add Syslog collector locations, with each location specified by Facility and EMS device.</td></tr>
<tr><td>Trace Settings</td><td>Displays the Trace Settings screen which allows you to define the parameters necessary to trace a media packet traversing the network.</td></tr>
</table>

TLS Management

When selected, the menu items (Figure 2-18) perform the actions described in Table 2-7.

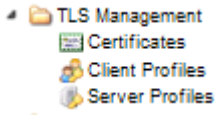


Figure 2-18. TLS Management Feature (Expanded View).

The **TLS Management** feature allows you to manage the parameters defined by the Transport Layer Security (TLS) protocol specification to efficiently administer the security services that establish and maintain a secure TCP/IP connection between two communicating entities. Implementing TLS within an enterprise VoIP network ensures communications session confidentiality, message integrity, and user authentication.

Successful TLS management requires that the two parties to a communications session (the *client* and *server*) be properly certified, so that their identity to each other can be unquestioningly verified and trusted. The mechanism used to authenticate subscriber identities are *certificates* that are issued by a trusted Certificate Authority (CA). The **TLS Management** features allows you to manage each facet of the TLS connection (certificates, clients, and servers) by selecting the desired TLS function (**Certificates**, **Client Profiles**, and **Server Profiles**) from the **Task Pane** and setting the corresponding parameters to very precisely define the manner in which you want the TLS feature to function.

Table 2-7. TLS Management Feature Descriptions.

Feature Item	Description
Certificates	Displays five tabs (**Generate CSR**, **View Certificates**, **Install Certificates**, **Install CA Root Certificate**, and **Install CRL**) which allow you to precisely define the certificates to be used in subsequent TLS sessions.
Client Profiles	Displays a list of all currently available client profiles in the Application Pane. You can also define additional client profiles if necessary using automated field requests to solicit the information necessary to authorized a client to participate in a secure TLS session.
Server Profiles	Defines a list of all currently available server profiles in the Application Pane. You can also define additional server profiles using automated field requests to solicit the information necessary to authorize a server to participate in a secure TLS session.

Application Pane

When certain security features are selected from the Task Pane (Figure 2-8), a list of available items (E-SBC device, VoIP server, rule set, etc.) to which that feature can be applied is displayed in the Application Pane (Figure 2-19). When the desired item is selected from the list in the Application Pane, the specific feature parameters that are assigned to that item are displayed in the Content Area of the display screen Figure 2-20), where they can be managed as desired.

Figure 2-19. E-SBC Control Center – Application Pane.

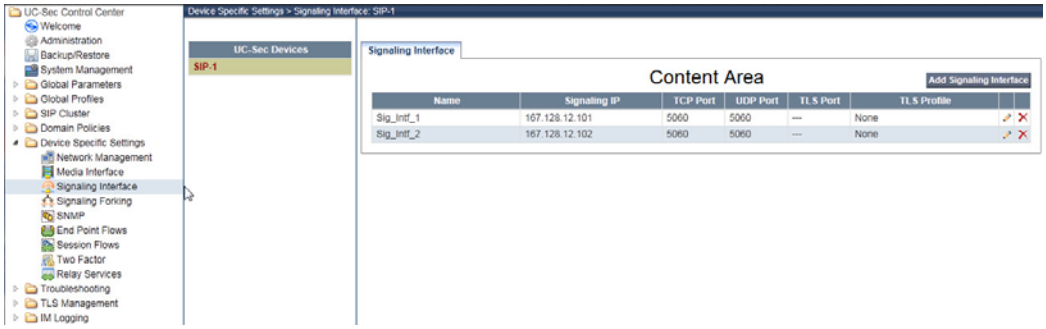


Figure 2-20. E-SBC Control Center – Content Area.

Content Area

Refer to Figure 2-20. This portion of the E-SBC Control Center presents the contents of the selected features or functions that are selected from the **Task Pane**. The different screens and windows displayed by the E-SBC Control Center use various pushbuttons and icons to perform certain functions. These are described in the section *Screen Pushbuttons and Icons*.

The Content Area of the Welcome screen (Figure 2-21) is different than the Content Area that is displayed when other features are selected from the Task Pane in that it does not contain an Application Pane, nor does it contain low-level function-specific information such as feature fields or parameter values. Instead, it contains various summary areas which display top-level, system-wide information such as which alarms and incidents are currently active, links to available Quick Links, a list of installed E-SBC security devices, E-SBC device deployment information, and an area for viewing and exchanging text messages with other administrators (Figure 2-22).

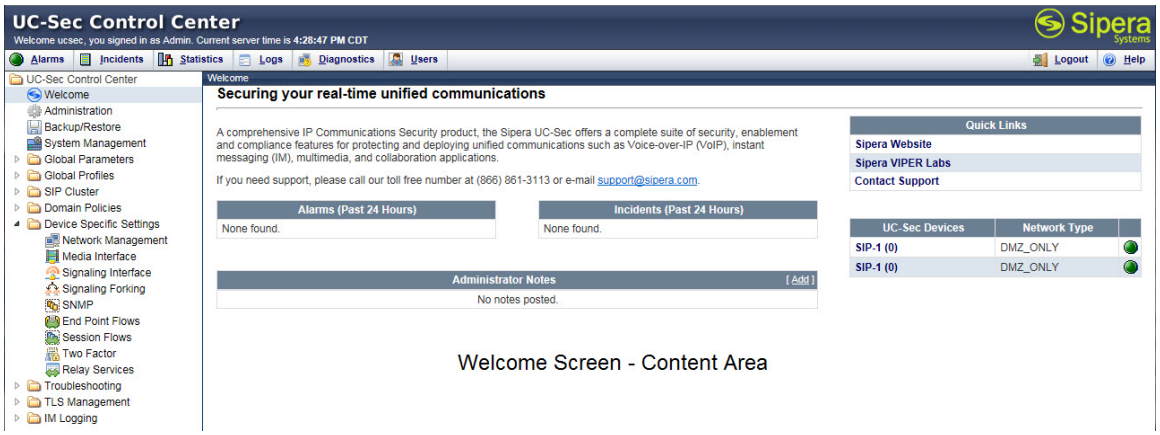


Figure 2-21. E-SBC Control Center – Content Area (Welcome Screen).

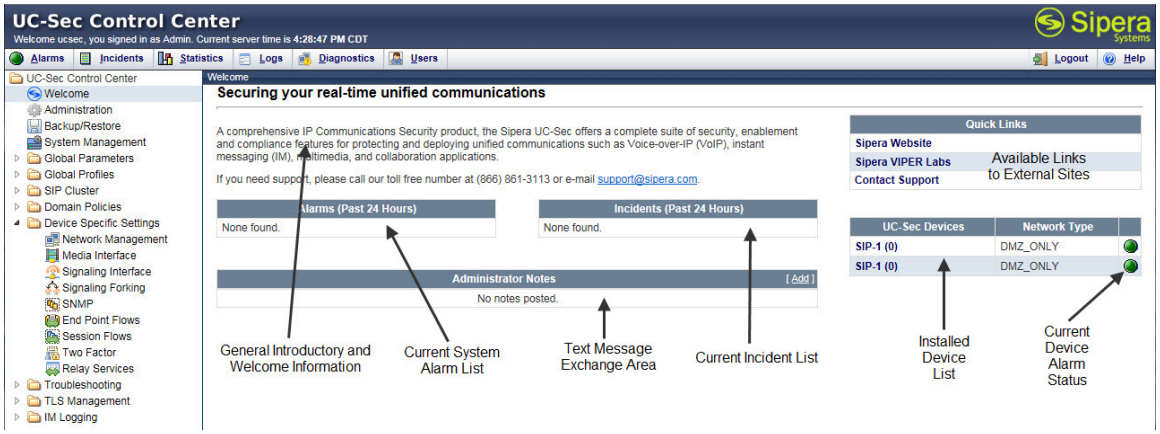


Figure 2-22. Welcome Screen Content Area Descriptions.

General Introductory and Welcome Information

This portion of the Content Area describes the purpose of the E-SBC security product and provides suggestions for using the Control Panel, such as for installing an E-SBC security device into the network or configuring a device previously installed.

Alarms

A streaming feed which displays currently active system alarms, parsed according to the E-SBC device type which generated it. More information on the listed alarms can be accessed by clicking the **Alarms** pushbutton from the **Tool Bar**. A separate **Alarms** window will be opened from which the alarm can be viewed and manually cleared.

Figure 2-23. Current System Alarms List.

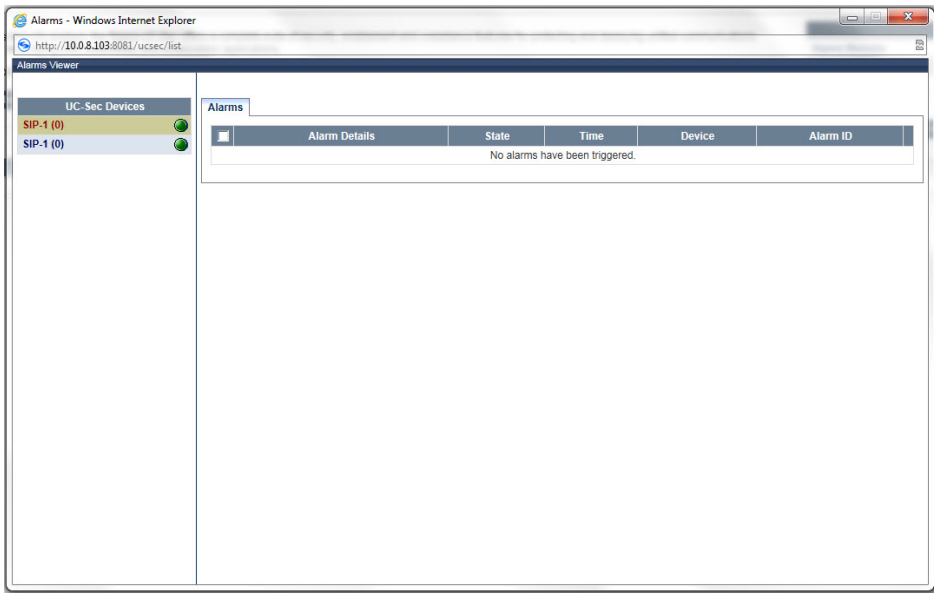


Figure 2-24. Alarms Window.

Latest Incidents

A streaming feed which displays currently active system incidents, also parsed according to the E-SBC device type which generated it. More information on the listed incidents can be accessed by clicking the **Incidents** pushbutton from the **Tool Bar.** A separate **Incidents** window will be opened from which the alarm can be viewed and manually cleared (Figure 2-26).

Note:	Incidents are associated with security issues while alarms are associated with hardware/connectivity issues.

Figure 2-25. Current System Incidents List.

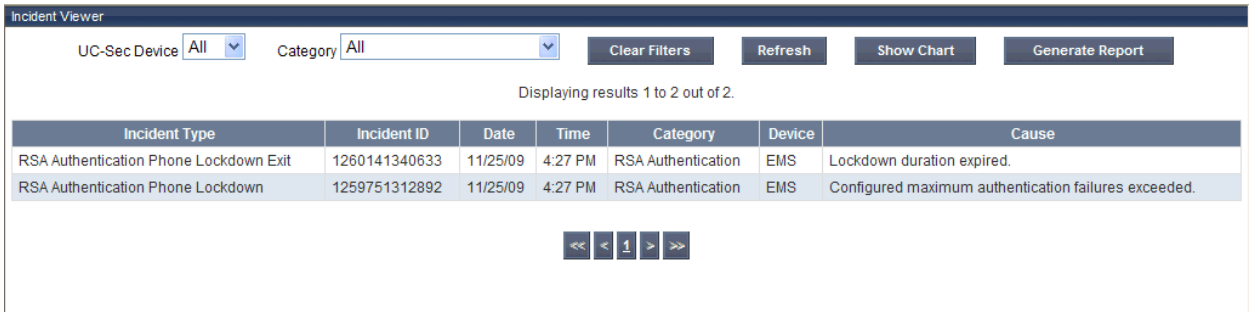


Figure 2-26. Incidents Window.

Administrator Notes

Refer to Figure 2-27. This portion of the **Content Area** allows you to view and exchange text messages with other E-SBC administrative users to ensure that important system, security, or administrative information is relayed when necessary. This feature allows you to edit existing messages posted by other users, add new messages of your own, or delete outdated or expired messages.

Messages posted in this area are stored in the EMS database and are retained when the system is powered down. Messages are continually displayed until such time as they are explicitly deleted by an administrative user.

Figure 2-27. Administrator Notes.

Quick Links

The **Quick Links** section (Figure 2-28) of the **Welcome Screen** provides a readily accessible list of external links to Sipera Systems, Inc.'s customer support sites: Sipera's homepage, Sipera's VIPER Labs, and e-mail access to Sipera Customer Support.

Figure 2-28. Quick Links.

Installed E-SBC Security Device List

The **Installed E-SBC Security Device List** provides a list of all the E-SBC security devices which are installed and provisioned in the enterprise VoIP network. In addition to the name of an E-SBC device, its location in the network and the manner in which it is deployed is also provided (Figure 2-29). A graphical representation of its location is displayed in upper-right-hand portion of the *Welcome Screen*.

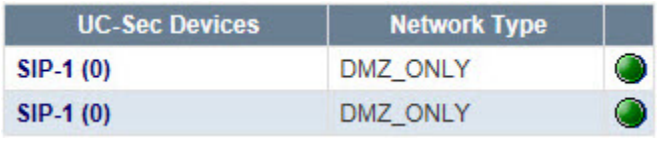
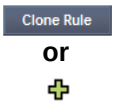


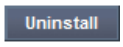
Figure 2-29. Installed E-SBC Security Device List.

Screen Pushbuttons and Icons

The pushbuttons and icons used by the different E-SBC Control Center screens and pop-up windows are described in Table 2-8.

Table 2-8. Screen Icon Descriptions.

Icon	Purpose	Description
	About	Displays a pop-up window which contains the version and build of the current software release.
	Activate Feature	Causes the currently selected features / parameters to be enabled.
	Add/ New	Allows you to create a new element, rule, or policy depending upon the screen currently being displayed.
	Alarm Status Indicator	Indicates the current alarm status: **Green** – No active alarms **Red** – One or more alarms are active. Also activates a separate **Alarms** pop-up window that displays a list of all active system alarms and their details.
	Cancel	Cancels the current operation and closes the window without saving any changes.
	Checkbox	Used to select or deselect specific items, features, parameters, or actions.
	**Clone**	Causes the currently selected rule or parameter to be copied to a new record to facilitate defining new rules.
	Close	Cancels the current operation and closes the window without saving any changes.
	Delete	Allows you to delete the selected element or item from the currently displayed list.
	Display Statistics	Displays the Statistics screen in a new window.
	Edit	Allows you to edit the currently displayed row or object.
	Expand	Expands the current selection to display nested items.
	Collapse	Collapses the currently expanded category display list.
	Help	Activates on-line help.
	Incidents	Activates a separate **Incidents** pop-up window to display all recently reported system-wide incidences..

Icon	Purpose	Description
	Logout	Logs you out of E-SBC Control Center and redisplays the login screen.
	Radio Button	Used to select or deselect the corresponding item.
	Reboot Device	Reboot the associated E-SBC security device.
	Shutdown Device	Shutdown the associated E-SBC security device.
	Restart Application	Restart an E-SBC application.
	View Configuration	View the configuration of the associated E-SBC security device.
	Install Device	Install the associated E-SBC security device into the network.
	Save	Allows you to save information for the element associated with the **Save** icon.
	Select All	Selects all the items in the current list.
	Show Calendar	Displays a monthly calendar, where the month, day, and year are user-selectable.
	Open SSH Session	Open a CLI-based secure shell session to the indicated E-SBC security device.
	Statistics	Activates a separate Statistics pop-up window that displays cumulative **Call**, **Policy**, and **Protocol** statistics.
	Undo / Cancel	Allows you to undo changes made to an element after it has been edited. **Undo** reverts the element back to its pre-edit state.
	Users	Opens a separate **Logged-in Users** pop-up window that displays all active Administrator accounts.
	Swap Device	Allows you to automatically substitute one E-SBC security device for another, thereby placing a new device into service with the same provisioning information as the one being replaced.
	**Uninstall**	Causes the selected item to be uninstalled (de-commissioned) from the network.

This page intentionally left blank.

Administrative User Accounts 3

This chapter explains how to create and manage Administrative user accounts.

Managing Administrative User Accounts

Administrative (Admin) user accounts are manually created and edited using the **Administration** feature selected from the **Task Panel**. Using this feature, you are able to create three levels of administrator: **Admin**, **Manager**, and **Supervisor**. The **Admin** user has full read/write access to all the features provided by the E-SBC security device, which includes adding, editing, and deleting other administrative accounts. The **Manager** has the same access privileges as the **Admin** user, with the exception of not being able to add new administrative accounts. The **Supervisor** has the least system access; this account only has read privileges for viewing incidence and statistical logs. The different levels of functional access are detailed in Figure 3-1.

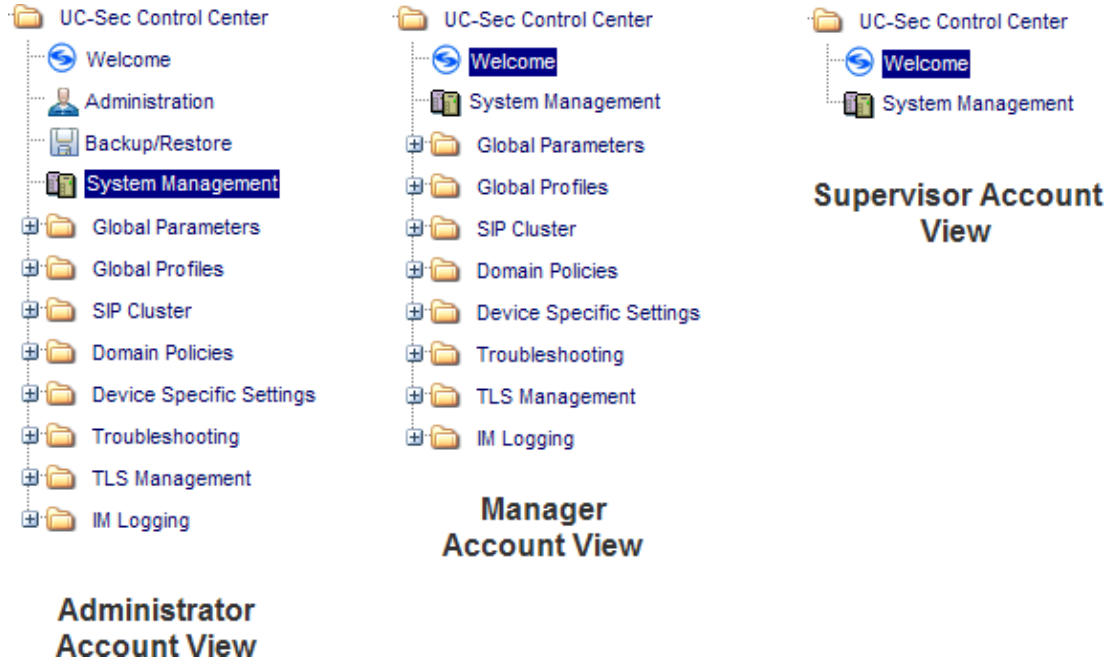


Figure 3-1. Available Administrative Functions by Access Level

Administrative Accounts

Use the following procedures to create, edit, and delete Administrative user accounts.

Notes

The current E-SBC release supports three types of Administrative account: **Administrator** (or **Admin**), **Manager**, and **Supervisor**. One **User account** is established by Sipera when the E-SBC equipment chassis is initially installed and configured for deployment using information provided by the customer.

Use this account information to perform the following procedures.

Creating a New Administrative Account

Use the following procedure to establish a new administrative account.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Administration** function from the Task Pane.
   The **Users** tab of the Administration screen is displayed (Figure 3-2).

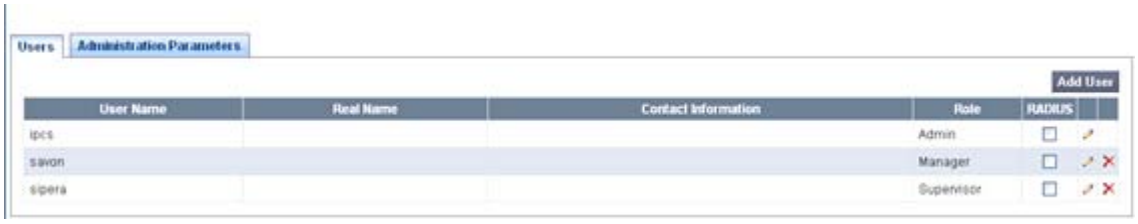


Figure 3-2. Default Administration Display.

3. Click the **Add User** button in the Applications Pane.
   The **Add New Administrative User** pop-up window is displayed (Figure 3-3).

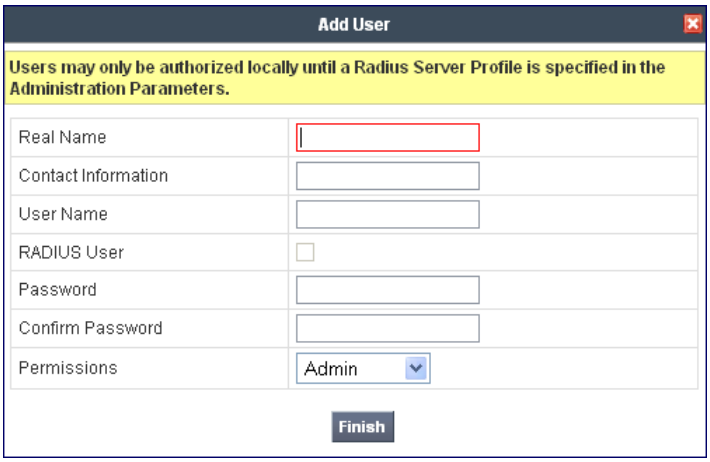


Figure 3-3. Add New Administrative User Pop-up Window.

4. Enter the requested information into the appropriate fields (Figure 3-3).
   Selecting clears the fields and closes the pop-up window without saving.

Table 3-1. Add New Administrative User Pop-up Window Field Descriptions.

Field	Description
Real Name	Real name of the individual for whom this account is being created.
Contact Information	Contact information (e.g., email, phone, number etc.) of the owner of this account.
User Name	System name assigned to the owner of this account.
RADIUS User	Checkbox indicating that the user will be authenticated via a RADIUS server. If checked (☑), the following **Password** and **Confirm Password** fields will be deactivated.
Password	The login password being assigned to this account. Only activated if the RADIUS User checkbox is unchecked (☐).
Confirm Password	A reliability feature to ensure the correct password has been entered in the previous field. Only activated if the RADIUS User checkbox is unchecked (☐).
Permission	The level of administrative access to be granted to this account. **Admin** — Highest level of system access, having full read/write permissions for all screens and features. Can create and delete new user accounts. **Manager** — Read/write access for all screens and functions, with the exception of not being able to create new user accounts. **Supervisor** — Only read access to certain incidence and statistical logs.

5. Select **Finish** to create the new administrative account and close the window or select the **Close** icon to cancel the operation and close the pop-up window without saving.
   The new account will be displayed in the Content Area (Figure 3-4).

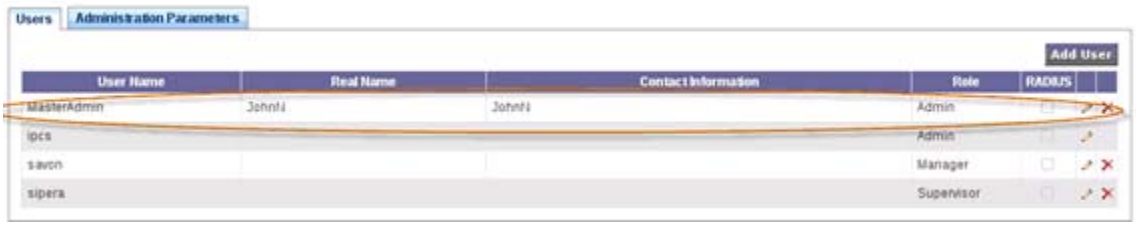


Figure 3-4. Updated Administration Display.

Setting Administrative Account Privileges

Use the following procedure to configure administration parameters for all existing user accounts (i.e., Administrator, Manager, and Supervisor).

1. Select the **Administration Parameters** tab.
   The **Administration Parameters** screen is displayed (Figure 3-5).

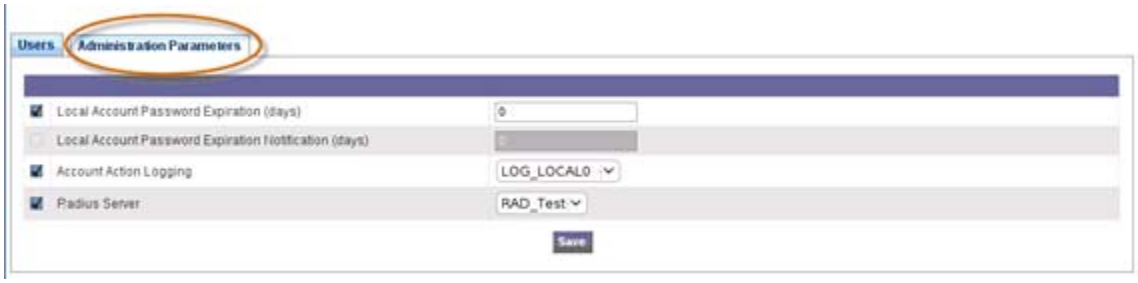


Figure 3-5. Administration Parameters Tab Display.

2. Enter the requested information into the appropriate fields in Table 3-2.

Table 3-2. Administration Parameters Tab Display Field Descriptions.

Field	Description
Local Account Password Expiration (days)	Checkbox indicating whether or not the password assigned to this user account will expire after the number of days indicated in the corresponding field. If checked (☑), the assigned password will expire after the indicated number of days. If unchecked (☐), the password assigned to this user account will not expire after a predetermined time period. It can be used indefinitely.
Local Account Password Expiration Notification (days)	Checkbox indicating whether or not an expiration notification should be given to the user when they log-on to the EMS informing them that their password will expire within the indicated number of days. If checked (☑), a notification will be displayed each time the user logs-on to the EMS. If unchecked (☐), a notification will not be displayed.
Account Action Logging	A checkbox indicating whether or not the actions performed by this user account are to be logged. If checked (☑), the users actions will be logged to the filed selected from the corresponding pull-down menu. If unchecked (☐), user actions are not logged and the corresponding pull-down menu is disabled.

Field	Description
Radius Server	A checkbox indicating whether or not RADIUS user accounts are to be authenticated. If checked (☑), RADIUS user accounts will be authenticated by the RADIUS server selected from the corresponding pull-down menu. If unchecked (☐), RADIUS user accounts will not be authenticated.

3. Select Save to save the parameter configuration.
   A notification will be displayed in the Content Area informing you that the new configuration has been successfully saved (Figure 3-6).

Figure 3-6. Administration Parameters Confirmation Display.

Editing an Existing Administrative Account

Use the following procedure to edit an existing administrative account.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Administration** function from the Task Pane.
   The **Users** screen is displayed (Figure 3-2).
3. In the Content Area, select the edit icon ( ) corresponding to the admin user account you want to edit.
   The **Edit User** pop-up window is displayed as shown in Figure 3-7.

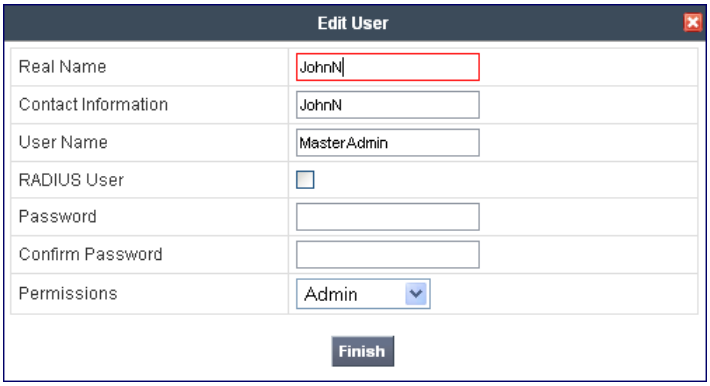


Figure 3-7. Edit Administrative User Pop-up Window.

4. Edit the desired fields.
5. Select **Finish** to update the administrative account record and close the window, or select the **Close** icon to close the window without saving.

Deleting an Existing Administrative Account

Use the following procedure to edit an existing administrative account:

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Administration** function from the Task Pane
   The **Administrative Users** screen is displayed (Figure 3-2).
3. In the Content Area, select the delete icon (✕) corresponding to the user account you want to delete.
4. A confirmation pop-up window is displayed similar to that shown in Figure 3-8.
5. Click **ok**.
   The desired administrative user account is deleted (Figure 3-9).

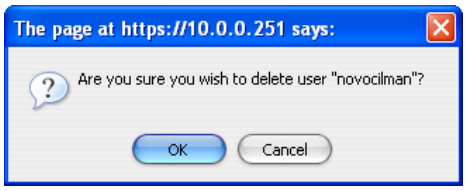


Figure 3-8. Delete Confirmation Pop-up Window.

Figure 3-9. Updated Administration Display.

Adding an E-SBC Device

When the EMS is set up as a separate device, one or more E-SBC devices must be added from the System Management function. Use the following procedure to add an E-SBC device.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **System Management** function from the Task Pane.
   The System **Management** screen is displayed (Figure 3-10).
3. In the Content Area, select the **Add Device** button to display the Add Device pop-up window (Figure 3-11).
4. In the Add Device pop-up window, complete the required information fields, and select the **Finish** button to save and exit.
   The device list will be redisplayed with the newly created device added to the list.

Figure 3-10. System Management Screen

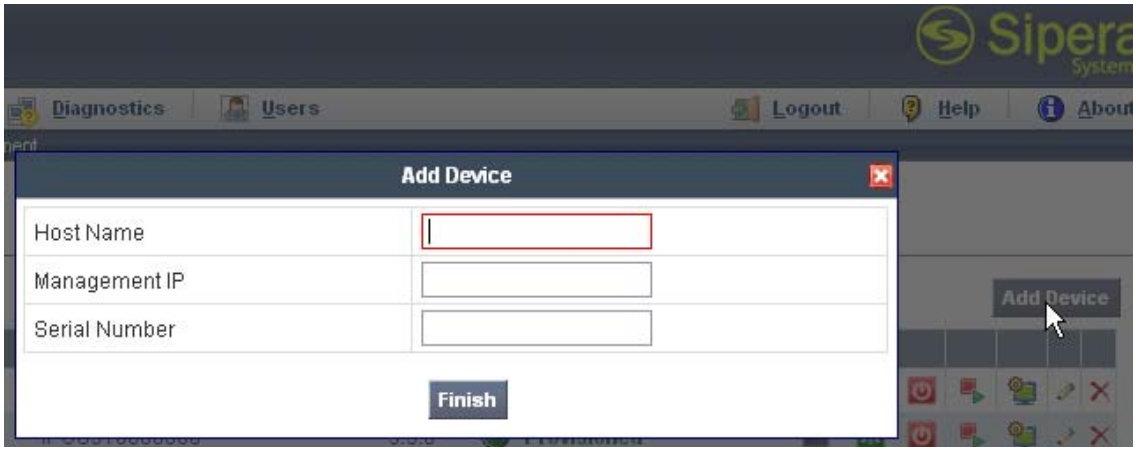


Figure 3-11. Add Device Pop-Up Window

Provisioning an E-SBC Device

Use the following procedure to provision an already installed E-SBC security device into an existing enterprise VoIP network.

1. Select the **System Management** feature from the Task Pane.
   The **System Management** screen is displayed (Figure 3-10).
2. Select the **Installed** tab if not already displayed.

Note:	E-SBC security devices which are physically installed into the network and available for provisioning are identified by a Registered (as opposed to Provisioned) status. In addition, the Installation icon ( ) is displayed only for those devices which have not yet been provisioned (Figure 3-10). E-SBC devices which have already been successfully provisioned display the View Config icon ( ).

3. Select the **Installation** icon ( ) corresponding to the device you want to provision.
   The **Installation** pop-up window is displayed (
Figure 3-12).

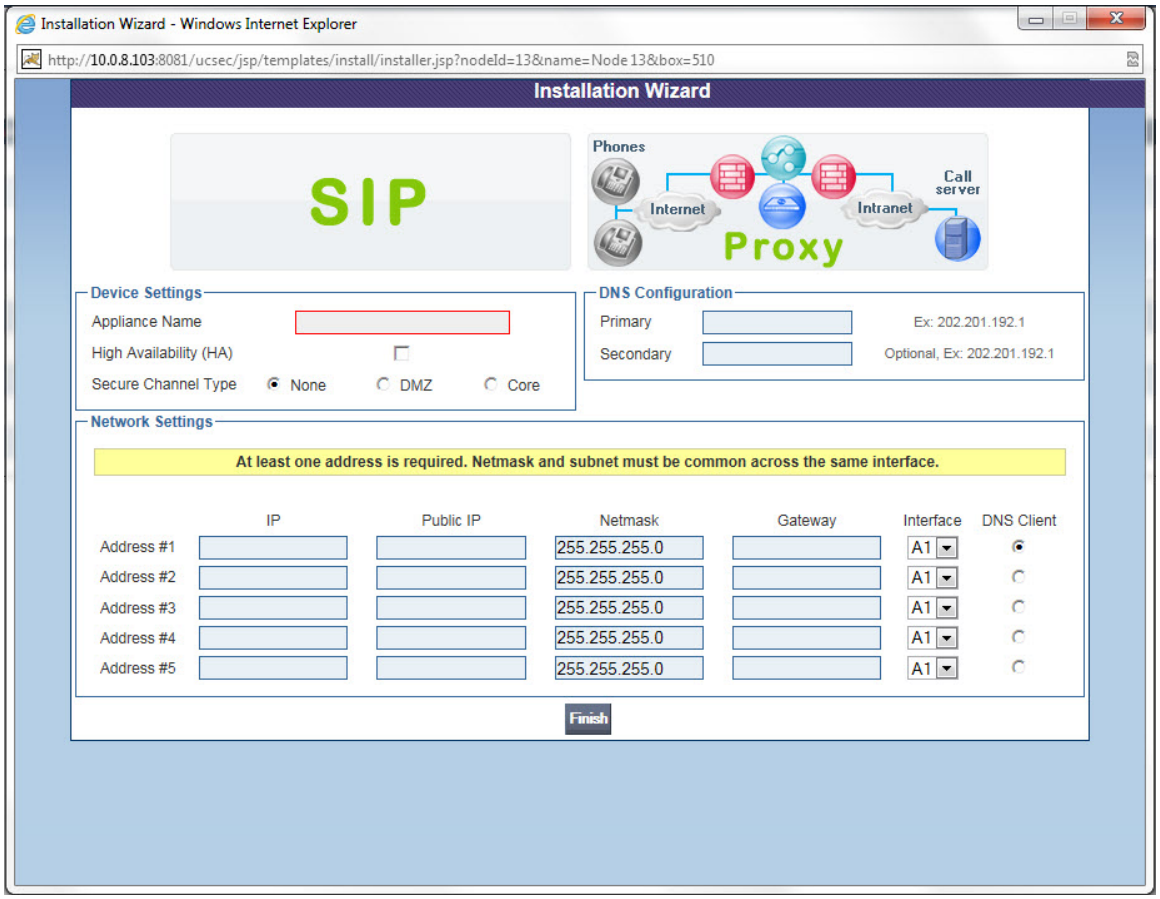


Figure 3-12. Installation Pop-Up Window

4. Enter an Appliance Name for the UC-Sec security device being provisioned and its deployment settings (i.e., HA and Secure Channel Type).
5. Table 3-1 provides a more complete description of the selections to be made on this window.

Table 3-3. Installation Wizard Field Descriptions – Installation Pop-Up Window

Field	Description
Appliance Name	A descriptive name assigned to the E-SBC security device being provisioned. This name will subsequently be used as the device host name.

Field	Description
High Availability (HA)	A checkbox indicating that the E-SBC security device being provisioned will be part of a High-Availability (HA) pair. If checked (☑), a drop-down window will be displayed containing a list of HA partners as shown below. Click to select the desired HA partner. **Note: For HA configuration instructions, refer to the next section in this chapter titled, "E-SBC High Availability (HA) Configurations."**
Secure Channel Type	Radio button indicating whether or not this E-SBC security device will be part of a secure channel. Available selections are: **None** — This E-SBC device will not be communicating via a secure channel. **DMZ** — This E-SBC security device will be deployed in the enterprise DMZ to enable secure communications with another UC-Sec security device deployed in the core. **Core** — This E-SBC security device will be deployed in the enterprise core to enable secure communications with another UC-Sec security device deployed in the DMZ.
DNS Configuration	
Primary	The IP address of the primary DNS server.
Secondary	The IP address of the secondary DNS server.
Network Settings	
IP	IP is the actual IP address of the E-SBC device (whether it is publically reachable or not) that is being configured.
Public IP	Public IP is the publically-reachable IP address of the E-SBC security device being configured and is the IP address that the device will use to access the external network. If near-end NAT is not employed, the Public IP address may be the same as the IP (actual) address.
Netmask	The subnet mask of the E-SBC device being configured.
Gateway	The IP address of the device the E-SBC security device will use to send local network traffic to other networks.
Interface	A drop-down menu from which you select the physical interface of the E-SBC security device which will be used to interface to the external, public network (**A1**, **A2**, **B1**, and **B2**).
DNS Client	Select the **DNS Client** radio button next to the interface (normally A1) that is reachable by the DNS servers that were defined previously in the **Primary** and **Secondary** fields in the **DNS Configuration** area.

Device Configuration 4

This chapter explains how to provision new E-SBC security devices using the **System Management** function from the Task Pane.

> **Note** The device installation feature can only be accessed and used by the **Admin** or **Manager** accounts. The **Supervisor** account cannot access or use this feature.

Prerequisites

To ensure the successful operation of this semi-automated feature, you must first ensure that the desired E-SBC security device has been properly installed and powered-up, according to the procedures described in the *Sipera E-SBC 1U Installation Guide* (101-5224-400).

Installing an E-SBC Device

Use the following procedure to provision an already installed E-SBC security device into an existing enterprise VoIP network.

1. Select the **System Management** feature from the Task Pane.
   The **System Management** screen is displayed.
2. Select the **Installed** tab if not already displayed.

E-SBC security devices which are physically installed into the network and available for provisioning are identified by a **Registered** (as opposed to **Provisioned**) status. In addition, the **Install Device** icon ( ) is displayed only for those devices which have not yet been provisioned. E-SBC devices which have already been successfully provisioned display the **View Config** icon ( ).

3. Select the **Install Device** icon ( ) corresponding to the device you want to provision.
   The **Installation** pop-up window is displayed (Figure 4-1).

Note:	Unless the EMS and E-SBC are in the same box, devices will not automatically appear on the System Management screen. In order for a device to appear in the System Management screen, it must be added with the "**Add Device**" button (as described in the section in Chapter 3, titled, "Adding a E-SBC Device"). Once the device has been added this way, it will appear in the System Management screen in "**New**" state. After that, when the device is brought up (via the procedures in the Installation Guides), it will move into "**Registered**" state. The **Install Device** icon will only appear if the device is in **Registered** state. The Provisioned state is an intermediate state between the initial **Registered** state and the final Commissioned state. A device should only be in either the **Registered** state or Commissioned state at any given time, remaining in the **Provisioned** state for a short period of time during the transition from **Registered** to **Commissioned** state. Depending upon the state of a device, some options may not be available, such as the **Edit Device** icon that is not an available option for devices in the ***Registered*** state.

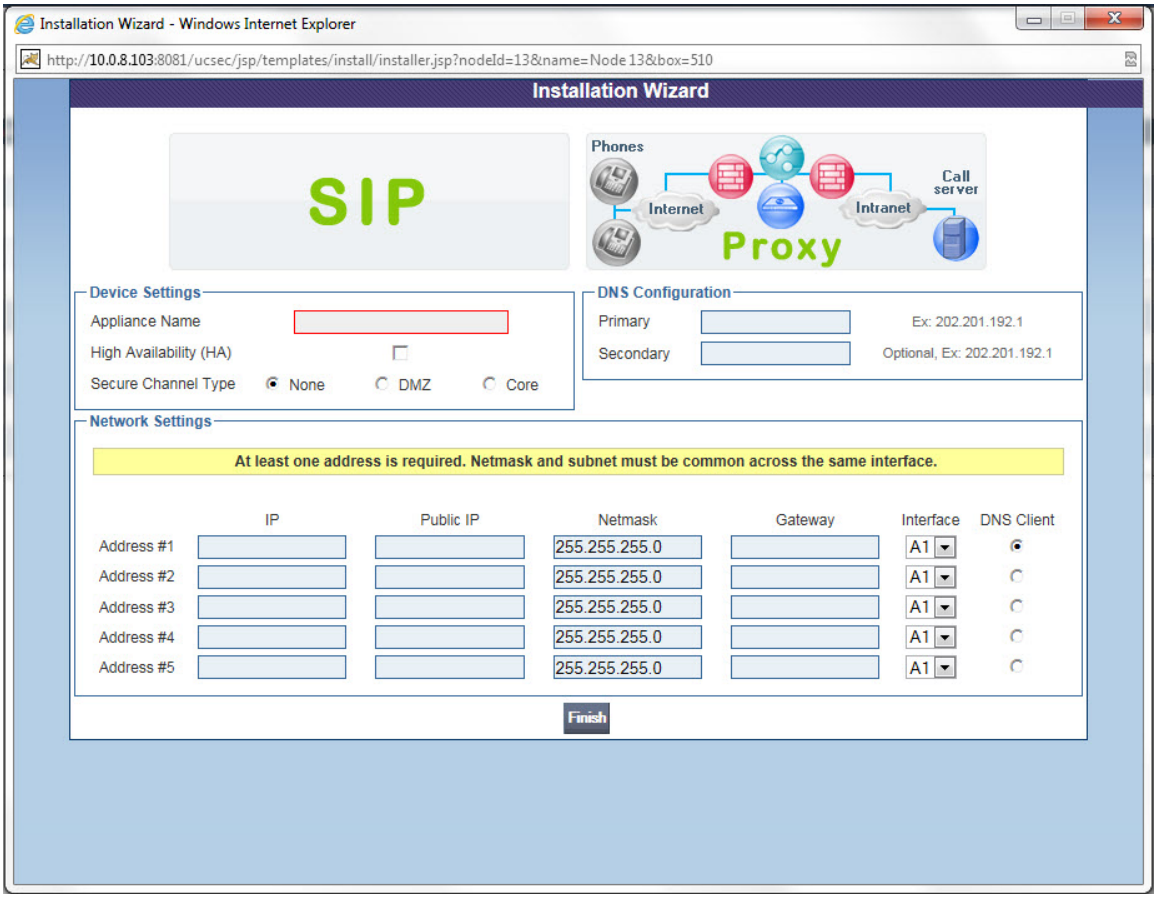


Figure 4-1. Installation Pop-up Window.

4. Enter an Appliance Name for the E-SBC security device being provisioned and its deployment settings (i.e., HA and Secure Channel Type).

Table 4-1 provides more complete descriptions of the selections to be made on this window.

Table 4-1. Installation Wizard Field Descriptions - Window 1.

Field	Description
Appliance Name	A descriptive name assigned to the E-SBC security device being provisioned. This name will subsequently be used as the device host name.
High Availability (HA)	A checkbox indicating that the E-SBC security device being provisioned will be part of a High-Availability (HA) pair. If checked (☑), a drop-down window will be displayed containing a list of HA partners as shown below. Click to select the desired HA partner. **Note: For HA configuration instructions, refer to the next section in this chapter titled, "E-SBC High Availability (HA) Configurations."** Device Settings High Availability (HA) ☑, failover to: IPCS510000005 Secure Channel Type ◉ None ○ DMZ ○ Core
Secure Channel Type	Radio button indicating whether or not this E-SBC security device will be part of a secure channel. Available selections are: **None** — This E-SBC device will not be communicating via a secure channel. **DMZ** — This E-SBC security device will be deployed in the enterprise DMZ to enable secure communications with another E-SBC security device deployed in the core. **Core** — This E-SBC security device will be deployed in the enterprise core to enable secure communications with another E-SBC security device deployed in the DMZ.
DNS Configuration	**DNS Configuration**
Primary	Primary
Secondary	Secondary
Network Settings	**Network Settings**
IP	IP is the actual IP address of the E-SBC device (whether it is publically reachable or not) that is being configured.
Public IP	Public IP is the publically-reachable IP address of the E-SBC security device being configured and is the IP address that the device will use to access the external network. If near-end NAT is not employed, the Public IP address may be the same as the IP (actual) address.
Netmask	The subnet mask of the E-SBC device being configured.
Gateway	The IP address of the device the E-SBC security device will use to send local network traffic to other networks.
Interface	A drop-down menu from which you select the physical interface of the E-SBC security device which will be used to interface to the external, public network (**A1**, **A2**, **B1**, and **B2**).
DNS Client	Select the **DNS Client** radio button next to the interface (normally A1) that is reachable by the DNS servers that were defined previously in the **Primary** and **Secondary** fields in the **DNS Configuration** area.

5. Click **Finish.**
   The **Final Installation** screen is displayed (Figure 4-2) informing you that the E-SBC security device is now installed, provisioned, and ready to be configured.

Caution!

In the **Final Installation** (Network Settings) screen that's displayed after selecting the **Finish** button, do not select the **Easy Config** button.

The **Easy Config** procedure is not applicable for E-SBC deployments. Instead, exit the **Final Installation** screen by selecting the X in the upper-right-hand corner of the screen, and then continue with the configuration.

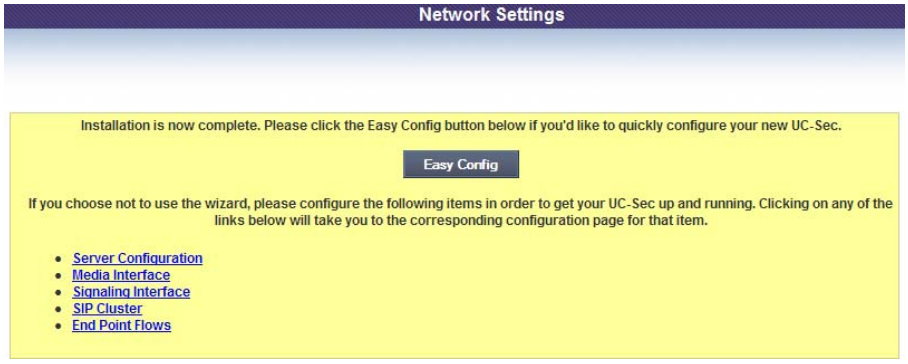


Figure 4-2. Final Installation Window

E-SBC High Availability (HA) Configurations

The Standard High Availability (HA) configuration (devices co-located) is performed from the System Management screen on two devices that have already been added using the **Add Device** function (described in the section in Chapter 3 titled, "*Adding a E-SBC Device*") and listed with a *Registered* status in the System Management screen, as shown in the example in Figure 4-3 below.

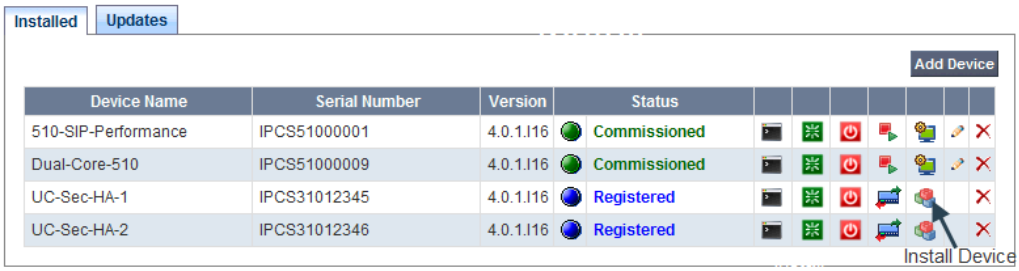


Figure 4-3. System Management Screen

1. Use the **Install Wizard** procedure (as described in the previous section in this chapter) by selecting the **Install Device** icon ( ) corresponding to the device you want to provision (see Figure 4-3 above) as the "***Active***" (primary) device.

Note:	As part of the Install Wizard design, the device you select here in Step 1 with the **Install Device** icon in the System Management screen (see Figure 4-3) will be automatically configured as the "**Active**" (primary) device. The device you select in the "**failover to**" drop-down list (**Error! Reference source not found.**) will be automatically configured as the "**Stand-By"** (secondary) device..

Selecting the **Install Device** icon ( ) will open the first Installation Wizard screen as shown in Figure 4-4 below.

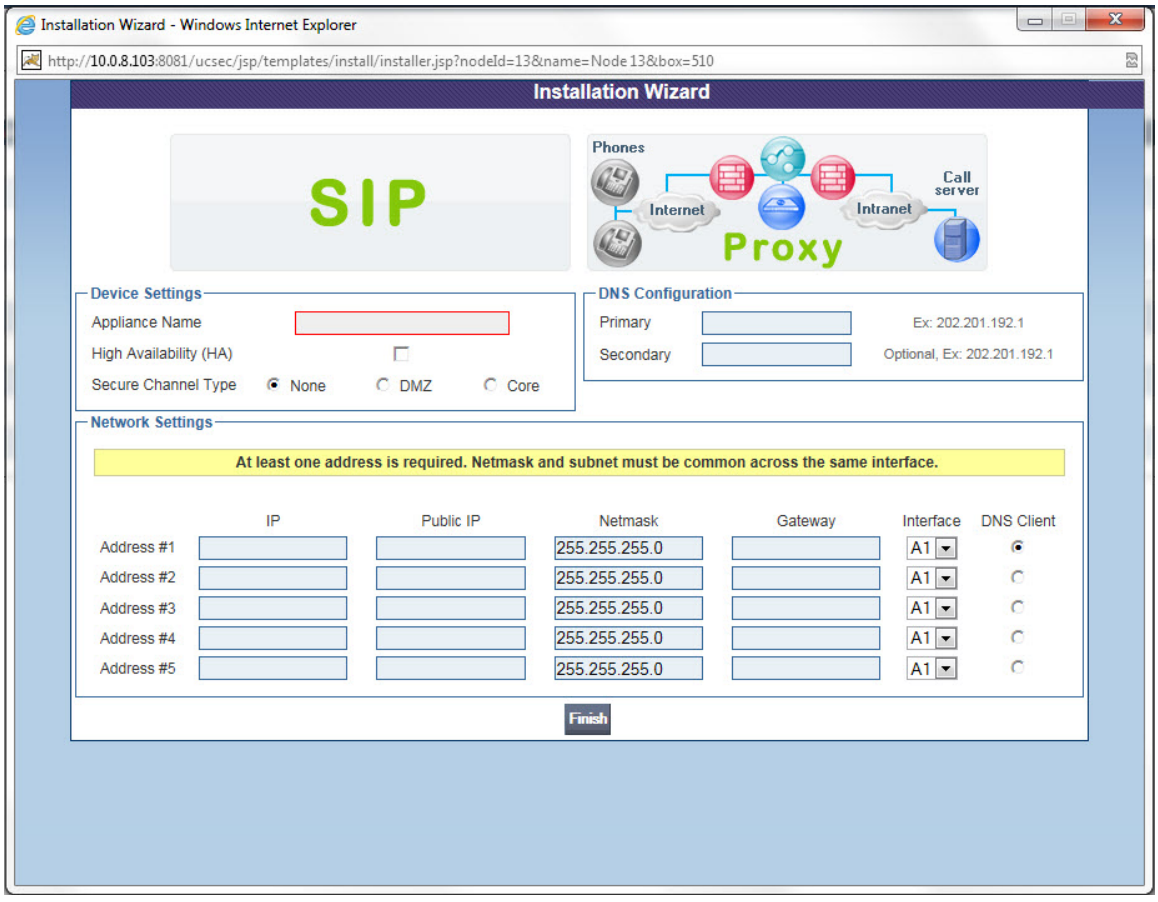


Figure 4-4. Installation Wizard Screen 1

2. Enter an Appliance Name for the E-SBC security device being provisioned and its deployment settings. Select the High Availability (HA) checkbox to display the drop-down list (Figure 4-5). and select the **Stand-By** (secondary) device serial number from the list.

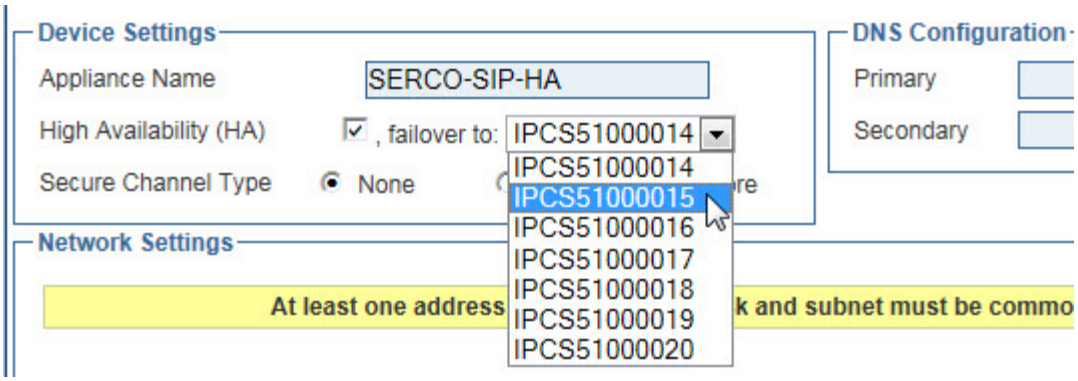


Figure 4-5. Failover To Drop-Down List

Note:	If the device you want to assign as the **Stand-By** device is not listed in the System Management screen, use the **Add Device** button (see the section in Chapter 3 titled, "**Adding a UC-Sec Device**") to add it.

3. Complete the required configuration information in Installation Wizard Screen and click **Finish** to continue with the configuration process. This will display a scrollable System Information screen similar to the examples shown in Figure 4-6 and in Figure 4-7 for Parts 1 and Part 2, respectively.

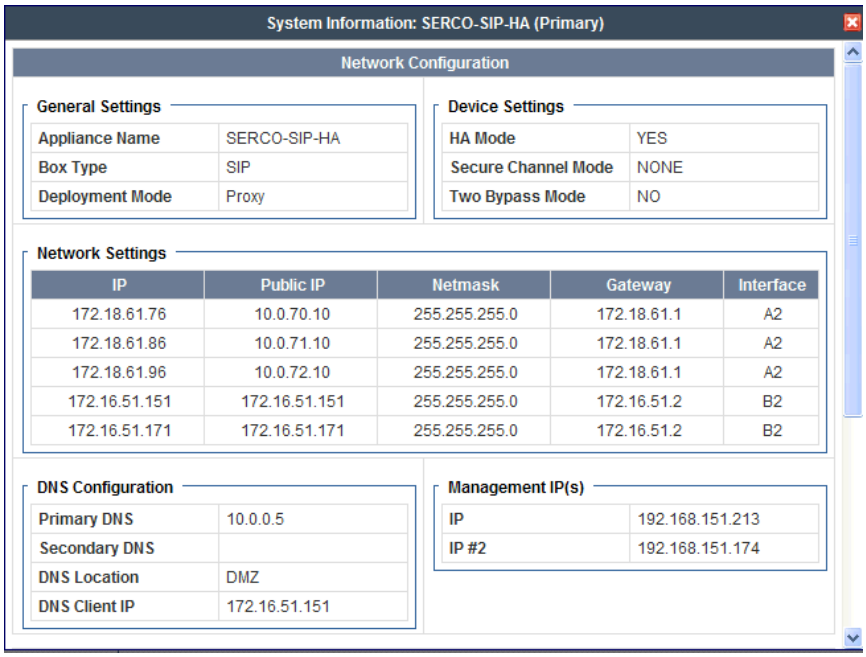


Figure 4-6. System Information Screen Part 1

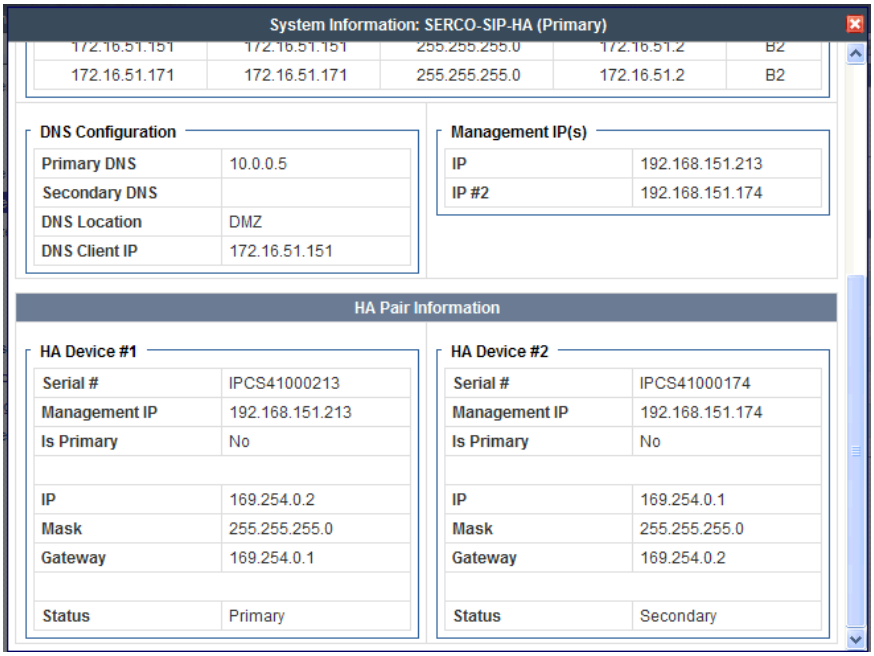


Figure 4-7. System Information Screen Part 2

Updating EMS Software

The **Element Management System** (EMS) or GUI interface can be upgraded when necessary using the **System Management** feature from the Task Pane. Use the following procedure to upgrade the E-SBC EMS.

Note:	Following a system upgrade, user should clear their browser cache before attempting to log in again. For instructions on clearing the browser cache, refer to the following link: http://www.google.com/support/accounts/bin/answer.py?hl=en&answer=32050

1. Select the **System Management** feature from the Task Pane.
2. The **System Management** screen is displayed.
3. Select the **Updates** tab.
4. The current EMS version and available upgrade options are displayed in the Content Area (Figure 4-8).
5. Verify the current EMS version in the **Version Information** portion of the tab display.
6. If the EMS is to be upgraded and the upgrade package has *not* already been uploaded to the EMS server, proceed to the procedure, Upgrade EMS from an Uploaded File.
7. If the EMS is to be upgraded and the upgrade package has already been uploaded to the EMS server, proceed to the procedure Upgrade EMS from a Local File.

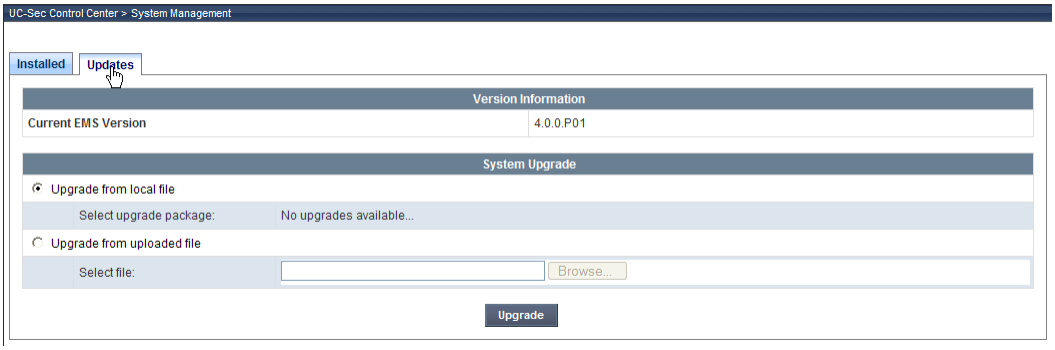


Figure 4-8. System Management Screen - Updates Tab Display.

Upgrade EMS from a Local File

1. Select the Upgrade from local file radio button from the System Upgrade portion of the tab display.
2. Select the upgrade file from the corresponding pull-down menu.
3. If no local upgrade packages are available, then the Select upgrade package: field will display No upgrades available. Proceed instead to the Upgrade EMS from an Uploaded File procedure.
4. Click Upgrade.
   The EMS software is upgraded. A series of informational pop-up windows will be displayed as the upgrade proceeds. A final pop-up window will be displayed to let you know when the upgrade is complete.

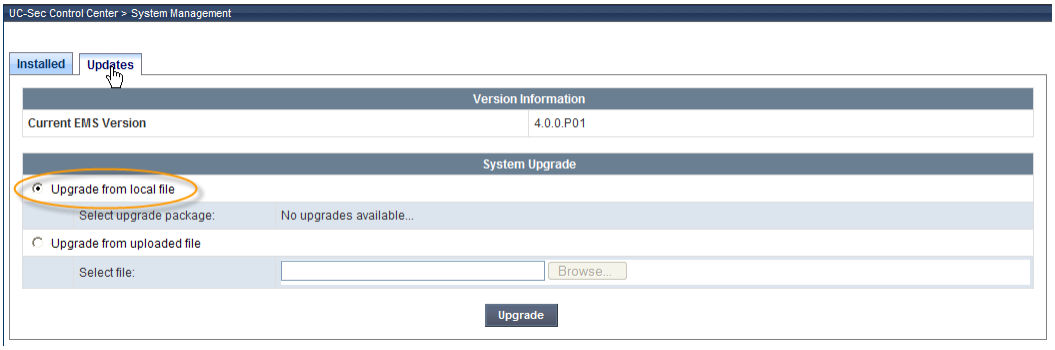


Figure 4-9. Upgrading the EMS from a Local File.

Upgrade EMS from an Uploaded File

1. Select the Upgrade from uploaded file radio button from the System Upgrade portion of the tab display.
2. Select the Browse button and search for upgrade package.
3. Click Upgrade.
   The EMS software is uploaded from your system to the EMS server, where it is automatically begins the upgrade procedure. A series of informational pop-up windows will be displayed throughout the upgrade process. A final pop-up window will be displayed to let you know when the upgrade is complete.

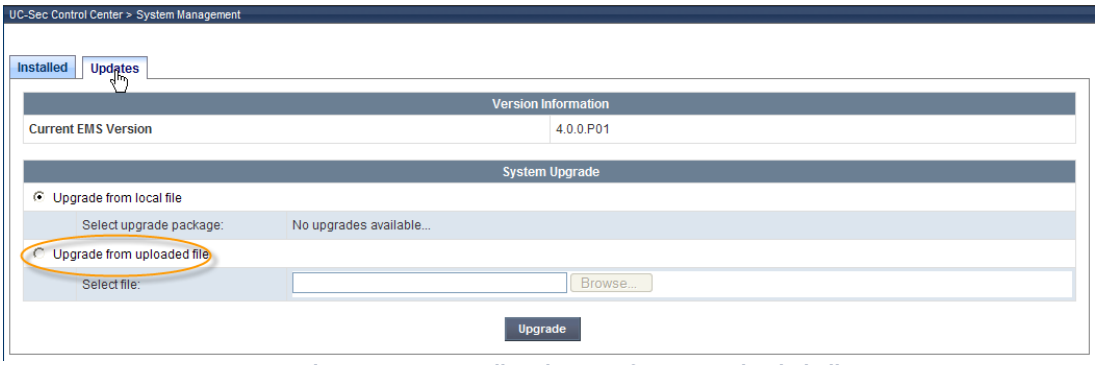


Figure 4-10. Upgrading the EMS from an Uploaded File.

Upgrade EMS – Non Service Affecting

Table 4- 2. EMS Upgrade – Non Service Affecting

Ref	Steps	Details
1.0	Upgrade EMS	
1.1	Log onto EMS as Administrator	Log onto the EMS GUI from Firefox.
1.2	Upload new E-SBC software	From GUI, click on System Management → Updates tab, select "Upgrade from uploaded file", click Browse, choose the file, and click Open.
1.3	Upgrade EMS	From GUI, click Upgrade. You may lose connectivity to the EMS during the upgrade.
1.3.1	Confirm EMS upgrade	Log onto the EMS GUI from Firefox. Click About in top right corner and confirm the version.
1.3.2	Back out	If EMS is unavailable or version information is inaccurate, initiate rollback (see Installation Guide)

Updating VIPER Signatures

When new scrubber packages or new VIPER signatures become available, an email is sent to the customers containing the following:

- An attachment which contains the rules SQL definitions in a tar.gz format signed with the secret signature
- The Package ID of the rules
- A description of the package
- The release date of the package
- The Vulnerability ID

Note:	The tar.gz file is the Scrubber package that is to be instated in the GUI from the Scrubber profile screen.

VIPER signatures are similar to Scrubber Packages, and are created by the VIPER team, and then packaged and released by the engineering team after testing.

Refer to the section titled, “Security Rules” in Chapter 5 and the section titled, “*Protocol Scrubber” in Chapter 7.*

Domain Policy Administration 5

This chapter explains how to create, manage, and assign domain policies (also referred to as *Unified Communications Policies*). These policies allow you maintain control over call flows entering or leaving the enterprise based upon a wide range of conditions and parameters.

Note Domain Policies are only applicable to SIP networks.

Governing Unified Communications with Domain Policies

Purpose

UC Policies allow enterprise UC administrators the flexibility to govern their Unified Communications through the enforcement of business rules. Different rules may be applied based on user identity, domain affiliation, network identity, time of day, and time of week.

How They Work

UC Policies have two high level concepts: **flows** and **domain policies**. When a packet is received by E-SBC, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. Please refer to Figure 5-1 below.

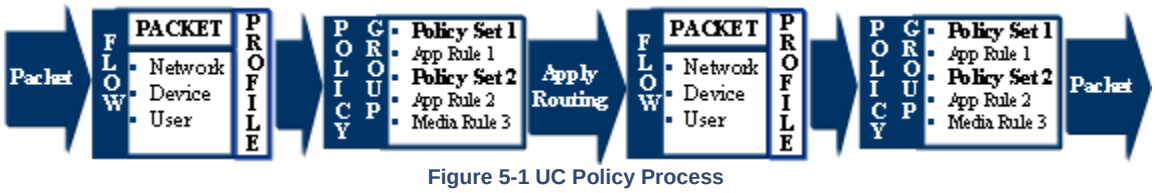


Figure 5-1 UC Policy Process

Flows

The packet field values configured in flows are matched to categorize a packet so that the appropriate policy can be applied. The flows are matched starting with the highest order (lowest numerical value). The most particular flows should be used at the top, while those lower in the order may be more general.

Endpoint Flows

- Used to determine signaling endpoints in order to apply the appropriate endpoint policy

Server Flows

- Identify SIP servers

Session Flows

- Determine the media (audio/video) sessions in order to apply the appropriate session policy

Domain Policies

End Point Policy Groups

- An ordered list of policy sets. The policy set with the highest order (lowest numerical value) is applied if Time of Day (ToD) matches. Smaller time windows should be used at the top, with larger time windows further down the order.

Policy Set

- A set of application, border, media, security, signaling, and ToD rules

Rules

- Determine the processing method, privileges, and authentication method of packets.

Session Policies

- Applied based on the source and destination of a media session. e.g. which codec to be applied to the media session between its source and destination

Profiles

Profiles are very similar to polices, but they are usually dependent on deployment. For example, they are dependent on which call server is being used, IP addresses being used, SIP domains, normal traffic behavior, etc. This differs from policies, in that policies are based on business and compliance requirements.

Detailed visual examples of matching flows and applying policies for securing a SIP Trunk with E-SBC are provided in Figure 5-2.

Example: Call Server with E-SBC Securing SIP Trunk

(Example is viewable in Figure 5-2.)

To Be Created by User

- End Point Policy Groups
  - Call Server Policy Group
  - Trunk Server Policy Group
- Endpoint Flows
  - Call Server to E-SBC Flow (Reverse used in opposite direction)
  - Trunk Server to E-SBC Flow (Reverse used in opposite direction)
- Session Policies
  - Trunk Server/Call Server SIP Phone Session Policy
- Session Flows
  - Trunk Server to Call Server SIP Phone Flow (bidirectional)

End Point Policy

Incoming

1. Packet sent received by E-SBC.
2. E-SBC determines flow.
3. Call Server to E-SBC Flow points to Call Server Policy Group; E-SBC applies policy and routs packet to determined destination.
4. Trunk Server to E-SBC REVERSE Flow points to Trunk Server Policy Group; E-SBC applies policy.
5. Packet sent to Trunk Server.

Outgoing

6. Packet received by E-SBC
7. E-SBC determines Flow.
8. Trunk Server to E-SBC Flow Points to Trunk Server Policy Group; E-SBC applies policy and routs packet to determined destination.
9. Call Server to E-SBC REVERSE Flow points to Call Server Policy Group; E-SBC applies policy.
10. Packet sent to Call Server.

Session Policy

1. Packet received by E-SBC.
2. E-SBC determines Flow.
3. Trunk Server to Call Server SIP Phone Session Flow points to Trunk Server/Call Server SIP Phone Session Policy; E-SBC applies policy.
4. Packet sent.

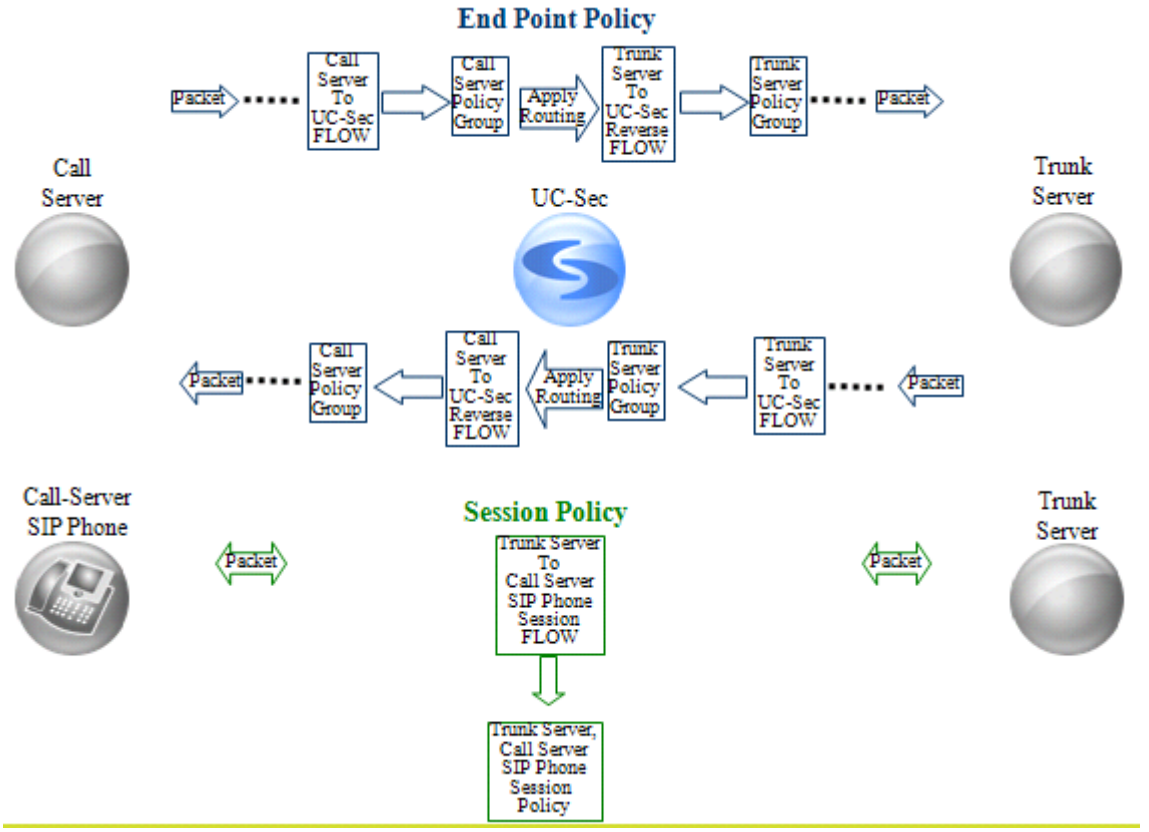


Figure 5-2 Securing a SIP Trunk

Configuring Rules and Policies

This section provides an overview of the process of configuring Rules and Policies, including descriptions of the E-SBC Architecture, the associations of Rules and Policies, an introduction to Rules and Profiles, creating Policy Groups, creating Session Policies, and points to remember regarding the configuration process.

Note:	**This section only provides a brief introduction to Rules, Profiles, and Policies. Detailed instructions for creating and editing each of the individual types of Rules, Profiles. Policies, and Policy Groups are provided in their respective sub-sections later on in this Chapter.**

Architecture

Figure 5-3 provides an illustration the E-SBC platform and associated network architecture.

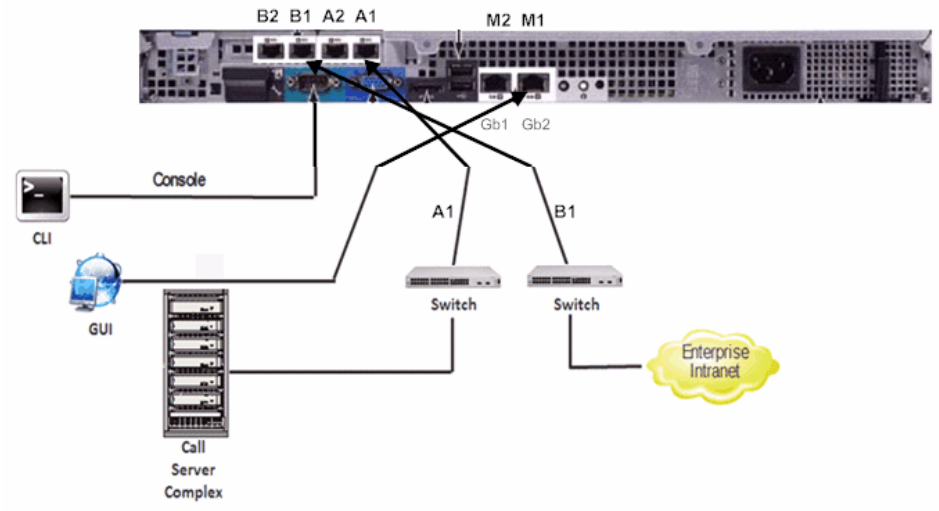


Figure 5-3 E-SBC Architecture

Rules and Policies Associations

Three Rules and Policies Associations drawings are provided in this section to illustrate the following:

- Figure 5-4 lists the Task Pane menu Feature selections ─ "Domain Policies" and "Global Profiles," along with their associated submenu Function selections for the categories of Rules, Profiles, and Policies.
- Figure 5-5 shows the types of signaling and media flows, with their associated policies and policy groups and sets, and with the elements and applications they control.
- Figure 5-6 illustrates the Session and Subscriber Flows along with their associated Policies.

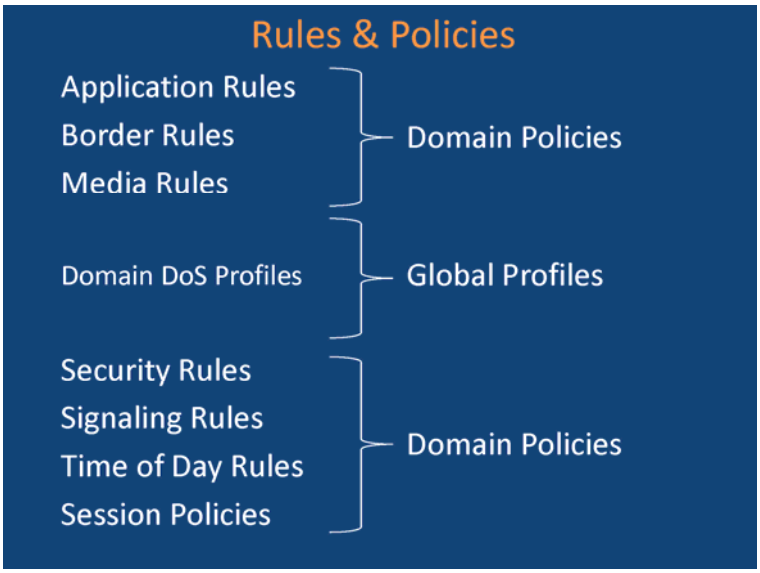


Figure 5-4 Rules and Policies Associations 1

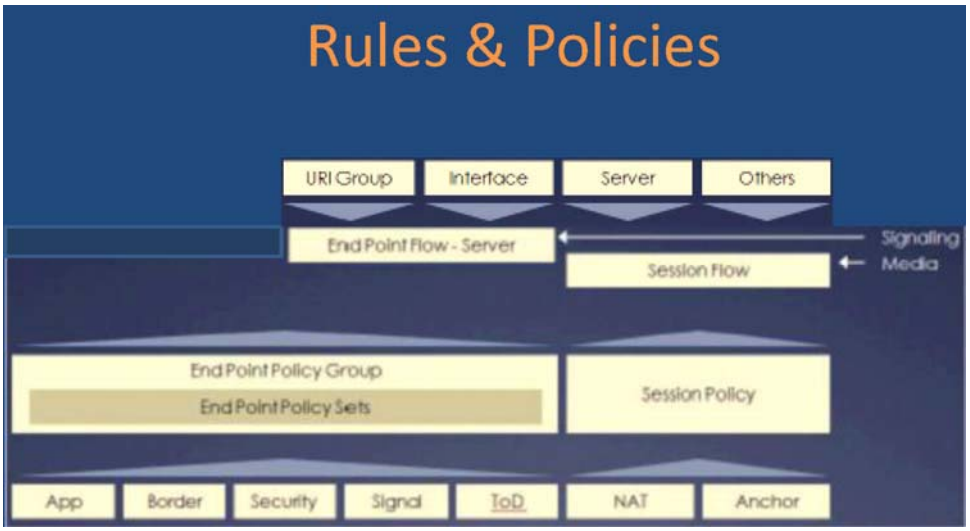


Figure 5-5 Rules and Policies Associations 2

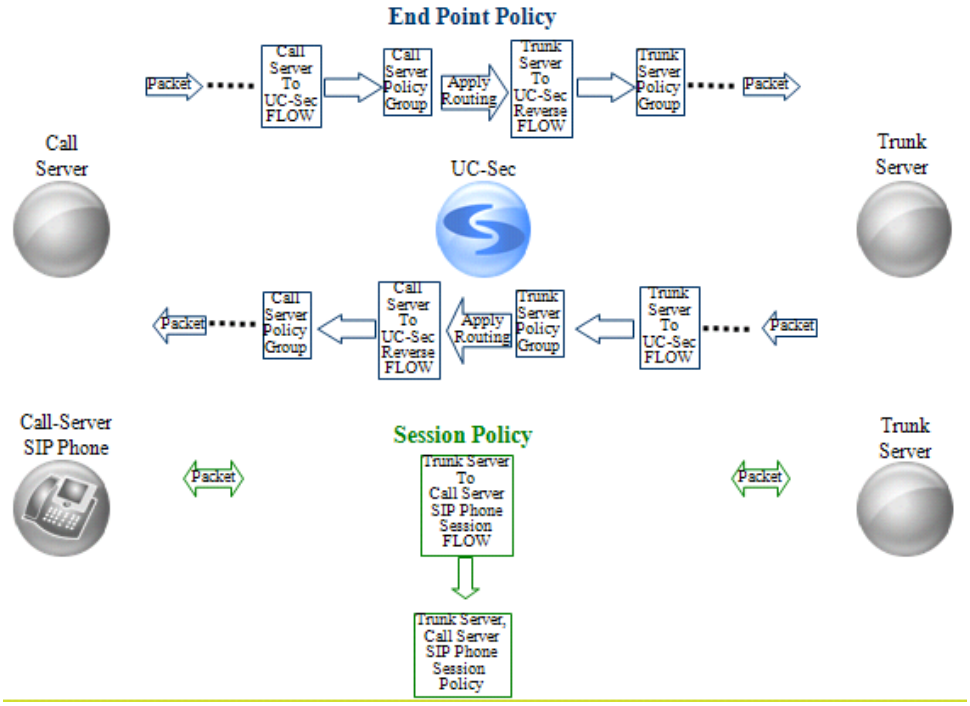


Figure 5-6 Rules and Policies Associations 3

Rules and Profiles Configuration Steps Checklists

This section provides quick-start configuration checklists for each of the following Rules and Profiles:

- Application Rules
- Border Rules
- Media Rules
- Domain DoS Rules
- Security Rules
- Signaling Rules
- Time of Day Rules

Note: **This section only provides brief configuration checklists for Rules and Profiles. Detailed instructions for creating and editing each of the individual types of Rules and Profiles are provided in their respective sub-sections later in this Chapter.**

Application Rules Checklist

Applications Rules are used to police SIP applications and rates.

1. Select: **Domain Policies > Application Rules**
   Application Rule Configuration Example
2. Add Rule
3. Name = App-*xxxx*
4. Allow bidirectional voice, video, IM at arbitrary rates
5. Finish

Border Rules Checklist

Border Rules are used to establish NAT traversal (usually line side).

1. Select: **Domain Policies > Border Rules**
   Border Rule Configuration Example
2. Add Rule
3. Name = Border-*xxxx*
4. Enable NAT
5. Check SIP and SDP published IP checkboxes
6. Finish

Media Rules Checklist

Media Rules are used to implement media-oriented security.

1. Select: **Domain Policies > Media Rules**
   Media Rule Configuration Example
2. Add Rule
3. Name = Media-*xxxx*
4. Select a media type (encrypted)
5. Select MAD
6. Select Media Silencing

7. Change Audio precedence to immediate
8. Finish

Domain DoS Profiles Checklist

Domain DoS Profiles are used to define the server-bound DoS counters used in Security Rules.

1. Select: **Global Profiles > Domain DoS Profile**
   Domain DoS Profile Configuration Example
2. Add Profile
3. Name = DoS-*xxxx*
4. Users = 1000
5. Client type = Other
6. Finish

Security Rules Checklist

Applications Rules are used to implement signaling-oriented security.

1. Select: **Domain Policies > Security Rules**
   Security Rule Configuration Example
2. Add Rule
3. Name = Secure-*xxxx*
4. Select **Enabled** from the dropdown.
5. Realm = dummy.com
6. Enable Authentication checking REGISTER, INVITE, BYE, and REFER
7. Select URI for compliance.
8. Enable Scrubber with Package 2
9. Enable Domain DoS with DoS-*xxxx*
10. Finish

Signaling Rules Checklist

Signaling Rules are used to change the behavior and QoS of SIP signaling and replies.

1. Select: **Domain Policies > Signaling Rules**
   Signaling Rule Configuration Example
2. Add Rule
3. Name = Signal-*xxxx*
4. Block Option Request Headers with 403 Forbidden
5. Finish

Time of Day Rules Checklist

Applications Rules are used to apply different rules at different times in a policy set.

1. Select: **Domain Policies > Time of Day Rules**
   Time of Day Rule Configuration Example
2. Add Rule
3. Name = Time-*xxxx*

4. Start date = Now
5. End date = Never
6. Time = All Day
7. Recurrence = Every Weekend
8. Finish

Creating a Policy Group Checklist

The End-Point Policy Group feature allows you to create *Policy Sets* and *Policy Groups*. A *Policy Set* is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and Time of Day (ToD).

A *Policy Group* is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of E-SBC security features to very specific types of SIP signaling messages traversing through the enterprise.

Note: **For detailed information on creating a Policy Group, refer to the section later on in this Chapter titled, "End-Point Policy Groups."**

Session Policies Checklist

Session Policies are used to prioritize media codecs, and select media anchoring.

1. Select: **Domain Policies > Session Policies**
   Session Policy Configuration Example
2. Name = Pol-*xxxx*
3. Codec Priority = 1) G.711 2) G.722
4. Check Media Anchoring
5. Finish

Note: **For detailed information on creating Session Policies, refer to the section later on in this Chapter titled, "Session Policies."**

Points to Remember

- Rules are grouped in Policy Sets
- Policy Sets are grouped in End-Point Policy Groups
- End-Point Policy Groups are assigned to End-Point Flows.
  Refer Figure 5-7.
- Session Policies control codec negotiation, and media anchoring.
- Session Policies are assigned to Session Flows.
  Refer to Figure 5-8.

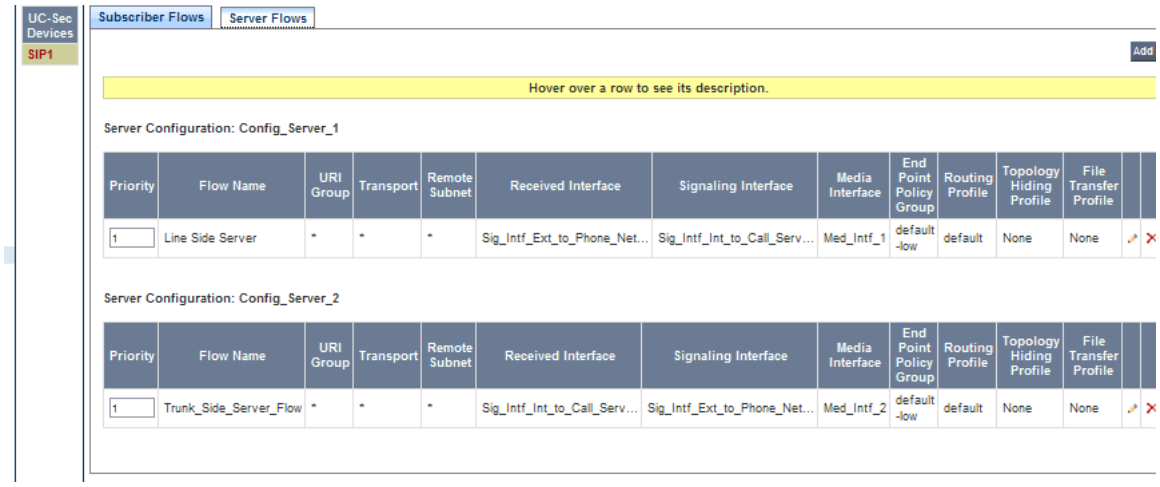


Figure 5-7 End-Point Policy Groups Assigned to Server Flows

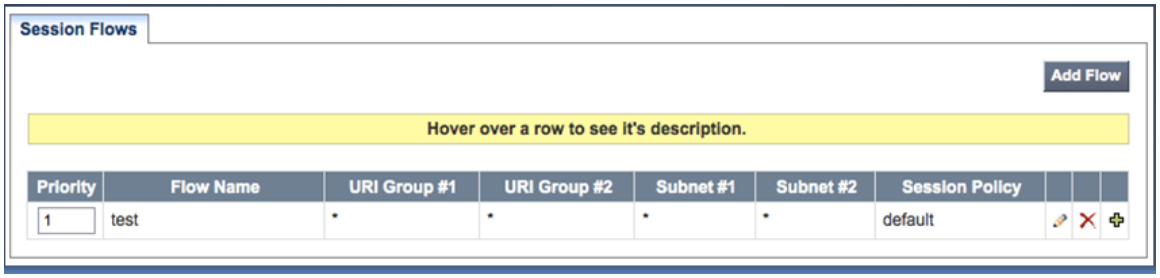


Figure 5-8 Session Policies Assigned to Session Flows

Managing Domain Policies

Application Rules

Application Rules allow you to define which types of SIP-based Unified Communications (UC) applications the E-SBC security device will protect: voice, video, and/or Instant Messaging (IM). In addition, you can determine the maximum number of concurrent voice and video sessions your network will process on order to prevent resource exhaustion.

Creating a New Application Rule

Use the following procedure to create a new **Application Rule**.

Caution! A default Application Rule set named **default** is provided by Sipera. Editing this rule set is not recommended, as improper configuration may cause subsequent calls to fail.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Application Rules** function from the **Domain Policies** feature from the Task Pane. Existing **Application Rule** sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Application Rule set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-9.

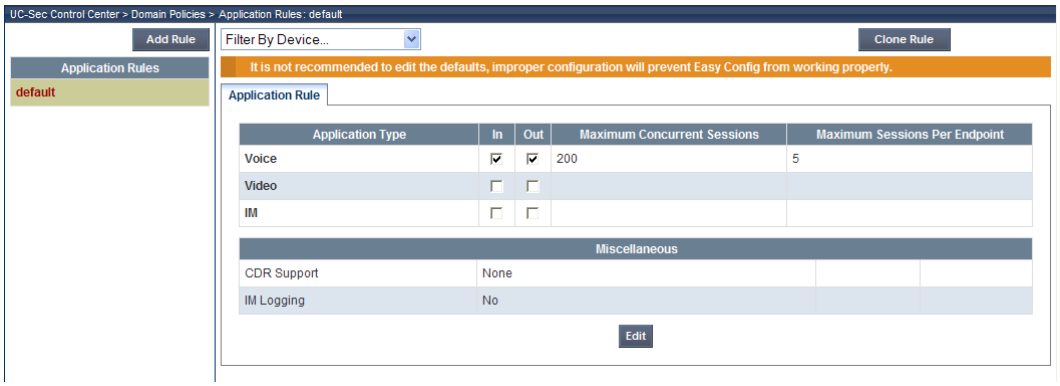


Figure 5-9 Application Rules Screen.

3. Select **Add Rule** from the Applications Pane.
   The Add Application Rule pop-up window is displayed (Figure 5-10).

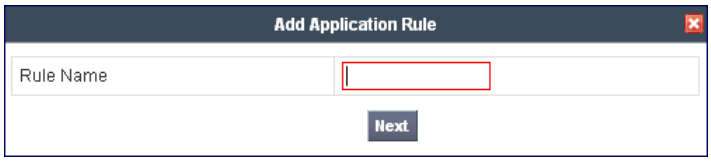


Figure 5-10 Add Application Rule Pop-up Window.

4. Enter a name for the new **Application Rule** and select **Next**.
   The Add Application Rule pop-up window is displayed (Figure 5-11).

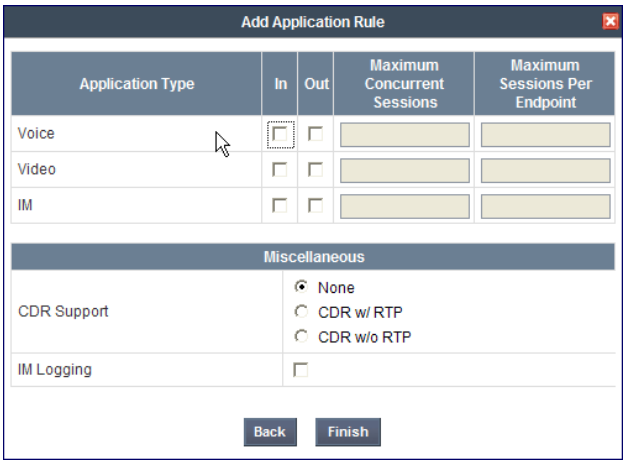


Figure 5-11 Add Application Rule Pop-up Window.

5. Enter the requested information into the appropriate fields.
   Table 5-1 describes each user-definable field displayed in the Add Application Rule pop-up window. Selecting the Cancel icon cancels the operation and closes the window without saving. Selecting Back redisplays the Add Application Rule pop-up window.

Table 5-1 Add Application Rule Pop-up Window Field Descriptions.

Field	Description
Application Type	The type of SIP application for which this **Application Rule** is being configured: **Voice**, **Video**, and **IM**.
In	Checkbox indicating that this **Application Rule** will apply to traffic (**Voice**, **Video**, and/or **IM**) entering the enterprise network.
Out	Checkbox indicating that this **Application Rule** will apply to traffic (**Voice**, **Video**, and/or **IM**) originating from within the enterprise network.
Maximum Concurrent Sessions	The maximum number of concurrent application sessions that will be allowed to be active for the selected application type (**Voice**, **Video**, and **IM**). Additional application requests will be blocked if this threshold is exceeded.
Maximum Sessions per Endpoint	The maximum number of concurrent application sessions that will be allowed to be active for the selected application type (**Voice**, **Video**, and **IM**) for any single end-point. Additional application requests will be blocked if this threshold is exceeded.
Miscellaneous	

Field	Description
CDR Support	**None:** Call detail records will not be provided. **Without RTP:** Call detail records with change in call states will be provided. **With RTP:** Call detail records with call quality and call statistics will be provided in addition to change in call states.
IM Logging	Enables the **IM Logging** feature.

6. Select **Finish**.
   The new Application Rule appears in the Application Pane (Figure 5-12).

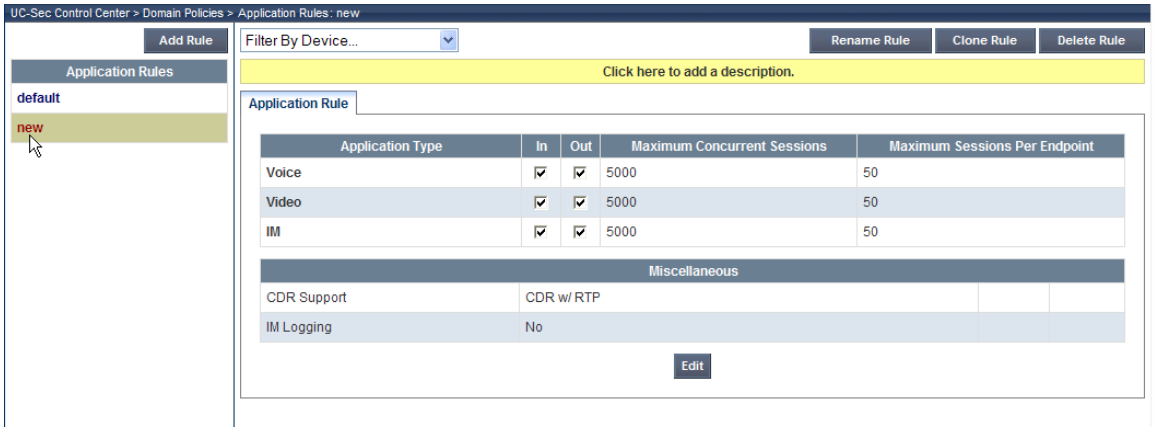


Figure 5-12 New Application Rule Display.

Cloning an Existing Application Rule

Use the following procedure to make an exact copy (clone) of an existing **Application Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Application Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing rule sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Application Rule set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-9.
3. In the Application Pane, select the **Application Rule** you want to clone (Figure 5-13).
4. Select **Clone Rule**.
   The **Clone Application Rule** pop-up window is displayed (Figure 5-14).
5. Enter a name for the new **Application Rule** and select **Finish** to save your changes or **Cancel** to cancel the cloning operation and close the window without saving.
   The Application Rule screen is redisplayed, showing the cloned Application Rule (Figure 5-15).

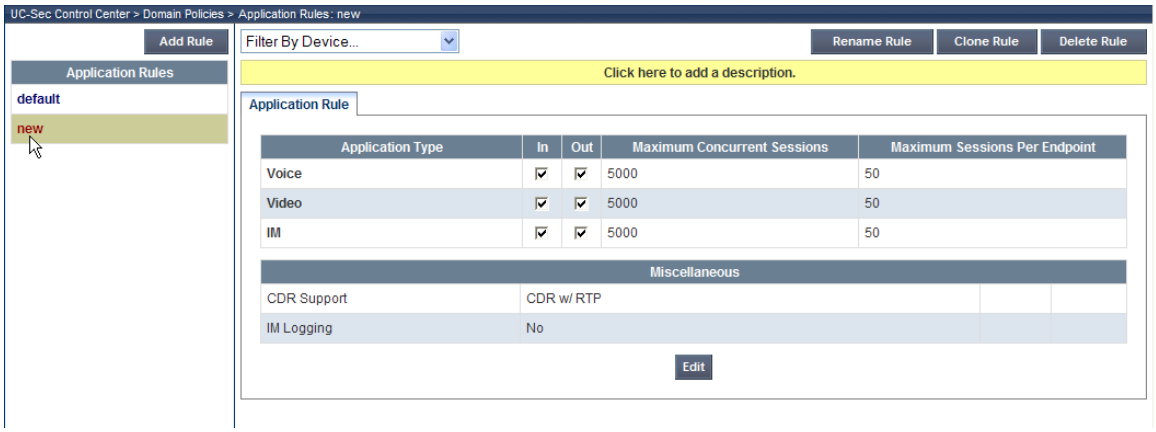


Figure 5-13 Selecting an Existing Application Rule.

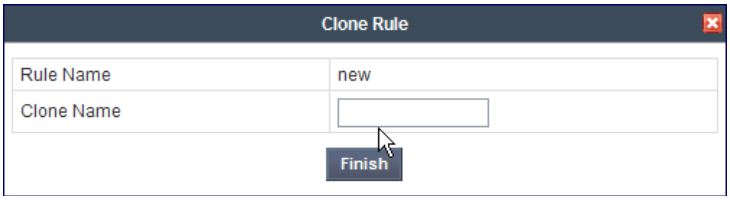


Figure 5-14. Clone Application Rule Pop-up Window.

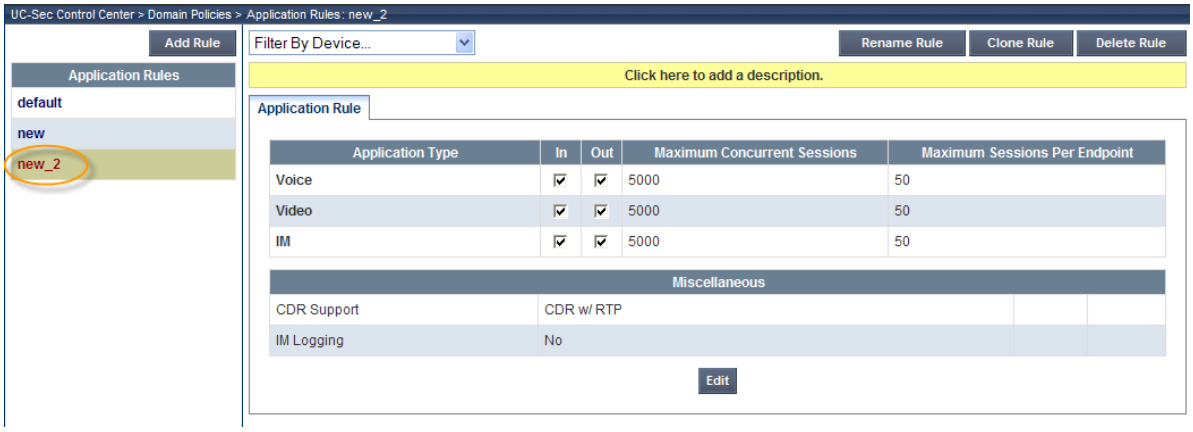


Figure 5-15 Updated Application Rules Screen.

Editing an Existing Application Rule

Use the following procedure to edit an existing **Application Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Application Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing rule sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Application Rule set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-9.
3. In the Application Pane, select the **Application Rule** you want to edit (Figure 5-13).
4. Select **Edit**.

The **Editing Rule** pop-up window is displayed (Figure 5-16).

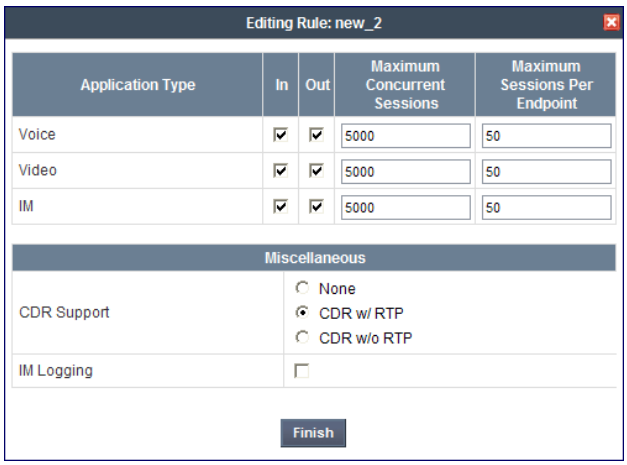


Figure 5-16. Edit Application Rule Pop-up Window.

5. Edit the desired fields and select **Finish** to save your changes or **Cancel** to revert to the previous values without saving.

If necessary, refer back to Table 5-1 for a description of each field.

Note:	The CDR files, which are generated based on the settings in the CDR Support area of the Edit Application Rule pop-up window above, can be viewed on the CDR Listing tab in the Advanced Options screen accessed from the Troubleshooting feature in the Task Pane. Refer to the section titled, "Viewing a CDR File" in Chapter 6 of this document.

Renaming an Existing Application Rule

Use the following procedure to rename an existing **Application Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Application Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing rule sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Application Rule set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-9.
3. In the Application Pane, select the **Application Rule** you want to rename.
4. Select **Rename Rule**.
   The **Rename Application Rule** pop-up window is displayed (Figure 5-17).
5. Enter a name for the **Application Rule** and select **Finish** to save your changes or **Cancel** to cancel the renaming operation and close the pop-up window without saving.

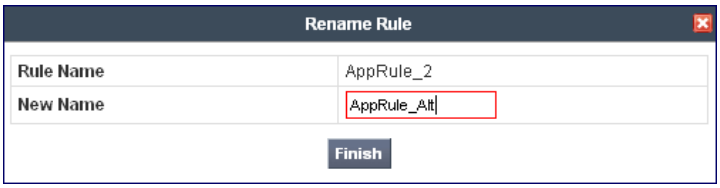


Figure 5-17. Rename Application Rule Pop-up Window.

Deleting an Existing Application Rule

Use the following procedure to delete an existing **Application Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Application Rules** function from the **Domain Policies** feature from the Task Pane.
   Existing rule sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Application Rule set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-9.
3. In the Application Pane, select the **Application Rule** you want to delete (Figure 5-13).
4. Select **Delete Rule**.
   A pop-up window is displayed similar to that shown in Figure 5-18 asking you to confirm your request to delete the Signaling Rule.

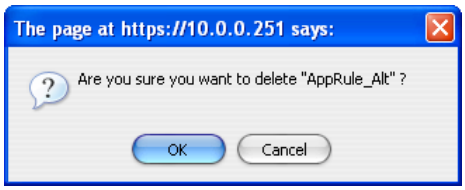


Figure 5-18. Delete Confirmation Pop-up Window.

5. Select **OK**.
   The **Application Rule** is deleted.

Border Rules

Border Rules allow you control NAT Traversal.

The NAT Traversal feature allows you to determine whether or not call flow through the DMZ needs to traverse a firewall and the manner in which pinholes will be kept open in the firewall to accommodate traffic.

Creating a New Border Rule

Use the following procedure to create a new **Border Rule**.

> **Caution!** A default Media Rule set named **default** is provided by Sipera. Editing this rule set is not recommended, as improper configuration may cause subsequent calls to fail.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Border Rules** function from the **Domain Policies** feature from the Task Pane. Existing **Border Rule** sets are displayed in the Application Pane in the Rules section, which defaults to the **NAT Traversal** tab display (Figure 5-19).

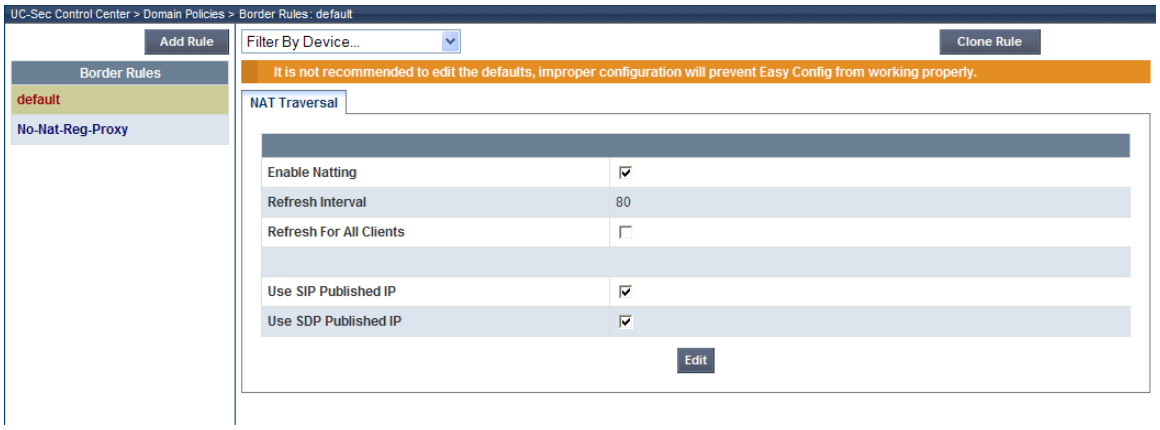


Figure 5-19 Border Rules Screen.

3. Select **Add Rule** from the Applications Pane.
   The Add Border Rule pop-up window is displayed (Figure 5-20).

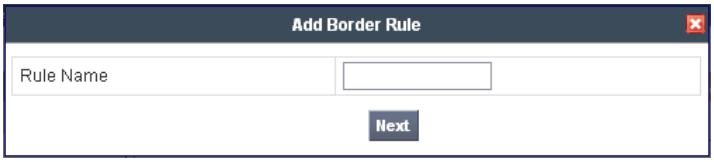


Figure 5-20. Add Border Rule Pop-up Window.

4. Enter a name for the new **Border Rule** and select **Next**.
   The Add Border Rule pop-up window is displayed (Figure 5-21).

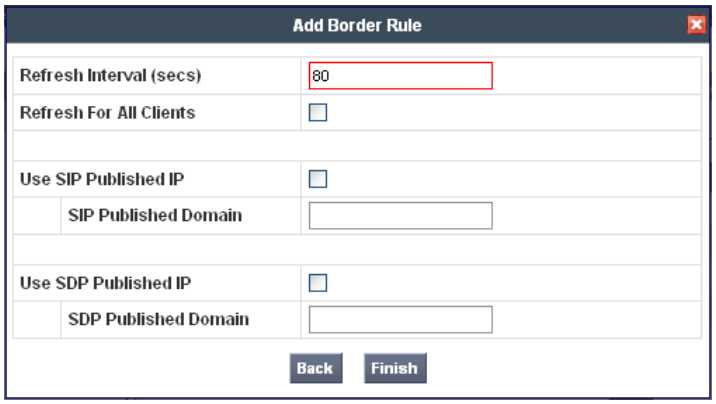


Figure 5-21. Add Borer Rule Pop-up Window.

5. Provide the requested information into the appropriate fields.
   Table 5-2 describes each user-definable field displayed in the Add Border Rule pop-up window. Selecting the **Cancel** icon cancels the operation and closes the window without saving.

Table 5-2 Add Border Rule – Topology Hiding and Learning Mode Pop-up Window Field Descriptions.

Field	Description
Refresh Interval (Sec)	The interval, in seconds, determining the frequency with which the far-end NAT device is refreshed.
Refresh for all Clients	Checkbox which enables (checked) or disables (unchecked) refreshing of all the clients registered through E-SBC.
Use SIP Published IP	Checkbox which determine whether or not the **Signaling IP** addresses of the enterprise call server and SIP phones as defined on the **Signaling Interface** tab of the **Signaling Interface** function (found under the **Device Specific Settings** feature) are used instead of the respective **SIP Published Domain**. If checked (), the **SIP Published Domain** field is inactivated and the published **Signaling IP** address is used to address the enterprise call server and SIP phones. If unchecked (), the **SIP Published Domain** field is activated and the published **Signaling IP** address not used; the **SIP Published Domain** is used instead to address the enterprise call server and SIP phones.
SIP Published Domain	The domain name of the enterprise call server and SIP phones. This field is only activated if the **Use SIP Published IP** is checked ().

Field	Description
User SDP Published IP	Checkbox which determine whether or not the **Media IP** addresses of the enterprise call server and SIP phones as defined on the **Media Interface** tab of the **Media Interface** function (found under the **Device Specific Settings** feature) are used instead of the respective **SDP Published Domain**. If checked (☑), the **SDP Published Domain** field is inactivated and the published **Media IP** address is used. If unchecked (☐), the **SDP Published Domain** field is activated and the published **Media IP** address not used; the **SDP Published Domain** is used.
SDP Published Domain	The domain name of the enterprise call server and SIP phones. This field is only activated if the **Use SDP Published IP** is checked (☑).

6. Select **Finish**.
   The new **Border Rule** is completed and added to the **Border Rules** section of the Application Pane (Figure 5-22).

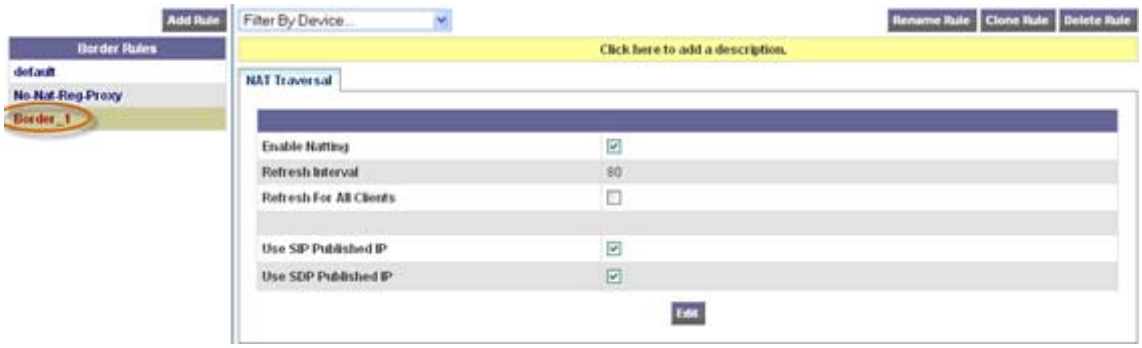


Figure 5-22 Updated Border Rules Screen.

Cloning a Border Rule

Use the following procedure to make an exact copy (clone) of an existing **Border Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Border Rules** function from the **Domain Policies** feature from the Task Pane.
3. Existing rule sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Border Rule set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-19.
4. In the Application Pane, select the **Border Rule** you want to clone.
5. Select **Clone Rule**.
6. The **Clone Rule** pop-up window is displayed (Figure 5-23).

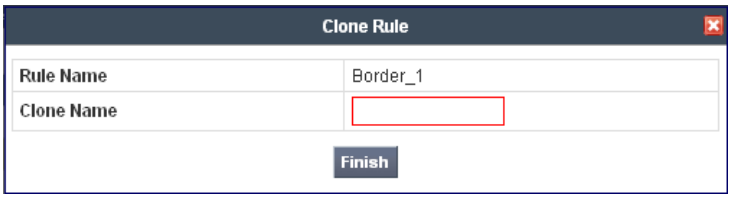


Figure 5-23. Clone Border Rule Pop-up Window.

7. Enter a name for the new **Border Rule** and select **Finish** to save your changes or **Cancel** to cancel the cloning operation and close the window without saving.
   The Border Rule screen is redisplayed (Figure 5-24), showing the cloned Border Rule.

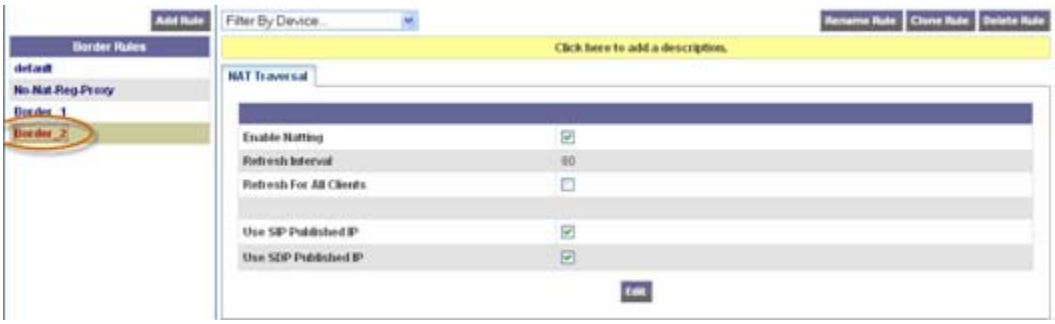


Figure 5-24 Updated Border Rule Screen.

Editing an Existing Border Rule

Use the following procedure to edit an existing **Border Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Border Rules** function from the **Domain Policies** feature from the Task Pane. Existing rule sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Border Rule set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-19.
3. In the Applications Pane, select the **Border Rule** set you want to edit.
   The parameters for that Border Rule set will be displayed in the Content Area.
4. Select **Edit**. An editable pop-up window will be displayed, similar to that shown in Figure 5-25.
5. Edit the desired fields and select **Finish** to save your changes or **Cancel** to cancel the operation and close the window without saving.

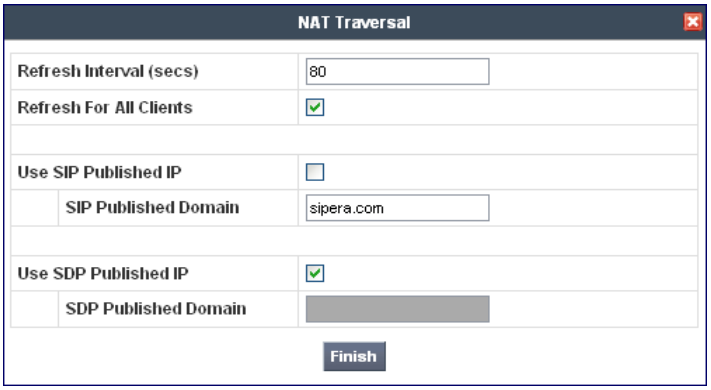


Figure 5-25 NAT Traversal Pop-up Window.

Renaming an Existing Border Rule

Use the following procedure to rename an existing **Media Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Border Rules** function from the **Domain Policies** feature from the Task Pane. Existing rule sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Border Rule set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-19.
3. In the Application Pane, select the **Border Rule** you want to rename.
4. Select **Rename Rule**.
   The **Rename Border Rule** pop-up window is displayed (Figure 5-26).
5. Enter a name for the **Border Rule** and select **Finish** to save your changes or **Cancel** to cancel the renaming operation and close the pop-up window without saving.

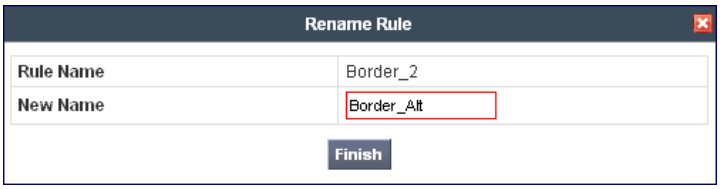


Figure 5-26. Rename Border Rule Pop-up Window.

Deleting an Existing Border Rule

Use the following procedure to delete an existing **Media Rule** set.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Border Rules** function from the **Domain Policies** feature from the Task Pane.
3. Existing rule sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Border Rule set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-19.
4. Select the **Border Rule** you want to delete.
5. Select **Delete Rule**.
6. The Delete Confirmation pop-up window is displayed (Figure 5-27).

7. Select **OK**.
8. The Border Rule set is deleted and the **Border Rules** screen is redisplayed.

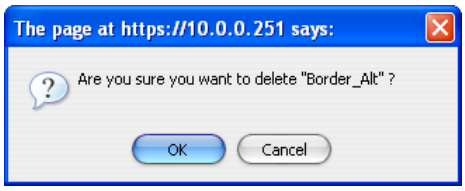


Figure 5-27. Delete Confirmation Pop-up Window.

Media Rules

Media Rules allow you to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the E-SBC security product.

Creating a New Media Rule

Use the following procedure to create a new **Media Rule**.

Caution! A default Media Rule set named **default** is provided by Sipera. Editing this rule set is not recommended, as improper configuration may cause subsequent calls to fail.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Media Rules** function from the **Domain Policies** feature from the Task Pane. Existing **Media Rule** sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Media Rule set are displayed in the Content Area of the E-SBC Control Center as shown in the Media Rules information screen (Figure 5-28).

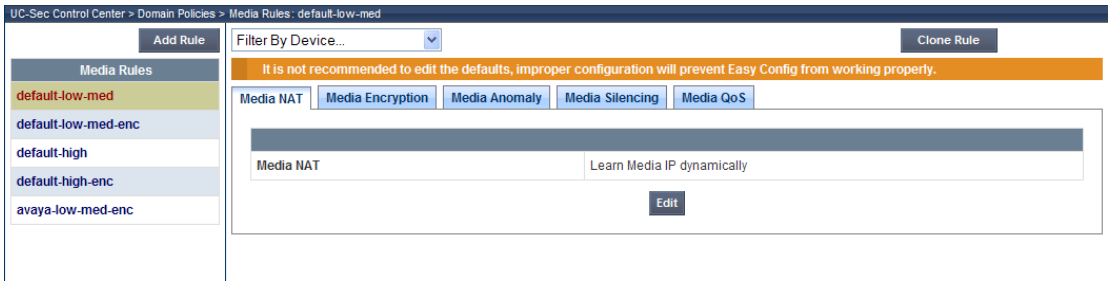


Figure 5-28. Media Rules Information Screen.

3. Select **Add Rule** from the Applications Pane.
   The first Add Media Rule pop-up window (Figure 5-29) is displayed.

Figure 5-29. Add Media Rule Pop-up Window 1.

4. Enter a name for the new **Media Rule** and select **Next**.
5. Select Media NAT settings and select **Next**.
6. A second Add Media Rule pop-up window is displayed (Figure 5-30).

Figure 5-30. Add Media Rule Pop-up Window 2.

Note:	Do not select the **Learn Media IP dynamically** checkbox in the Add Media Rule pop-up window (Figure 5-30) unless later on you will also be selecting the **Enable Turing Test** checkbox in Figure 5-37**.** For information and instructions on enabling the Turing Test, refer to a later section in this chapter titled, "Configuring a Media Rule for Reverse Turing Test."

7. Select the appropriate Media NAT enforcement strategy for RTP injection detection/prevention using one of the two checkboxes. Table 5-3 describes each user-definable field displayed in Figure 5-30.

Table 5-3 Add Media Rule – Media NAT Pop-up Window Field Descriptions.

Field	Description
	Media NAT
Enforce Signaling and Media IP correlation	The Media IP and port are known.
Learn Media IP dynamically	The Media IP and port are learned dynamically.

Note:	**Media NAT** settings protect against RTP Injection Attacks. See the **Detect RTP Injection Attack** and **Asymmetric RTP** settings in Step-12.

8. A third Add Media Rule pop-up window is displayed (Figure 5-31).

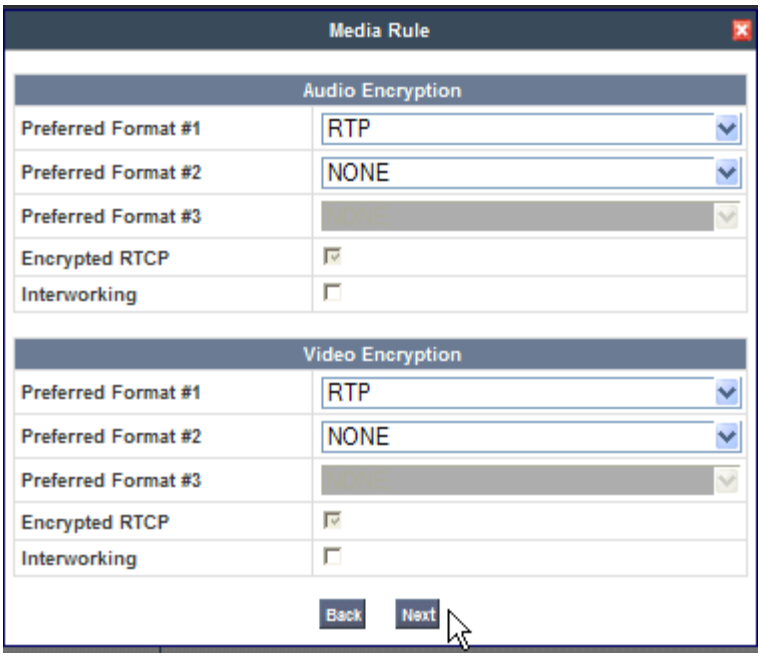


Figure 5-31. Add Media Rule Pop-up Window 3.

9. Enter the requested information into the appropriate fields using the checkboxes and pull-down windows. Table 5-4 describes each user-definable field displayed in the **Media Encryption** pop-up window. Selecting the **Cancel** icon cancels the operation and closes the window without saving.

Table 5-4 Add Media Rule - Codec Prioritization Pop-up Window Field Descriptions.

Field	Description
Audio Media Encryption and Video Media Encryption	
Preferred Format #1	The most preferred encryption method for media traffic. Available selections are: • RTP • SRTP_AES_CM_128_HMAC_SHA1_32 • SRTP_AES_CM_128_HMAC_SHA1_32
Preferred Format #2	The second most preferred encryption method for media traffic. Available selections are the same as those for **Format #1**.
Preferred Format #3	The least most preferred encryption method for media traffic. Available selections are the same as those for **Format #1**.
Encrypted RTCP	Checkbox indicating whether or not encryption will be used for RTCP.
Interworking	When the interworking checkbox is checked, it allows media from an encrypted media end-point flow. The reverse, unencrypted to encrypted, is also true. The interworking checkbox should be checked for the media rules in both end-point flows. Unless end-to-end encryption must be enforced, it is recommended that this checkbox be checked.

10. Select **Next**.
    A fourth Add Media Rule window is displayed (Figure 5-32).

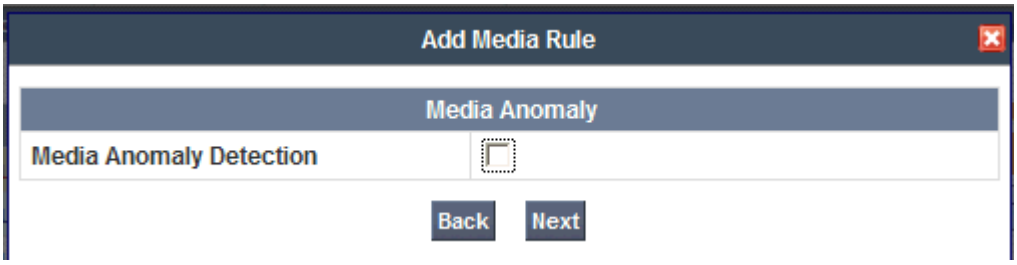


Figure 5-32. Add Media Rule Pop-up Window 4.

11. Click the checkbox (☑) to enable the **Media Anomaly Detection** feature. Leave blank (☐) if no **Media Anomaly Detection** will be used.
    Enable the Media Anomaly Detection feature to do the following:

    - This feature detects Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks on a RTP media stream.
    - The acceptable data rate for a given RTP stream is 20% more than the predefined bandwidth for the codec being used.
    - Whenever the incoming data rate on an RTP stream exceeds the acceptable data rate, a Media DoS attack incidence is reported.
    - If different sources are trying to send data over the RTP stream resulting in exceeding the acceptable data rate, up to five such sources are tracked and reported as a Media DDoS attack.
    - Enable RTP Injection Protection:
        - Looks for extraneous traffic being injected into the RTP stream.
        - Detects RTP Injection and generates an alert but allows the extraneous traffic to pass through without dropping any packets unless a DoS attack is detected.
        - RTP Injection is not detected for asymmetric RTP traffic and not detected in HA configurations for failed-over calls.

    All RTP traffic is limited by dropping the packets exceeding the acceptable data rate in a given second.

Note:	If Media Anomaly Detection is selected, choose whether or not to detect an RTP injection attack. Then designate whether or not the RTP connection is asymmetric and select an action to be taken.

12. If, in the previous step, you clicked the checkbox (☑) to enable the **Media Anomaly Detection** feature, an additional option checkbox is revealed, **Detect RTP Injection Attack**, as shown in a fifth Add Media pop-up window (Figure 5-33).

    Click the checkbox (☑) to enable the **Detect RTP Injection Attack** feature. Leave blank (☐) if not used. Select **Next**.

Note:	The **Detect RTP Injection Attack** checkbox enables the detection of an RTP injection attack. Also see the Media NAT enforcement strategy settings in Step 7.

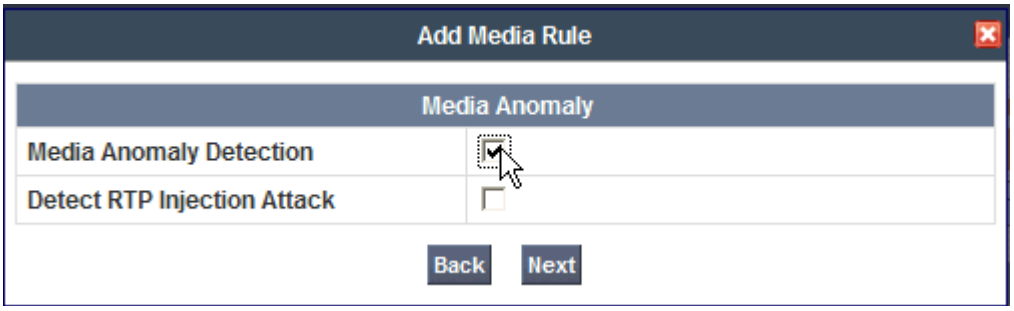


Figure 5-33. Add Media Rule Pop-up Window 5.

13. If, in the previous step, you clicked the checkbox (☑) to enable the **Detect RTP Injection Attack** feature, additional options are revealed, an **Asymmetric RTP** checkbox and an **Action** drop-down list, as shown in a sixth Add Media pop-up window (Figure 5-34) shown below.

    Click the checkbox (☑) to enable the **Asymmetric RTP** feature. Leave blank (☐) if not used. If checked, select an **Action** and select **Next**.

Note:	The **Asymmetric RTP** checkbox enables asymmetric RTP streams, where the payload type is not the same in both directions.

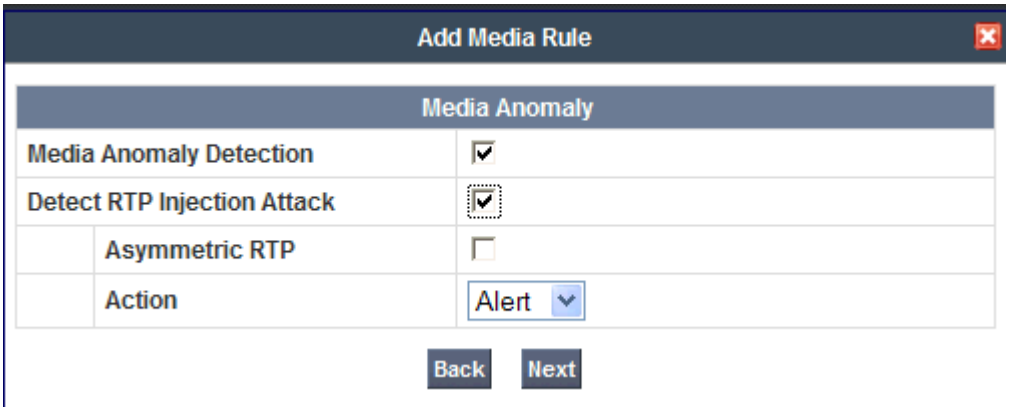


Figure 5-34. Add Media Rule Pop-up Window 6.

14. A seventh Add Media Rule pop-up window (Figure 5-35) is displayed.

    Click the checkbox (☑) to enable the **Media Silencing** feature. Leave blank (☐) if not used. If checked, enter a timeout value (in seconds) and select **Next**.

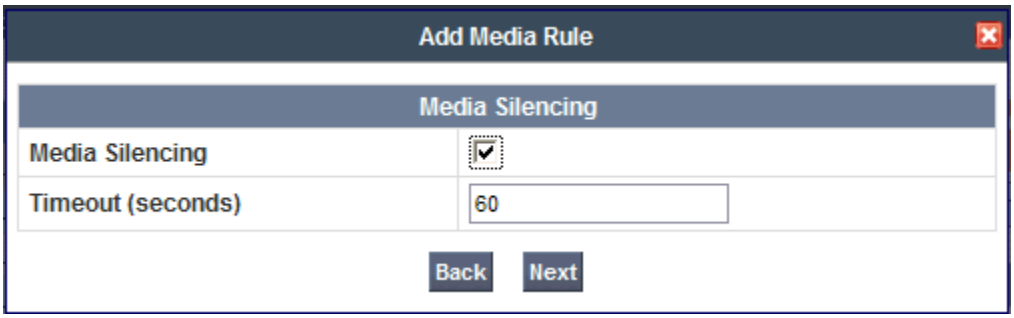


Figure 5-35. Add Media Rule Pop-up Window 7.

Table 5-5 describes the user-definable fields in Figure 5-35.

Table 5-5 Add Media Rule – Media Silencing Pop-up Window Field Descriptions.

Field	Description
Media Silencing	Checkbox indicating whether or not the **Media Silencing** feature is to be activated. If the Media Silencing feature detects the absence of media packets from one leg of the call in session within the time period defined by the **Timeout** field, an incidence is sent to the Syslog. If media packets are not detected in either direction during the same **Timeout**, then the call is terminated with a BYE message. If checked ☑, the media silencing feature is activated. If unchecked ☐, the media silencing feature is *not* activated.
Timeout (seconds)	The time period within which the media silencing feature 'listens' for media packets from both legs of a call. If no media packets are detected in this period, then either a Syslog entry is generated or the call is terminated.

15. An eighth Add Media Rule pop-up window (Figure 5-36) is displayed.

    Enter the requested information into the appropriate fields.

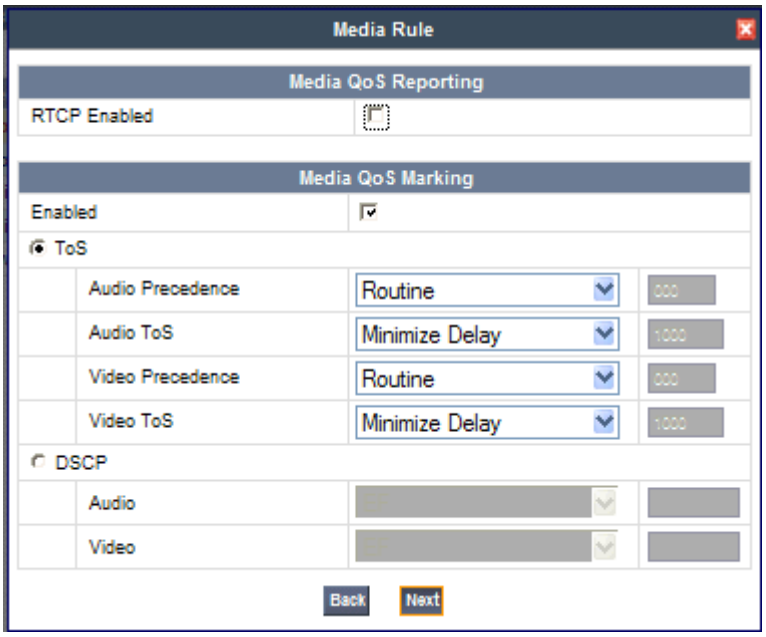


Figure 5-36. Add Media Rule Pop-up Window 8.

Table 5-6 describes each user-definable field displayed in Figure 5-36 above.

Table 5-6 Add Media Rule – QoS Reporting and Marking Pop-up Window Field Descriptions.

Field	Description
	Media QoS Reporting
RTCP Enabled	Checkbox indicating whether or not RTCP is enabled for media QoS reports. When RTCP is enabled, RTCP statistics will be included in the Call Detail Report (CDR). If checked ☑, RTCP is enabled. If unchecked ☐, RTCP is disabled.
	Media QoS Marking
Enabled	Checkbox indicating whether or not Type-of-Service (**ToS**) quality standards will be applied to audio and video streams. If checked ☑, the **ToS** quality standards will be applied and the **ToS** and **DSCP** radio buttons are activated. If unchecked ☐, the **ToS** quality standards will be applied and the **ToS** and **DSCP** radio buttons are *not* activated.
ToS	A radio button indicating that ToS quality standards will be applied to audio and video streams. ToS quality standards can be applied to four (4) audio/video parameters: **Audio Precedence**, **Audio ToS**, **Video Precedence**, and **Video ToS**. Select the desired quality level from the corresponding drop-down menu. When the ToS option is selected, the **DSCP** quality option is disabled.

Field	Description
DSCP	A radio button indicating that ToS quality standards will be applied to audio and video streams. ToS quality standards can be applied to audio and video streams. Select the desired quality level from the corresponding drop-down menu. When the ToS option is selected, the DSCP quality option is disabled.

16. Select **Next**.
17. A ninth Add Media Rule pop-up window (**Figure 5-37**) is displayed.

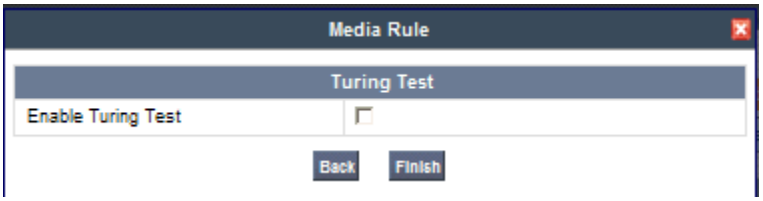


Figure 5-37. Add Media Rule Pop-up Window 9.

18. See the note below. Click **Finish** without selecting the checkbox (☑) to enable the Turing Test feature. This checkbox should be left blank (☐) if no Turing Test will be used.

Note:	Do not select the **Enable Turing Test** checkbox in **Figure 5-37** unless you previously selected the **Learn Media IP dynamically** checkbox in the Add Media Rule pop-up window (**Figure 5-30**) . For information and instructions on enabling the Turing Test, refer to a later section in this chapter titled, “Configuring a Media Rule for Reverse Turing Test.”

The newly-updated Media Rule screen (Figure 5-38) is displayed.

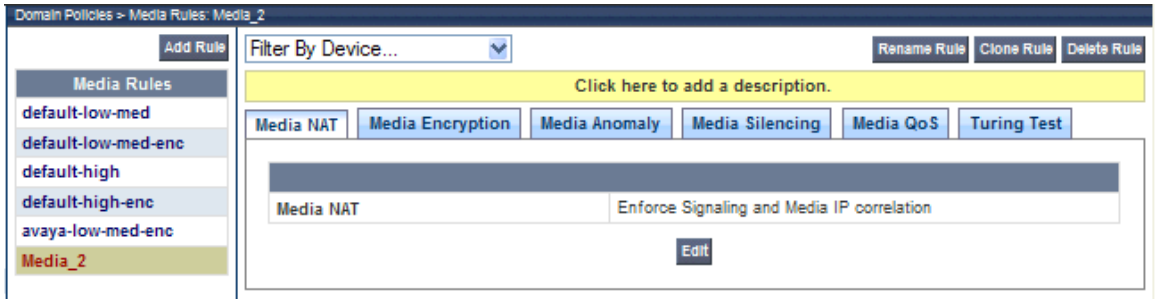


Figure 5-38. Updated Media Rule Screen.

Cloning an Existing Media Rule

Use the following procedure to make an exact copy (clone) of an existing **Media Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Media Rules** function from the **Domain Policies** feature from the Task Pane.

Existing rule sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Media Rule set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-39.

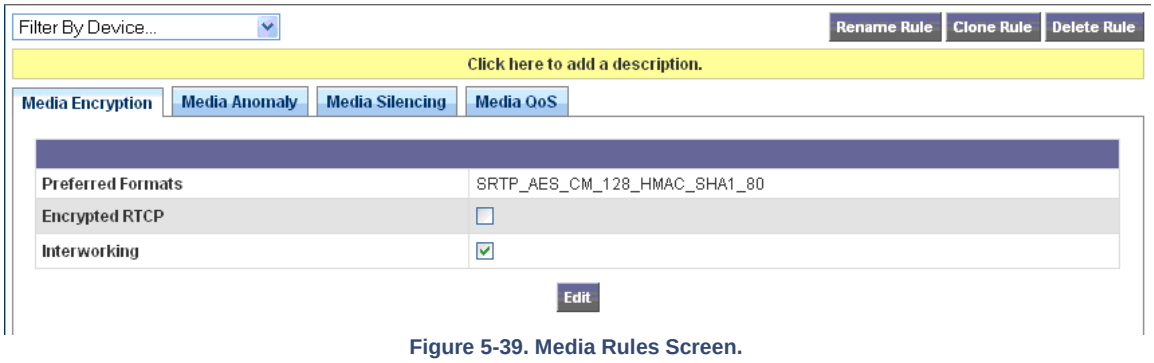


Figure 5-39. Media Rules Screen.

3. In the Application Pane, select the **Media Rule** you want to clone (Figure 5-40).
4. Select **Clone Rule**.
   The **Clone Rule** pop-up window is displayed (Figure 5-41).

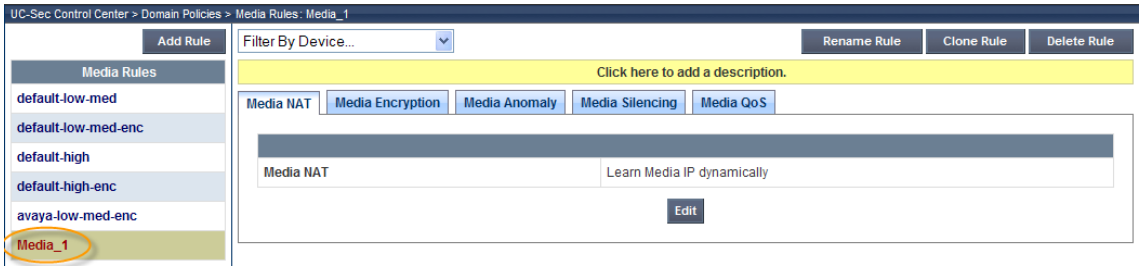


Figure 5-40. Selecting an Existing Media Rule Set.

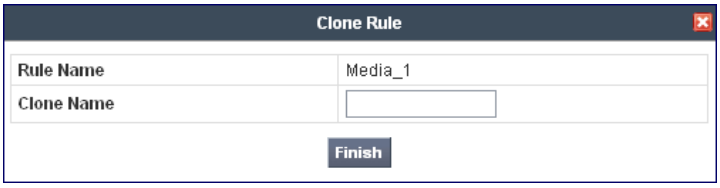


Figure 5-41 Clone Rule Pop-up Window.

5. Enter a name for the new **Media Rule** and select **Finish** to save your changes or **Cancel** to cancel the cloning operation and close the window without saving.
   The Media Rule screen is redisplayed (Figure 5-42), showing the cloned Media Rule.

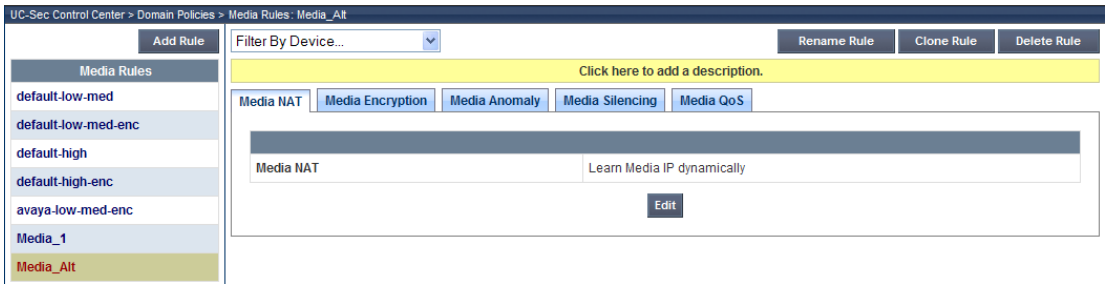


Figure 5-42. Updated Media Rule Screen.

Editing an Existing Media Rule

Use the following procedure to edit an existing **Media Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Media Rules** function from the **Domain Policies** feature from the Task Pane. Existing rule sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Media Rule set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-39.
3. In the Applications Pane, select the **Media Rule** set you want to edit (Figure 5-40). The parameters for that Media Rule set will be displayed in the Content Area.
4. Select the Media **Rule Parameter Tab** whose values you want to edit (Figure 5-43). The corresponding parameters will be displayed in the Content Area.
5. Select **Edit**.
   An editable pop-up window will be displayed (Figure 5-44) for Media Encryption parameters.
6. Edit the desired fields and select Finish to save your changes or Cancel to cancel the operation and close the window without saving.

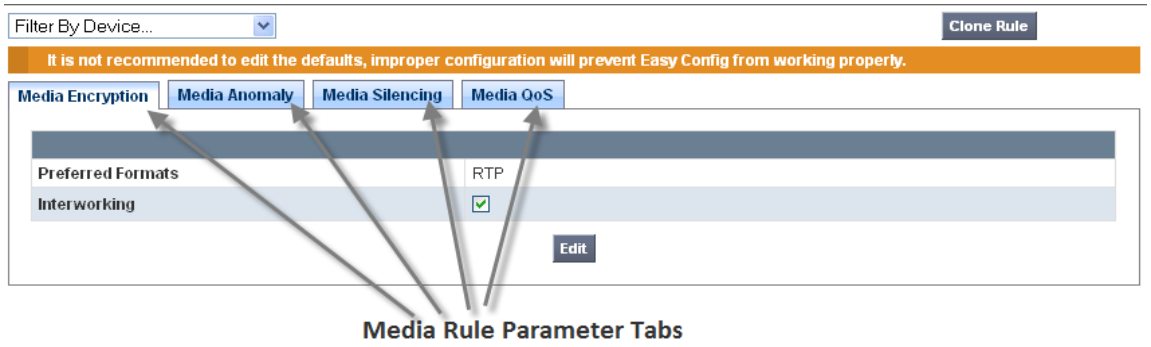


Figure 5-43 Selecting Media Rule Parameter Tabs.

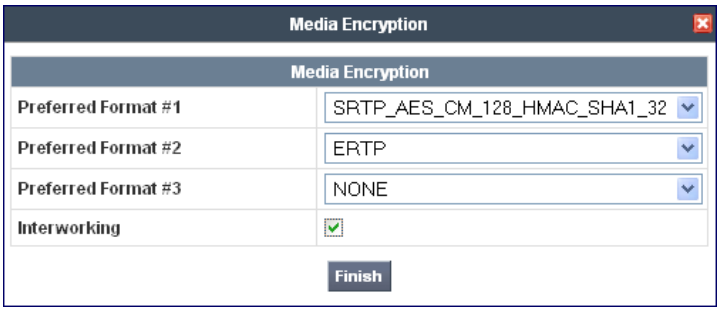


Figure 5-44 Media Encryption Pop-up Window.

Renaming an Existing Media Rule

Use the following procedure to rename an existing **Media Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Media Rules** function from the **Domain Policies** feature from the Task Pane. Existing rule sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Media Rule set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-39.
3. In the Application Pane, select the **Media Rule** you want to rename (Figure 5-40).
4. Select **Rename Rule**.
   The **Rename Rule** pop-up window is displayed (Figure 5-45).

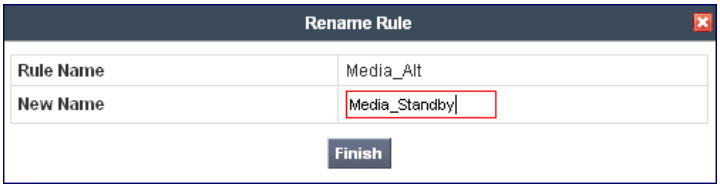


Figure 5-45. Rename Rule Pop-up Window.

5. Enter a name for the **Media Rule** and select **Finish** to save your changes or **Cancel** to cancel the renaming operation and close the pop-up window without saving.

Deleting an Existing Media Rule

Use the following procedure to delete an existing **Media Rule** set.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Media Rules** function from the **Domain Policies** feature from the Task Pane. Existing rule sets are displayed in the Application Pane in the Rules section. The parameters comprising a selected Media Rule set are displayed in the Content Area of the E-SBC Control Center.
3. Select **Delete Rule**.
   The Delete Confirmation pop-up window is displayed.
4. Select **OK**.
   The Media Rule set is deleted and the **Media Rules** screen is redisplayed.

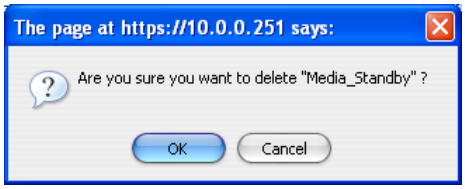


Figure 5-46. Delete Confirmation Pop-up Window.

Configuring a Media Rule for Reverse Turing Test

Reverse Turing Test is used to prompt and test the called party or transferred party (internal users) of the conversation at call initiation and also at the invocation of important call features, such as resume following a call placed on hold, internal transfer, or conference server. The response by internal users or conference server to the automated prompts and tests is a way of acknowledging that the call with the external user should be considered non-secure. The Reverse Turing Test operation is described below, followed by the configuration steps.

Call Setup

- All the calls initiated from Trunk side and towards internal user will be subjected to Turing Test.
- As soon as internal user picks up the call, he/she will be prompted to enter some random set of digits. Only after internal user successfully enters the requested digits he will be allowed to continue with the call. On the failure to enter correct digits within the timeout period, call will be disconnected and caller is notified of the same.
- While E-SBC is trying to prompt and verify the digits from internal user, E-SBC will play relevant messages and tones towards trunk side caller.

Call Hold/Resume

- When an internal user puts the trunk-side caller on hold and later when he/she resumes the call, internal user will be subjected to Turing Test.
- Failure to enter valid digits within the timeout period will disconnect the call in a gracious manner.
- While E-SBC is trying to prompt internal user, external user should still be played some music.

Call Transfer

- When an internal user is transferred to another internal user, transfer target will be subjected to Turing Test.

Conference Call

- E-SBC does not verify the use cases where users connect to a pre configured bridge. When an external user is re-directed to a conference server, E-SBC will play a prompt towards the conference IP for digit verification.
- When more than one external user is connected to a conference, the prompt will be played as many times. Currently, E-SBC will not support the feature where multiple streams in the same conference (by using IP and port) are detected and a prompt is played only once.

Failure Treatment

- When a turing test fails, a call failure announcement is played to both parties, and one of the parties should initiate a call release.

To configure a Media Rule for Turing Test, complete the following procedure steps:

1. Login to the E-SBC control center as the Admin.
2. As shown in the example in Figure 5-, select the **Media Rules** function from the **Domain Policies** feature from the Task Pane.

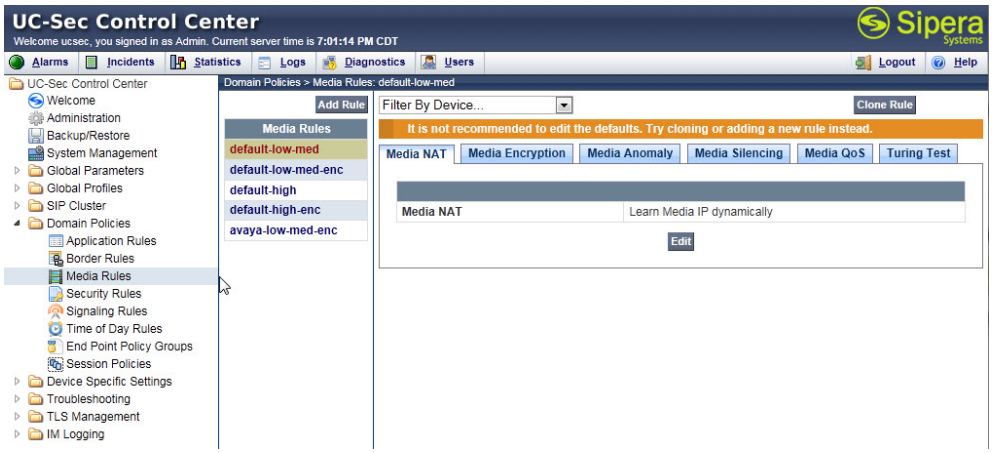


Figure 5-47 Selecting Media Rules

3. Click the **Add Rule** button (located above the Media Rules list) as shown above in Figure 5- to display the first Add Media Rule screen, as shown in Figure 5-48 in the example below.

Figure 5-48 Add Media Rule Screen 1

4. As shown above in Figure 5-48, enter a Media Rule profile name, and click **Next** to display a second Add Media Rule screen with a section titled Media NAT as shown in Figure 5-49 below.

Figure 5-49 Add Media Rule Screen 2

5. In the second Add Media Rule screen (Figure 5-49), leave the default option "Learn Media IP dynamically," selected, and select **Next** to display a third Add Media Rule screen (Figure 5-50 Add Media Rule Screen 3) with a section titled Media Encryption.

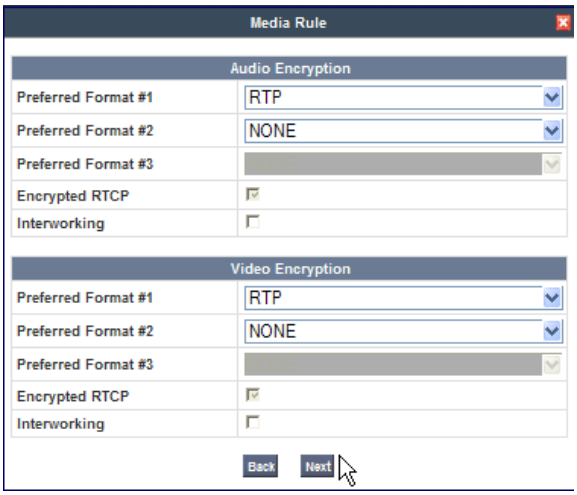


Figure 5-50 Add Media Rule Screen 3

6. In the third Add Media Rule screen, select the preferred media formats as shown in the example (Figure 5-50) or as per the deployment requirements, and then select **Interworking** and click **Next** to display a fourth Add Media Rule screen with a section titled Media Anomaly, as shown in Figure 5-51 below.

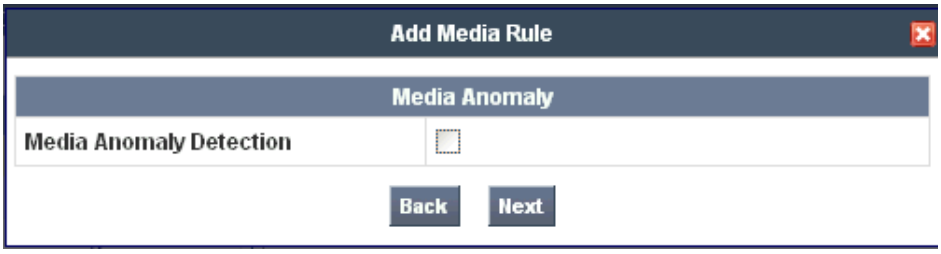


Figure 5-51 Add Media Rule Screen 4

7. In the fourth Add Media Rule screen above, leave the default setting (Media Anomaly Detection unchecked) and click Next to display a fifth Add Media Rule screen with a section titled Media Silencing, as shown in Figure 5-52 in the example below.

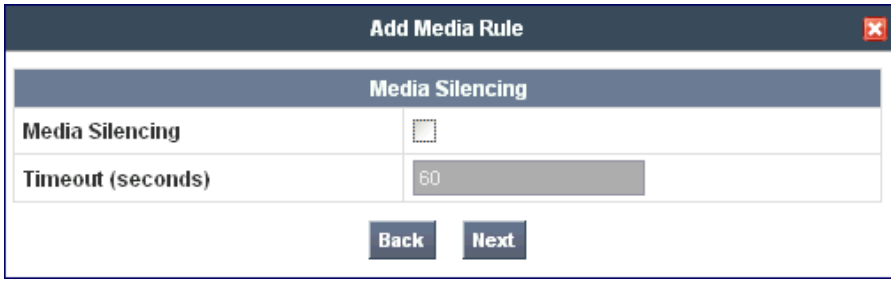


Figure 5-52 Add Media Rule Screen 5

8. In the fifth Add Media Rule screen (Figure 5-52), disable the Media Silencing feature and click **Next** to display a sixth Add Media Rule screen with sections titled Media QoS Reporting and Media QoS Marking, as shown in Figure 5-53.

Note:	**Keeping Default values for Media silencing does not affect Turing test feature.**

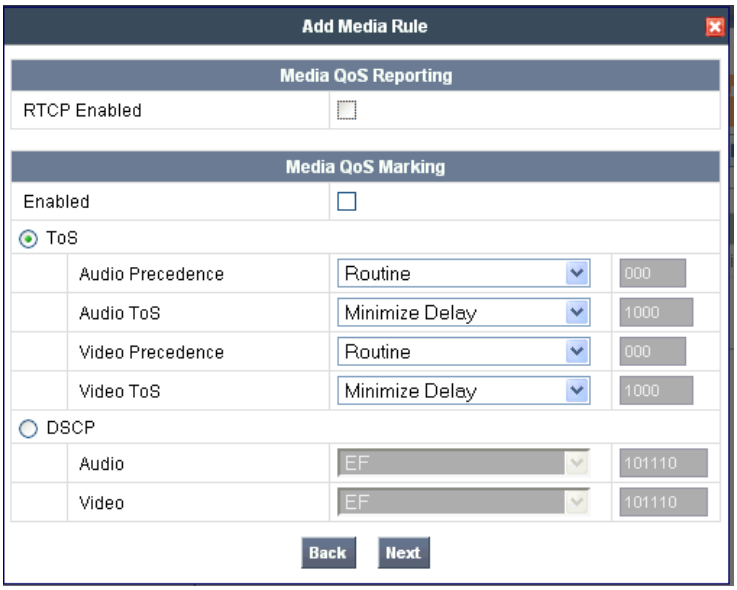


Figure 5-53 Add Media Rule Screen 6

9. In the sixth Add Media Rule screen, disable the Media QoS Reporting and Media QoS Marking features by deselecting their checkboxes, and then click **Next** to display a seventh Add Media Rule screen with a section titled Turing Test, as shown in Figure 5-54 below.

Note:	**Keeping Default values for Media QOS Marking does not affect Turing test feature..**

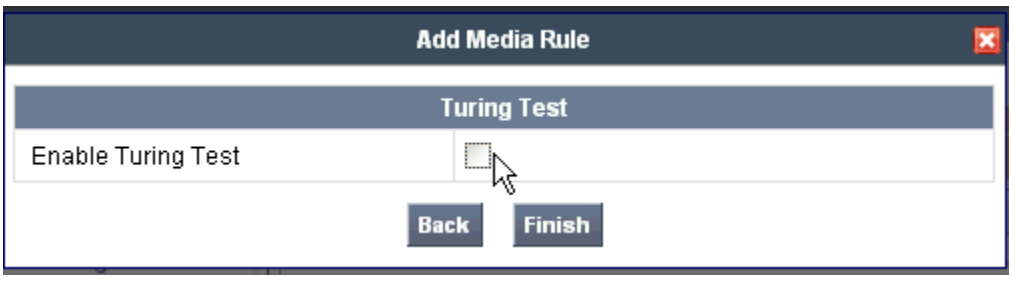


Figure 5-54 Add Media Rule Screen 7

10. In the seventh Add Media Rule screen (Figure 5-54), select the checkbox to enable the Turing Test feature, and to display the expanded Turing Test

configuration dialog in an eighth Add Media Rule screen shown in Figure 5-55 below.

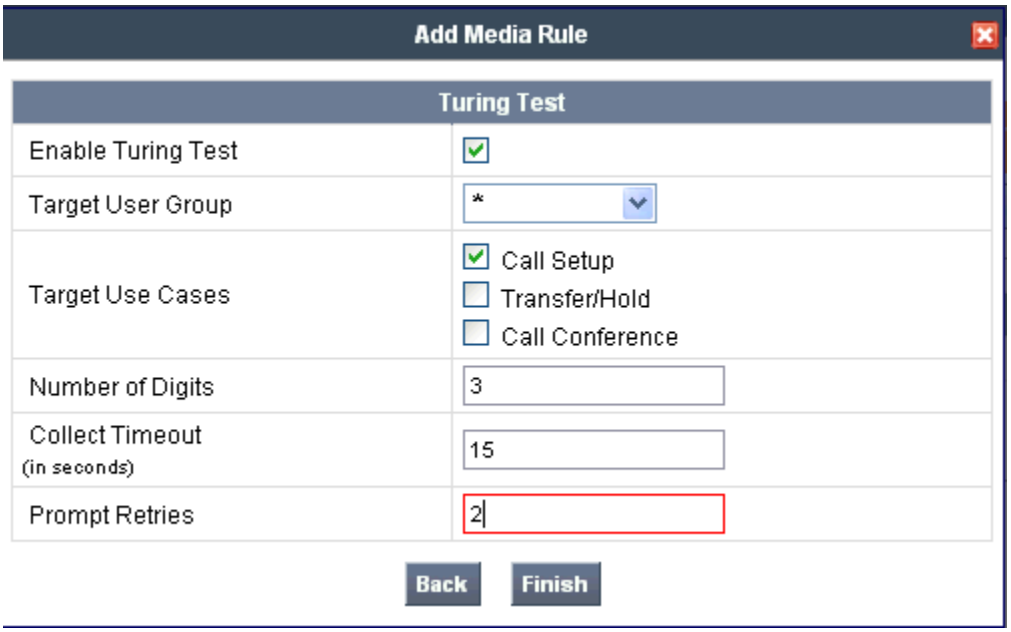


Figure 5-55 Add Media Rule Screen 8

11. In the eighth Add Media Rule screen (Figure 5-55), make all of the appropriate selections and entries, which are listed and described in Table 5-7 below.

Table 5-7 Turing Test Parameter Descriptions.

Field	Description
Target User Group	Configure the User group for which the signaling traffic needs to be Forked. The User group needs to be URI group profile configured in URI Group section.
Target Use Cases	Select all Use cases the Signaling Forking needs to be done: • Call Setup • Transfer/Hold • Call Conference
Number of Digits	Number of digits to be prompted and verified. Default value is “3”. Minimum is “1” and Maximum is “9”.
Collect timeout	Maximum time user has to press the prompted digits before E-SBC times out. Default is 5. Min is 1 and Max is 15.
Prompt retries	Number of times E-SBC will retry prompting on failure to collect the digits. Minimum is ‘1’ and Maximum is ‘3’.

12. Click **Finish** to save and exit.

13. Select the **End Point Policy Groups** function of the **Domain Policies** feature, as shown in Figure 5-56 below. This will display the Policy Groups screen shown in Figure 5-57 below.

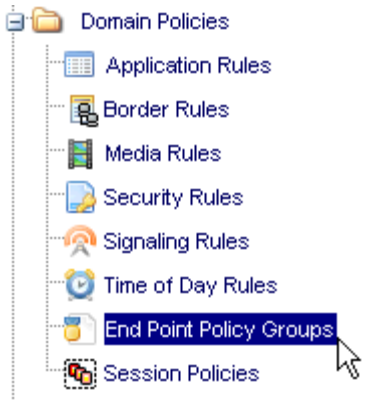


Figure 5-56 Add Media Rule Screen 8

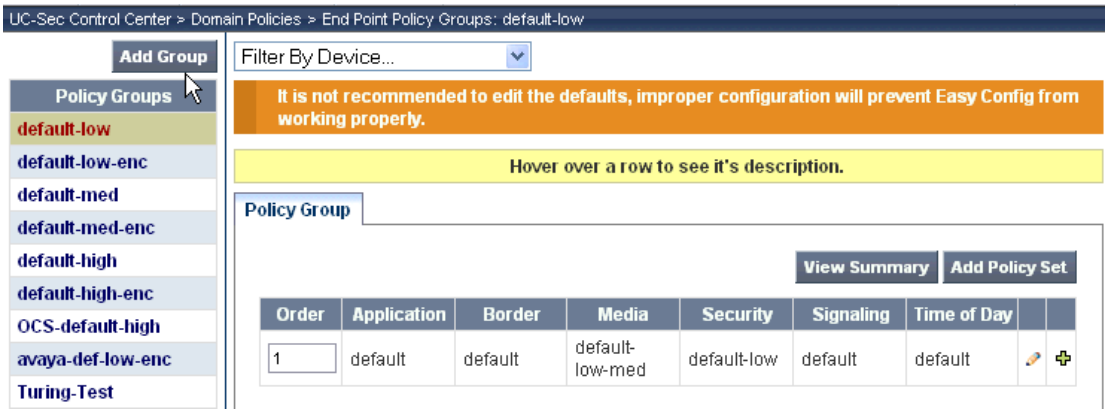


Figure 5-57 Policy Groups Screen

14. In the Policy Groups screen (Figure 5-57), click on the **Add Group** button, as shown in the example, to display the **Add Policy Group** screen shown in Figure 5-58 below. In the first Add Policy Group screen below enter a group name and click **Next** to display a second Add Policy Group screen as shown in Figure 5-59.

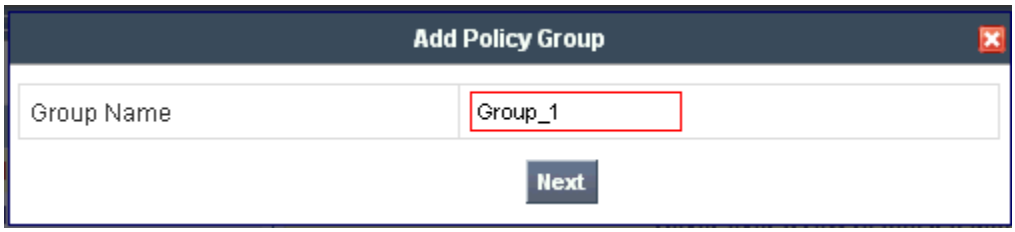


Figure 5-58 Add Policy Group Screen 1

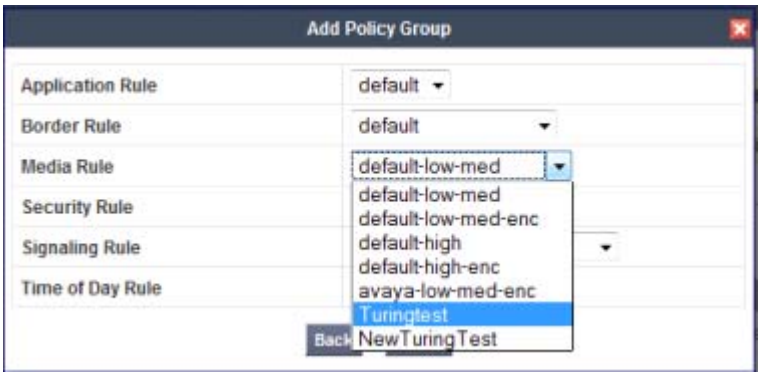


Figure 5-59 Add Policy Group Screen 2

15. In the second Add Policy Group screen (Figure 5-59), in **Media Rule** drop-down list, select the **Media Rules** profile created as described in earlier steps as shown in Figure click **Next** to save, exit, and redisplay the **Policy Groups** screen with the newly-created group (**Group_1**) displayed in the list, as shown in Figure 5-60 in the example below.

Figure 5-60 Updated Policy Groups Screen

16. Select the **End Point Flows** function of the **Device Specific Settings** feature to display the Subscriber and Server Flows screen, as shown in Figure 5-61.

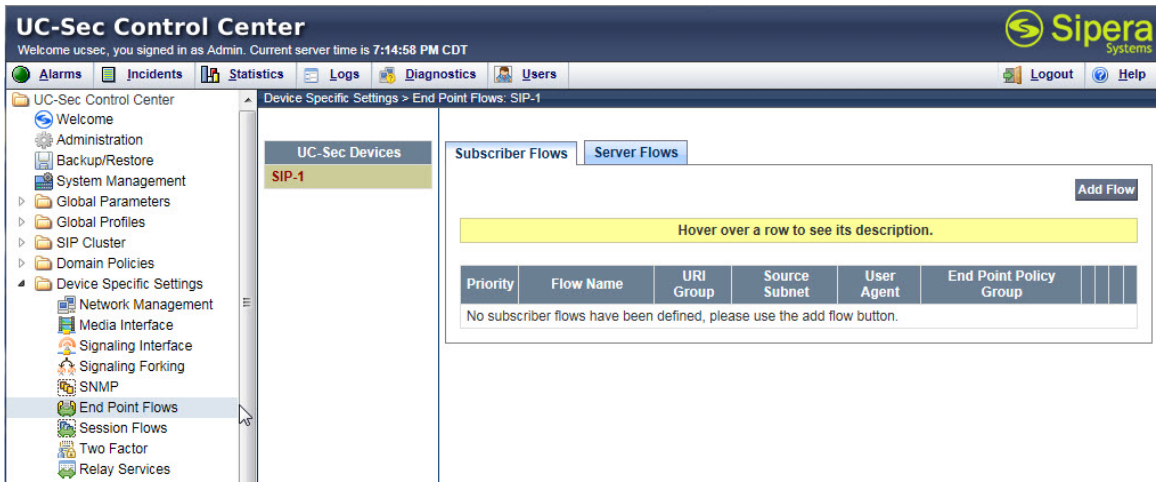


Figure 5-61 Subscriber and Server Flows Screen

17. In the Subscriber and Server Flows screen (Figure 5-61), select the Server Flows tab to display the Server Flows screen, as shown in Figure 5-62 below.

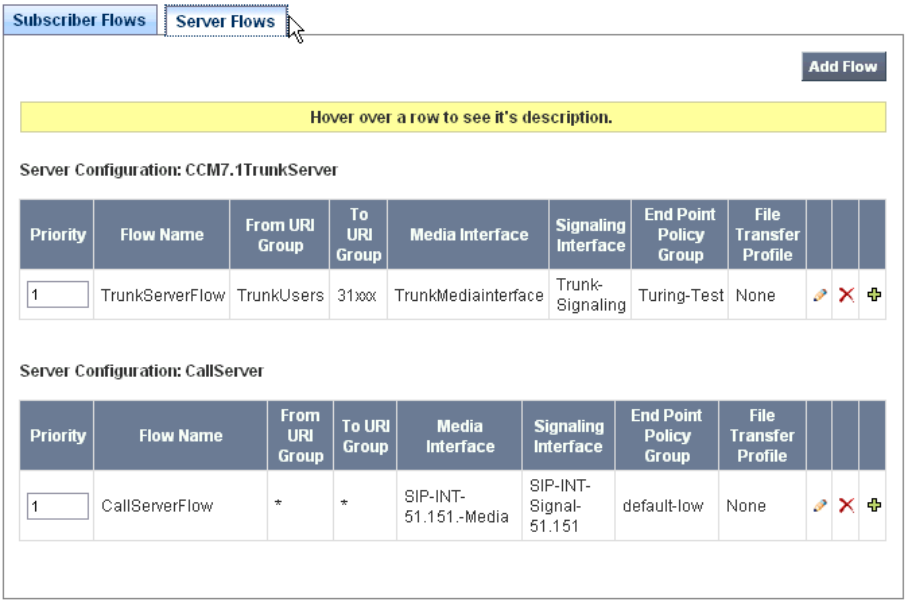


Figure 5-62 Server Flows Screen

18. In the Server Flows screen (Figure 5-62), on the Trunk Server Flow information line, click on the Edit pencil icon *( )* located on the right-hand end of the line, as shown in Figure 5-63. Clicking on the **Edit** button displays the **Edit Flow** screen shown in Figure 5-64.

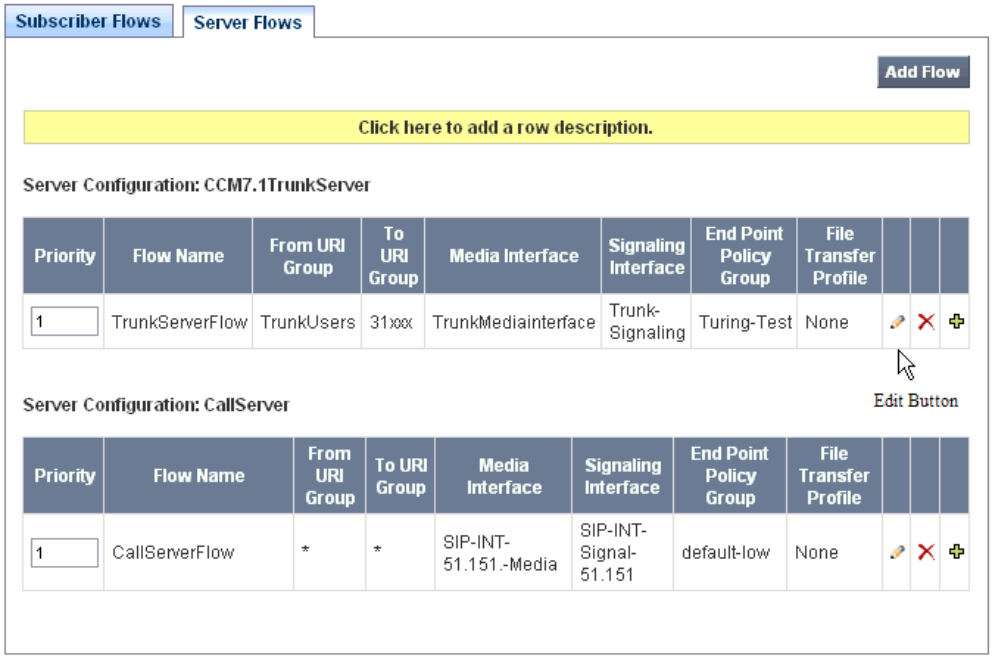


Figure 5-63 Editing the Trunk Server Flow

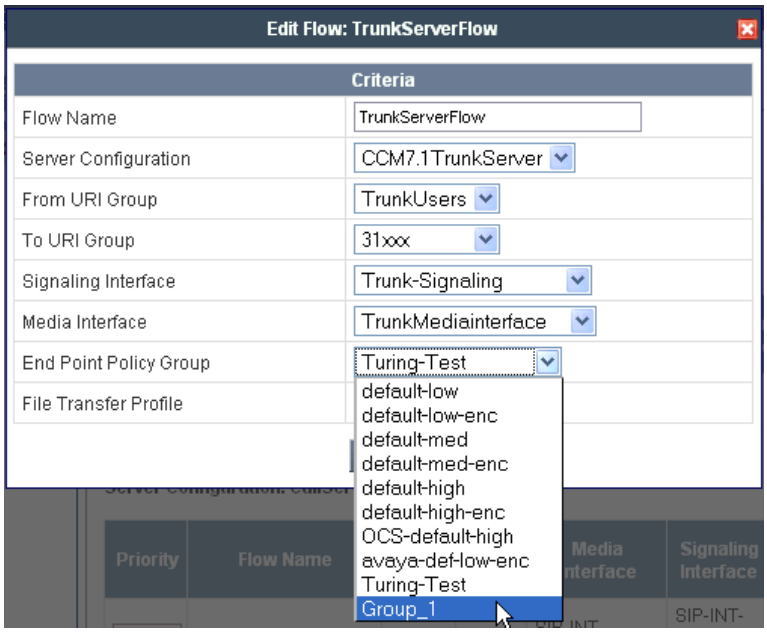


Figure 5-64 Edit Flow Screen

19. In the Edit Flow screen, in the End Point Policy Group drop-down list, select the name of the new group that you defined previously, as shown in the example above.

20. To view and/or edit an existing Turing Test feature, select the **Media Rules** function from the **Domain Policies** feature from the Task Pane, and then select the Turing tab that is located on the right-hand portion of the screen, as shown in Figure 5-65 below.

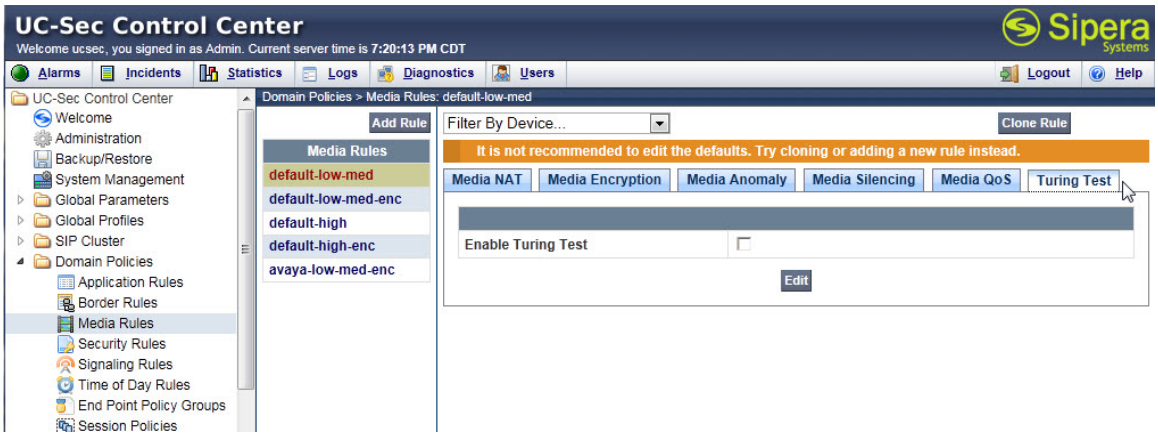


Figure 5-65 Selecting Media Rules Turing Tab

21. From the Media Rules Turing tab, you can view the existing Turing Test configuration settings. To change one or more of the settings, click on the Edit button at the bottom of the screen to display the Turing Test Edit screen shown in the example shown in the figure below.

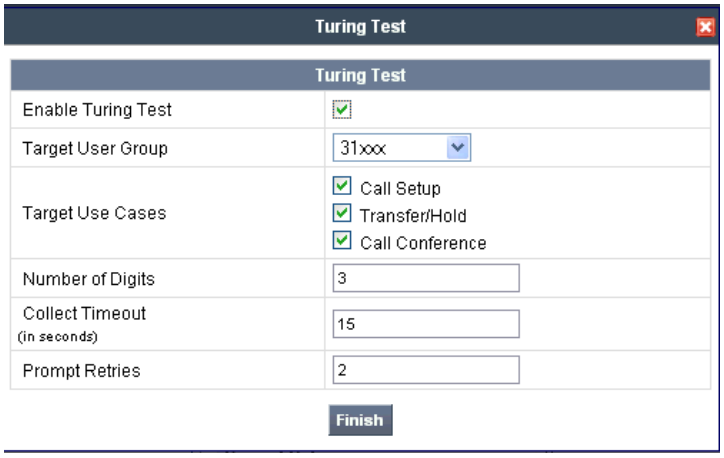


Figure 5-66 Turing Tab Edit Screen

22. After making changes in the Turing Tab Edit screen (Figure 5-66), click on **Finish** to save, exit, and redisplay the Media Rules Turing Test tab screen, to verify that the changes were entered and saved.

Security Rules

Security Rules allow you to define which enterprise-wide VoIP and Instant Message (IM) security features will be applied to a particular call flow. Security Rules allows you to configure Compliance, Scrubber, and Domain DoS. In addition to determining which combination of security features are applied, you can also define the security feature profile so that the feature is applied in a specific manner to a specific situation.

Note:	Scrubber Packages must be enabled in the Security Rules of Domain Policies. Only then will the Scrubber Packages take effect.

Once the Scrubber Packages are enabled in the Security Rules, a list of packages would be needed for the Security Rule. Refer to the section titled, “Protocol Scrubber” in Chapter 7.

Five security features can be controlled by enabling/disabling the Security Rules listed below:

- Authentication: Not applicable for E-SBC deployments.
- From URI Blacklist: Can be enabled to reject the calls from the devices configured in the Black list group.
- FingerPrint: Not applicable for E-SBC deployments.
- Scrubber: Can be enabled to detect and drop malformed messages.
- Domain Dos: Can be enabled to detect DoS attacks within a Domain policy.

Creating a New Security Rule

Use the following procedure to create a new **Security Rule.**

Caution!

A default Security Rule set named **default** is provided by Sipera. Editing this rule set is not recommended, as improper configuration may cause subsequent calls to fail.

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Security Rules** function from the **Domain Policies** feature from the Task Pane. Existing **Security Rule** sets are displayed in the Application Pane. The parameters comprising a selected **Security Rule** set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-67

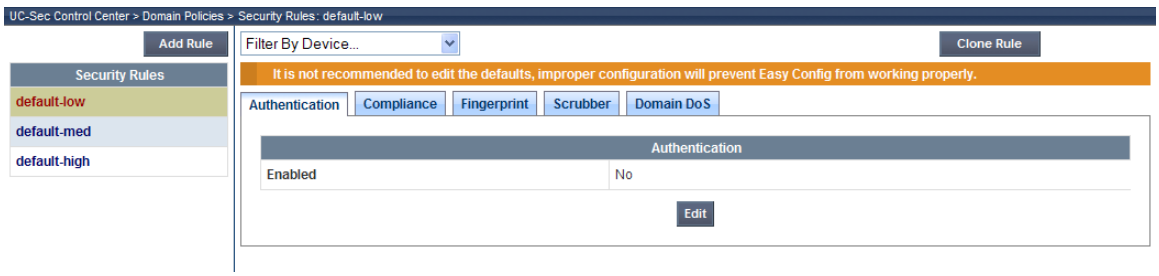


Figure 5-67 Security Rules Display Screen.

3. Select **Add Rule** from the Application Pane.
   The **Add Security Rule Name** pop-up window is displayed (Figure 5-68).

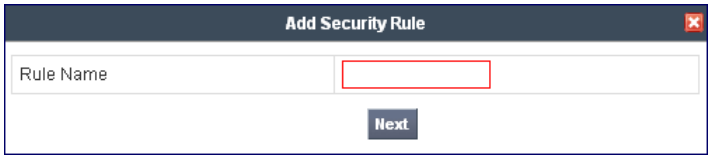


Figure 5-68 Add Security Rule Pop-up Window.

4. Provide a name for the new **Security Rule** and press **Next.**
   The **Add Security Rule – Features and Authentication** pop-up window is displayed (Figure 5-69).

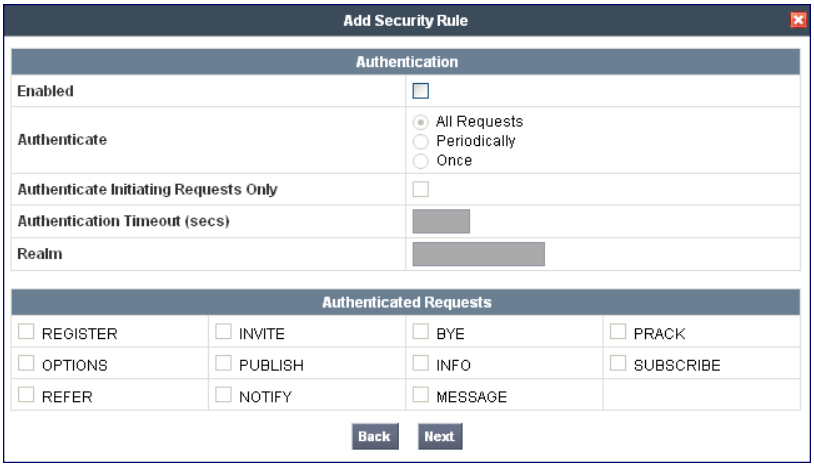


Figure 5-69 Add Security Rule: Authentication Pop-up Window.

5. In the Add Security Rule screen, do not select the Enabled checkbox, just select the Next button. The Add Security Rule: Compliance pop-up window is displayed (Figure 5-70X).

Figure 5-70 Add Security Rule: Compliance Pop-up Window.

6. From the drop-down window, select the **From/To Blacklist** to be used to check the validity of subscribers using the network. When **From URI Blacklist** is enabled, calls are rejected from devices in the Blacklist group.
7. Select **Next.**
   The **Add Security Rule: Fingerprint Profile** pop-up window is displayed (Figure 5-71).

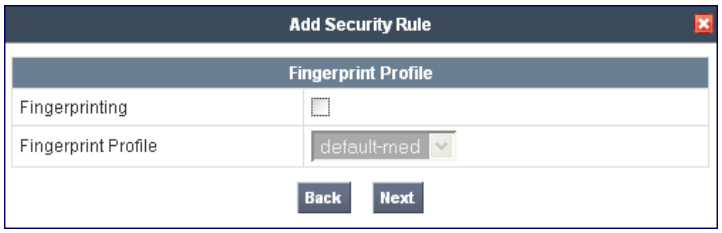


Figure 5-71 Add Security Rule: Fingerprint Profile Pop-up Window.

8. Enter the requested information into the appropriate fields.
   Table 5-8 describes each user-definable field displayed in the **Add Security Rule: Fingerprint Profile** pop-up window.

Table 5-8 Add Security Rule: Fingerprint Profile Pop-up Window Field Descriptions.

Field	Description
Fingerprinting	A checkbox indicating whether or not the **Fingerprinting** feature will be enabled. When Fingerprinting is enabled, spoofed messages will be detected and dropped. If checked (☑), the **Fingerprinting** feature is enabled and the **Fingerprint Profile** field is activated. If unchecked (☐), the **Fingerprinting** feature is not enabled and the Fingerprint **Profile** field is inactivated.
Fingerprint Profile	A pull-down menu from which you select the profile to be used by the **Fingerprinting** feature.

9. Select **Next.**
   The **Add Security Rule: Scrubber Profile** pop-up window is displayed (Figure 5-72).

Note: New Scrubber Packages and VIPER signatures are added here.

VIPER signatures are similar to Scrubber Packages, and are created by the VIPER team, and then packaged and released by the engineering team after testing.

Refer to the section titled, “Updating VIPER Signatures” in Chapter 4 and the section titled, “Protocol Scrubber,” in Chapter 7.

Figure 5-72 Add Security Rule: Scrubber Profile Pop-Up Window.

Note:	Before adding a new scrubber package to a security rule here, you must first install the scrubber package on the E-SBC from the Scrubber feature of Global Parameters. Refer to Figure 5-73 below that shows how to select the Scrubber function of the Global Parameters feature, and refer to the section titled, "Installing a Scrubber Rules Package," in Chapter 7.

Figure 5-73 Scrubbers Feature of Global Parameters

10. Enter the requested information into the appropriate fields shown in Figure 5-72 in the Add Security Rule Scrubber Profile pop-up screen. Refer to Table 5-9 below, which describes each of the user-definable fields.

Table 5-9 Add Security Rule: Scrubber Profile Pop-up Window Field Descriptions.

Field	Description
Enable Scrubber	A checkbox indicating whether or not the **Scrubber** feature will be enabled. If checked (☑), the **Scrubber** feature is enabled and the **Scrubber Packages** field is activated. If unchecked (☐), the **Scrubber** feature is not enabled and the **Scrubber Packages** field is inactivated.
Scrubber Packages	A collection of existing **Scrubber Packages** which can be selected for use by the **Scrubber** feature.

11. Select **Next.** The **Add Security Rule: Domain DoS** pop-up window is (Figure 5-74) displayed.

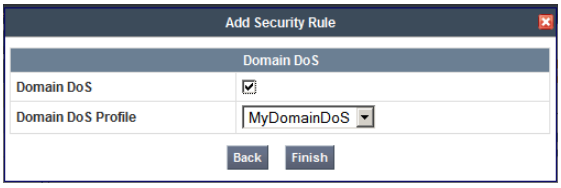


Figure 5-74 Add Security Rule: Domain DoS Pop-up Window.

12. Upon selecting the **Domain DoS** checkbox, entering a profile name, and clicking **Finish**, an Add Domain/URI pop-up window is displayed for entering a comma-separated list of Whitelist URIs.

Note:	Before enabling Domain DoS in the Add Security Rule: Domain DoS pop-up window (*see* Figure 5-74), you must first create a Domain DoS profile, if there are not any profiles created, by selecting the Domain DoS feature of the Global Profiles function (see Figure 5-75, and refer to the section titled, "Adding a New Domain DoS Profile," in Chapter 7). Selecting the Domain DoS checkbox (Figure 5-74) enables the Domain DoS Profile drop-down information field below it, to allow the user to select from several Domain DoS profiles.

Figure 5-75 Domain DoS Feature of Global Profiles

13. Table 5-10 describes each user-definable field displayed in the **Add Security Rule: Domain DoS** pop-up window.

Table 5-10 Add Security Rule: Domain DoS Pop-up Window Field Descriptions.

Field	Description
Domain DoS	A checkbox indicating whether or not the **Domain DoS** feature will be enabled. If checked (☑), the **Domain DoS** feature is enabled and the **Domain DoS Profile** field is activated. If unchecked (☐), the **Domain DoS** feature is not enabled and the **Domain DoS Profile** field is inactivated.
Domain DoS Profile	A collection of existing DoS profiles which can be selected for use by the **Domain DoS** feature.
Add Domain/URI	Accepts a comma-separated list of Whitelist URIs of allowed users.

14. Select **Finish.**
    The new **Security Rule** set is added to the **Security Rule** list (Figure 5-76).

Figure 5-76 Updated Security Rule Screen.

Cloning an Existing Security Rule

Use the following procedure to make an exact copy (clone) of an existing **Security Rule.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Security Rules** function from the **Domain Policies** feature from the Task Pane. Existing **Security Rule** sets are displayed in the Application Pane. The parameters comprising a selected **Security Rule** set are displayed in the Content Area (see Figure 5-76) of the E-SBC Control Center area.
3. In the Application Pane, select the Security Rule you want to clone (Figure 5-77). The configuration parameters of the selected **Security Rule** are displayed in the Content Area.

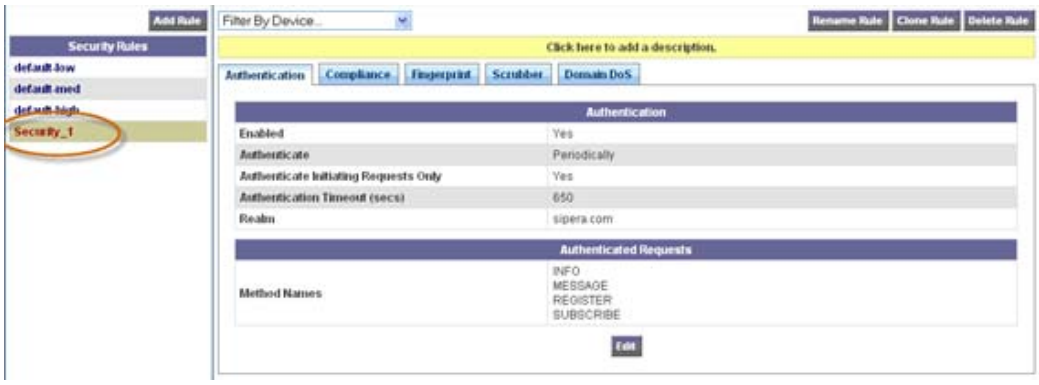


Figure 5-77 Selecting an Existing Security Rule Set.

4. Select **Clone Rule**
   The **Clone Security Rule** pop-up window is displayed (Figure 5-78).

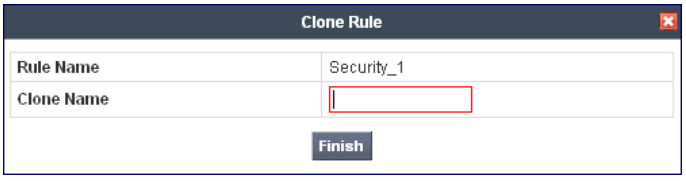


Figure 5-78 Clone Rule Pop-up Window.

5. Enter a name for the new **Security Rule** and select **Finish** to save the new rule or **Cancel** to cancel the cloning operation and close the window without saving.
   The cloned Security Rule screen is redisplayed with the cloned rule listed in the Application Pane (Figure 5-79).

Figure 5-79 Updated Security Rule Display Screen.

Editing an Existing Security Rule

Use the following procedure to edit an existing **Security Rule.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Security Rules** function from the **Domain Policies** feature from the Task Pane. Existing **Security Rule** sets are displayed in the Application Pane. The parameters comprising a selected **Security Rule** set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-67
3. In the Application Pane, select the **Security Rule** you want to edit (Figure 5-80).
   The selected **Security Rule** is displayed in the Content Area.

Figure 5-80 Selecting an Existing Security Rule Set.

4. Select the tab (**Authentication**, **Compliance**, **Fingerprint**, **Scrubber**, or **Domain DoS**) containing the security parameters you want to edit (Figure 5-81).
   The security parameters contained in that tab will be displayed in the Content Area.

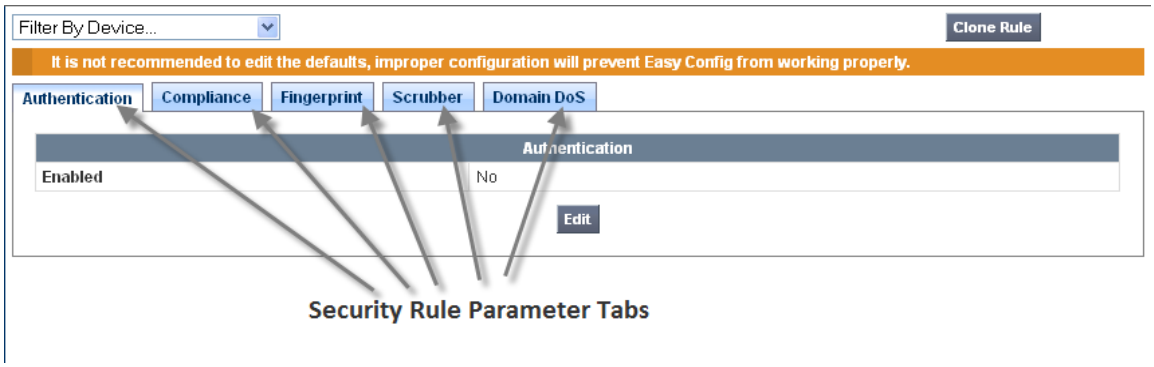


Figure 5-81 Security Rule Set Parameter Tabs.

5. For the **Authentication**, **Compliance**, and **Fingerprint** security tabs, select **Edit**. For the **Domain DoS** security tab, go to step 7. For the **Scrubber** security tab, go to step 9.
   An editable pop-up window is displayed similar to that shown for the Security tab (Figure 5-82).

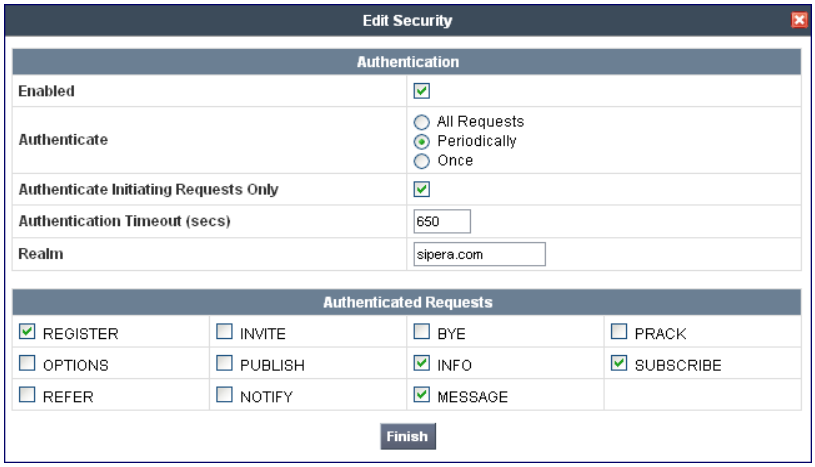


Figure 5-82 Edit Security Rule: Authentication Pop-up Window.

6. Edit the desired fields and select **Finish** to save your changes or **Cancel** to cancel the operation and close the editing pop-up window without saving.
7. For the **Domain DoS** security tab, select the **Edit DoS Settings** button.
8. The **Edit Domain DoS** pop-up window is displayed (Figure 5-83).

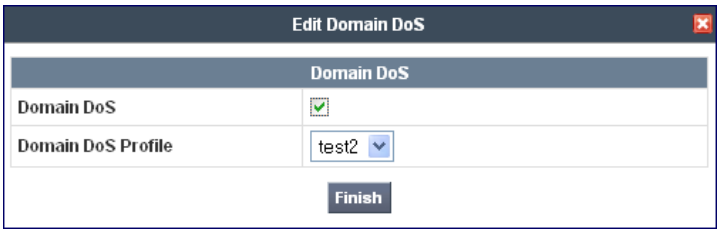


Figure 5-83 Edit Domain DoS Pop-up Window.

9. Edit the fields as desired and select Finish. If necessary, refer back to Table 5-10.
10. Select **Disable Scrubber** (or **Enable Scrubber**) if the **Scrubber** feature is enabled.

Renaming an Existing Security Rule

Use the following procedure to rename an existing **Security Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Security Rules** function from the **Domain Policies** feature from the Task Pane. Existing **Security Rule** sets are displayed in the Application Pane. The parameters comprising a selected **Security Rule** set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-67.
3. In the Application Pane, select the **Security Rule** you want to rename (Figure 5-77).
4. Select **Rename Rule**.
   The **Rename Rule** pop-up window is displayed (Figure 5-84).

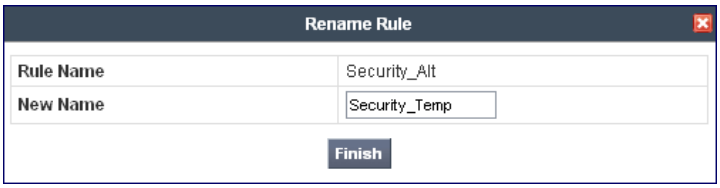


Figure 5-84 Rename Security Rule Pop-up Window.

5. Enter a new name for the **Security Rule** and select **Finish** to save your changes or **Cancel** to cancel the renaming operation and close the window without saving.

Deleting an Existing Security Rule

Use the following procedure to delete an existing **Security Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Security Rules** function from the **Domain Policies** feature from the Task Pane. Existing **Security Rule** sets are displayed in the Application Pane. The parameters comprising a selected **Security Rule** set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-67.
3. In the Applications Pane (Figure 5-77), select the **Security Rule** set you want to delete.
4. In the Content Area, select **Delete Policy**.

A pop-up window is displayed similar to that shown in Figure 5-85 asking you to confirm your request to delete the **Security Rule.**

5. Select **OK**.
   The **Security Rule** is deleted and the security Rule screen is redisplayed.

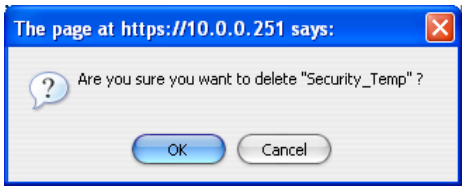


Figure 5-85 Delete Confirmation Pop-up Window.

Signaling Rules

Signaling Rules allow you to define the action to be taken (*Allow*, *Block*, *Block with Response*, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the E-SBC, they are parsed and "pattern-matched" against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

Creating a New Signaling Rule

Use the following procedure to create a new **Signaling Rule.**

Caution! A default Signaling Rule is provided by Sipera. Editing this default rule set is not recommended, as improper configuration may cause subsequent calls to fail.

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Signaling Rules** function of the **Domain Policies** feature from the Task Pane.
   Existing **Signaling Rule** sets are displayed in the Application Pane. The parameters comprising a selected **Signaling Rule** set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-86.

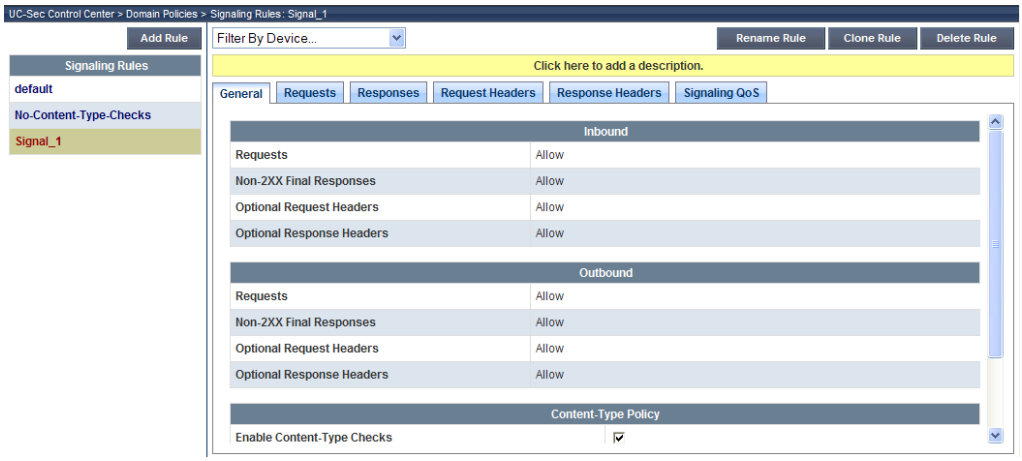


Figure 5-86 Signaling Rules Display Screen.

3. Select **Add Rule** from the Applications Pane.
   The **Add Signaling Rule** pop-up window is displayed (Figure 5-87).

Figure 5-87 Add Signaling Rule Pop-up Window.

4. Enter a name for the new **Signaling Rule** and select **Next.**
   The **Add Signaling Rule** pop-up window is displayed (Figure 5-88).

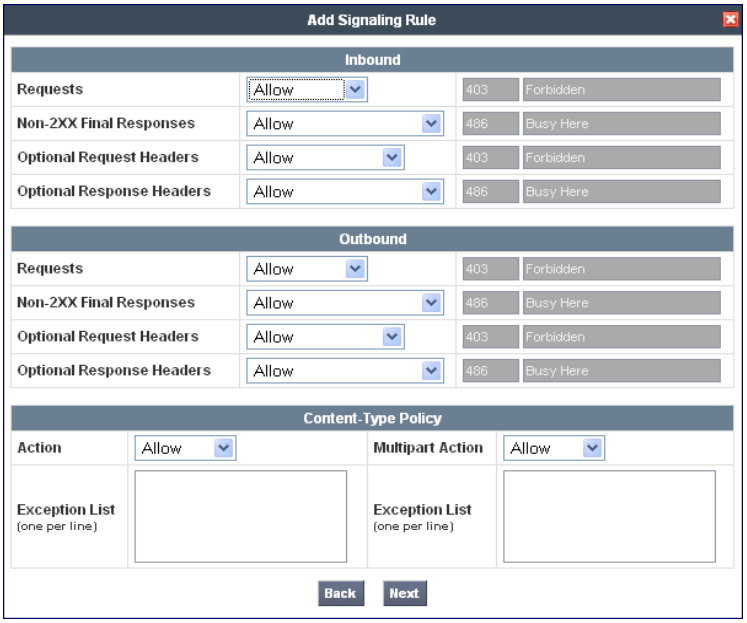


Figure 5-88 Add Signaling Rule Pop-up Window.

5. Provide the desired responses for each field (Table 5-11).

Table 5-11 Add Signaling Rule Pop-up Window Field Descriptions.

Field	Description
	Inbound
Requests	Drop-box allowing you to determine how incoming SIP request messages will be treated by this policy. Available options are **Allow** and **Block with…**. **Allow** — Allow all incoming SIP request messages. The corresponding fields to the right are inactivated. **Block with…** — Block all incoming SIP request messages and return the response indicated in the corresponding fields.
Non-2xx Final Responses	Drop-box allowing you to determine how incoming Non-2xx Final SIP response messages will be treated by this policy. Available options are **Allow** and **Change response to…**. **Allow** — Allow all incoming Non-2xx Final Response messages. The corresponding fields to the right are inactivated. **Change Response to…** — Block all incoming Non-2xx Final Response messages and return the response indicated in the corresponding fields.
Optional Request Headers	Drop-box allowing you to determine how optional request headers contained in incoming SIP messages will be treated by this policy. Available options are **Allow**, **Remove Header**, and **Block with…**. **Allow** — Allow all incoming SIP messages that contain optional request headers. The corresponding fields to the right are inactivated. **Remove Header** — Strip optional request headers from all incoming SIP messages and allow the message to proceed. **Block with…** — Block all incoming SIP messages that contain an optional request header and return the response indicated in the corresponding fields.

Optional Response Headers

Drop-box allowing you to determine how optional response headers contained in incoming SIP messages will be treated by this policy. Available options are **Allow**, **Remove Header**, and **Block with…**.

Allow	Allow all incoming SIP messages that contain optional response headers. The corresponding fields to the right are inactivated.
Remove Header	Strip optional response headers from all incoming SIP messages and allow the message to proceed.
Block with…	Block all incoming SIP messages that contain an optional response header and return the response indicated in the corresponding fields.

Outbound

Requests

Drop-box allowing you to determine how outbound SIP request messages will be treated by this policy. Available options are **Allow** and **Block with…**.

Allow	Allow all outbound SIP request messages. The corresponding fields to the right are inactivated.
Block with…	Block all outbound SIP request messages and return the response indicated in the corresponding fields.

Non-2xx Final Responses

Drop-box allowing you to determine how outbound Non-2xx Final SIP response messages will be treated by this policy. Available options are **Allow** and **Change response to…**.

Allow	Allow all outbound Non-2xx Final Response messages. The corresponding fields to the right are inactivated.
Change Response to…	Block all outbound Non-2xx Final Response messages and return the response indicated in the corresponding fields.

Optional Request Headers

Drop-box allowing you to determine how optional request headers contained in outbound SIP messages will be treated by this policy. Available options are **Allow**, **Remove Header**, and **Block with…**.

Allow	Allow all outbound SIP messages that contain optional request headers. The corresponding fields to the right are inactivated.
Remove Header	Strip optional request headers from all outbound SIP messages and allow the message to proceed.
Block with…	Block all outbound SIP messages that contain an optional request header and return the response indicated in the corresponding fields.

Optional Response Headers	Drop-box allowing you to determine how optional response headers contained in outbound SIP messages will be treated by this policy. Available options are **Allow**, **Remove Header**, and **Block with…**. **Allow** – Allow all outbound SIP messages that contain optional response headers. The corresponding fields to the right are inactivated. **Remove Header** – Strip optional response headers from all outbound SIP messages and allow the message to proceed. **Block with…** – Block all outbound SIP messages that contain an optional response header and return the response indicated in the corresponding fields.
Content-Type Policy	
Action	Drop-down menu from which you choose the action to be taken by the E-SBC security device when considering the content portion of SIP signaling messages. Available options are **Allow** and **Remove**. **Allow** – Allows the content in each SIP signaling message to pass, with the exception of those items contained in the **Exceptions List** which are removed. **Remove** – Removes all content from each SIP signaling message, with the exception of the items contained in the **Exceptions List** which are allowed to pass.
Exception List	The specific terms which are to be passed ort blocked, according to the action specified in the **Action** field.
Multipart Action	Drop-down menu from which you choose the action to be taken by the E-SBC security device when considering the multi-part content portion of SIP signaling messages. Available options are **Allow** and **Remove**. **Allow** – Allows the multi-part content in each SIP signaling message to pass, with the exception of those items contained in the **Exceptions List** which are removed. **Remove** – Removes all the multi-part content from each SIP signaling message, with the exception of the items contained in the **Exceptions List** which are allowed to pass.
Exception List	The specific terms which are to be passed ort blocked, according to the action specified in the **Multipart Action** field.

6. Select **Next.**
   The **Add Signaling Rule: QoS** pop-up window is displayed (Figure 5-89).
7. Referring to Table 5-12, provide the desired responses for each field.

Table 5-12 Add Signaling Rule: QoS Pop-up Window Field Descriptions.

Field	Description
Enabled	A checkbox indicating whether or not the **Signaling Quality-of-Service (QoS)** feature will be enabled. Check the box (☑) to enable the Signaling QoS statistics feature or leave the box blank (☐) to disable the Signaling QoS statistics feature.
ToS	Radio button allowing you to select Type-of-Service (ToS)
DSCP	The value of the six most significant values of the **Differentiated Services** (DiffServ) field. These values, referred to as the **Differentiated Services Point Code** (DSCP), are used to provide guaranteed service to critical network traffic. Use the pull-down menu to select the desired DSCP value.

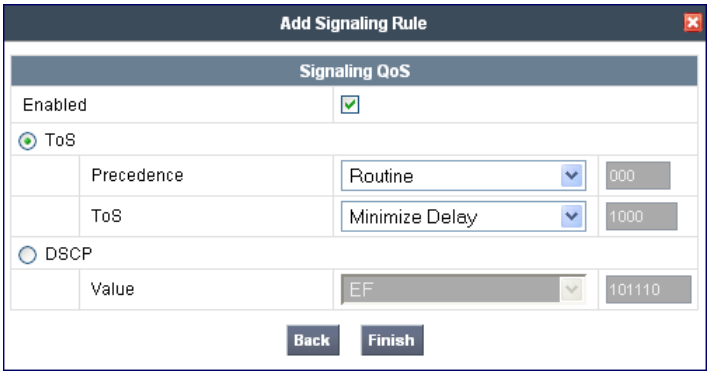


Figure 5-89 Add Signaling Rule: QoS Pop-up Window.

8. Select **Finish.**
   The new **Signaling Rule** set is added to the **Signaling Rule** list in the Application Pane of the E-SBC Control Center (Figure 5-90).

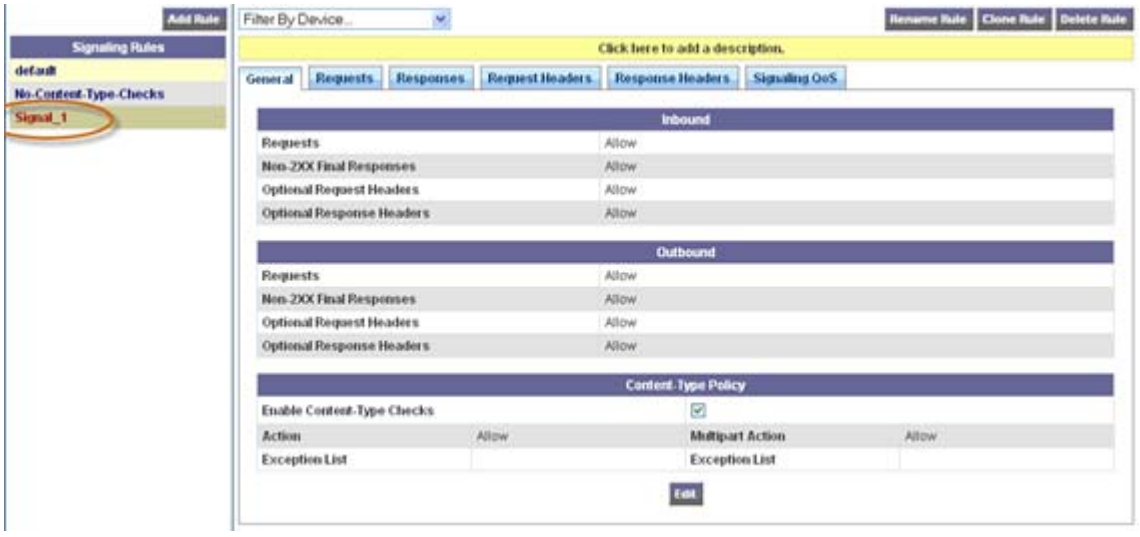


Figure 5-90 Updated Signaling Rule Screen.

Editing an Existing Signaling Rule

Signaling Rules are edited by selecting the desired parameter tab from the Content Area and adding a new parameter set or changing an existing set. Parameter tabs which can be edited are: **General, Requests, Responses, Request Headers, Response Headers,** and **Signaling QoS.** Together the functions provided by these tabs characterize a particular signaling packet flow. Use the following procedure to add or edit these values from the Signaling Rules screen (Figure 5-91).

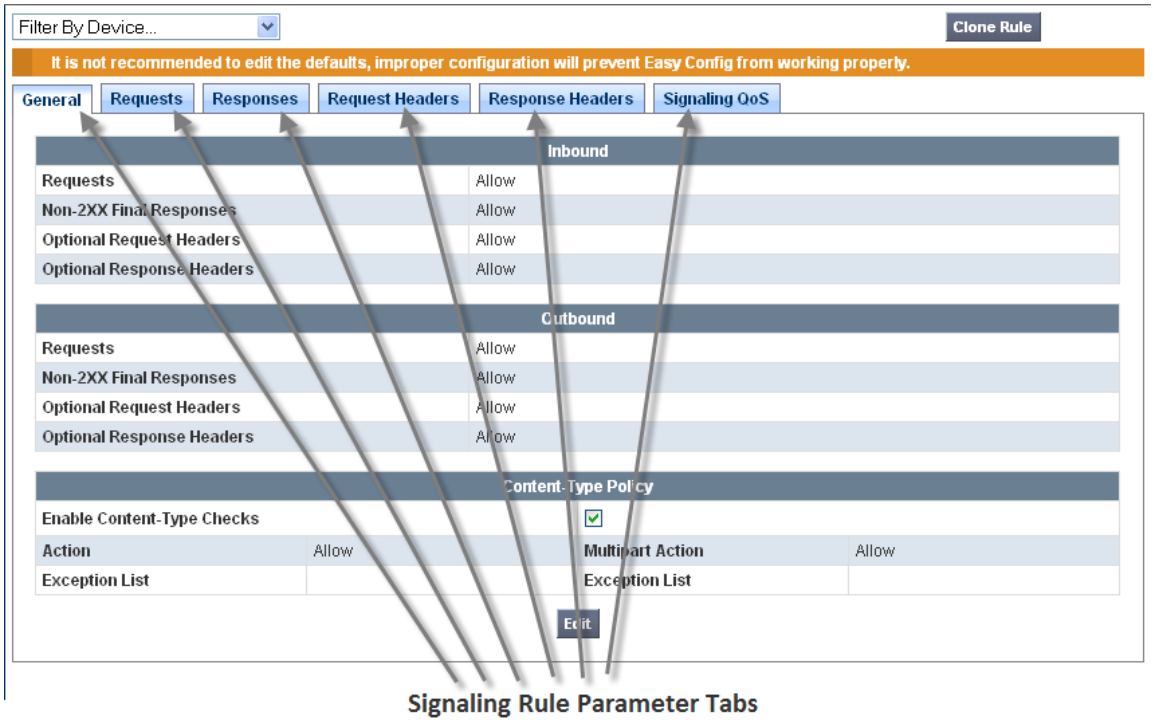


Figure 5-91 Signaling Rule Parameter Tabs.

General Parameters Tab

Use the following procedure to edit the **General** parameters for an existing **Signaling Rule.**

1. Select the **General** parameter tab.
   General signaling parameters will be displayed in the Content Area.

2. Select **Edit.**
   The **General Control** pop-up window is displayed (Figure 5-92).

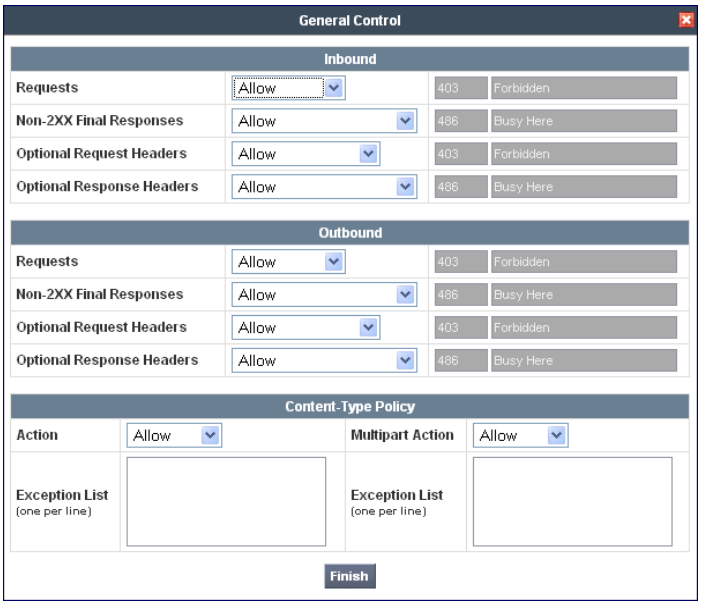


Figure 5-92 General Control Pop-up Window.

3. Edit the desired responses for each field by selecting the corresponding radio button (if necessary, refer back to Table 5-11).
4. Select **Finish**.

Requests Parameters Tab

Adding Request Parameters

Use the following procedure to add **In Request** and **Out Request** parameters for a **Signaling Rule** (if none are already defined). **In Requests** refer to SIP message requests being directed to enterprise end-points. **Out Requests** refer to SIP message requests being directed to end-points external to the enterprise.

1. Select the **Requests** parameter tab.
   The **Requests** parameters will be displayed in the Content Area.
2. Select either the **Add In Request Control** or **Add Out Request Control** button.
   The corresponding **Add Request Control** pop-up window is displayed (Figure 5-93).

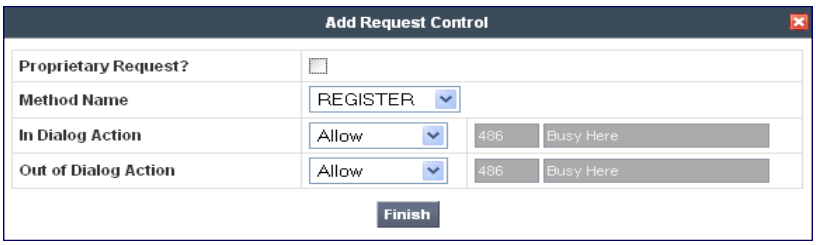


Figure 5-93 Add Request Control Pop-up Window.

3. Provide the desired responses for each field (Table 5-13).

Table 5-13 Add Request Control Pop-up Window Field Descriptions.

Field	Description
Proprietary Request?	A checkbox indicating whether or not the **Request** being defined is a non-standard SIP request. Check the box (☑) to designate a non-standard SIP request message or leave the box blank (☐) to indicate a standard SIP request message.
Method Name	The type of standard SIP request message for which this signaling policy will apply. Select the desired **Method Name** from the corresponding drop-down box. This field will be grayed-out if the **Proprietary Request?** field is checked ☑.
In-Dialog Action	The action to be taken for the SIP request message defined in the **Method Name** field when the session is in-dialog. Available action options are **Allow**, and **Block with Response**. If the **Block with Response** selection is made, the two fields to the right will be activated, allowing you to provide the type of response to be sent.
Out-of-Dialog Action	The action to be taken for the SIP request message defined in the **Request** field when the session is out-of-dialog. Available action options are **Allow**, **Block**, and **Block with Response**. If the **Block with Response** selection is made, the two fields to the right will be activated, allowing you to provide the type of response to be sent.

4. Select **Finish.**
   The selected values are displayed in the **Requests** tab display (Figure 5-94).

Figure 5-94 Updated Requests Parameters Tab.

Editing Request Parameters

Use the following procedure to edit existing **Add In Request Control** or **Add Out Request Control** parameters.

1. Select the **Requests** parameter tab.
   The **Requests** parameters will be displayed in the Content Area.

2. Select the edit ( ) icon corresponding to the specific request control parameter set you want to edit.
   The **Edit Request Control** pop-up window is displayed (Figure 5-95).

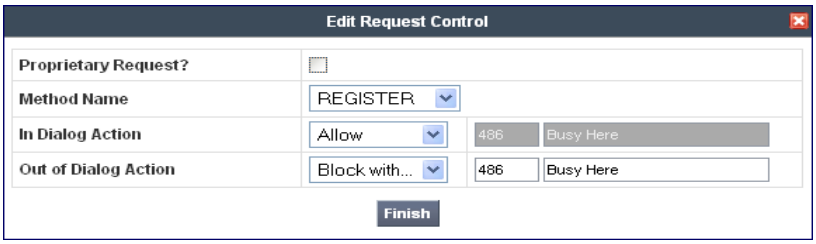


Figure 5-95 Edit Request Control Pop-up Window.

3. Edit the information in the pop-up window according to the information contained in Table 5-13.
4. Select **Finish.**

Responses Parameters Tab

Adding Response Parameters

Use the following procedure to add **In Response** and **Out Response** parameters for a **Signaling Rule** (if none are already defined). **In Responses** refer to SIP message responses being directed to enterprise end-points. **Out Responses** refer to SIP message responses being directed to end-points external to the enterprise.

1. Select the **Responses** parameter tab.
   The **Response** parameters will be displayed in the Content Area.
2. Select either the **Add In Response Control** or **Add Out Response Control** button.
   The **Add Response Control** pop-up window is displayed (Figure 5-96).

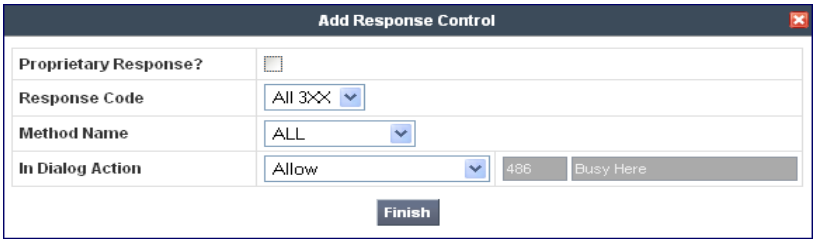


Figure 5-96 Add Response Control Pop-up Window.

3. Select the desired responses for each field (Table 5-14).

Table 5-14 Add Response Control Pop-up Window Field Descriptions.

Field	Description
Proprietary Response?	A checkbox indicating whether or not the **Response** being defined is a non-standard SIP response. Check the box (☑) to designate a non-standard SIP response or leave the box blank (☐) to indicate a standard SIP response.
Response Code	The specific response message to be sent for the received SIP request. Select the desired response from the drop-down box. This field will be grayed-out if the **Proprietary Request?** field is checked ☑.
Method Name	The SIP message which will trigger the **Response Code** selected in the previous field. Select the desired SIP message from the drop-down box.
In-Dialog Action	The action to be taken if the proprietary response is generated in-dialog (session established). Available action options are **Allow** and **Change Response to …**. If the **Change Response to …** selection is made, the two fields to the right will be activated, allowing you to provide the type of response to be sent.

4. Select **Finish.**
   The selected values are displayed in the **Responses** tab display (Figure 5-97).

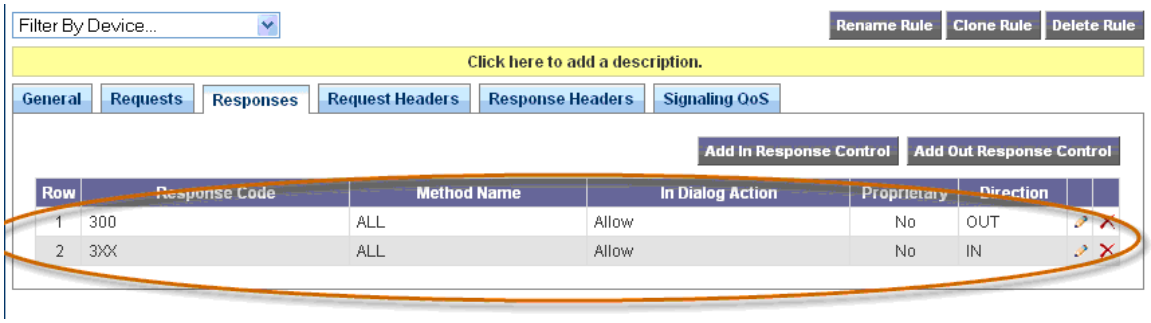


Figure 5-97 Updated Responses Parameters Tab.

Editing Response Parameters

Use the following procedure to edit existing **Add In Response Control** or **Add Out Response Control** parameters.

1. Select the **Reponses** parameter tab.
   The **Response** parameters will be displayed in the Content Area.
2. Select the edit (✎) icon corresponding to the specific response control parameter set you want to edit.
   The **Edit Response Control** pop-up window is displayed (Figure 5-98).
3. Edit the information in the pop-up window according to the information contained in Table 5-14.

4. Select **Finish.**

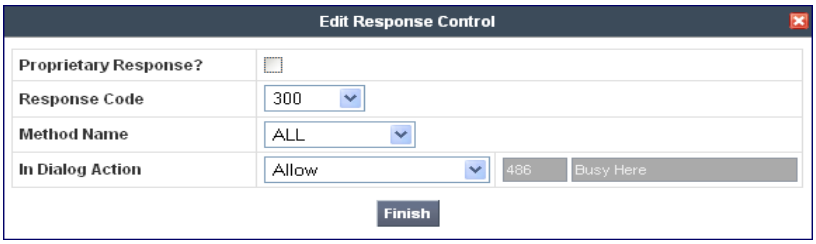


Figure 5-98 Edit Response Control Pop-up Window.

Request Headers Parameters Tab

Adding Request Header Parameters

Use the following procedure to add **In Header Control** and **Out Header Control** parameters for a **Signaling Rule** (if none are already defined.) **In Header Control** parameters are applied to the headers of SIP messages directed to enterprise end-points. **Out Header Control** parameters are applied to the headers of SIP messages directed to end-points external to the enterprise.

1. Select the **Request Headers** parameter tab.
   The **Request Headers** parameters will be displayed in the Content Area.
2. Select either the **Add In Header Control** or **Add Out Header Control** button.
   The **Add Header Control** pop-up window will be displayed (Figure 5-99).

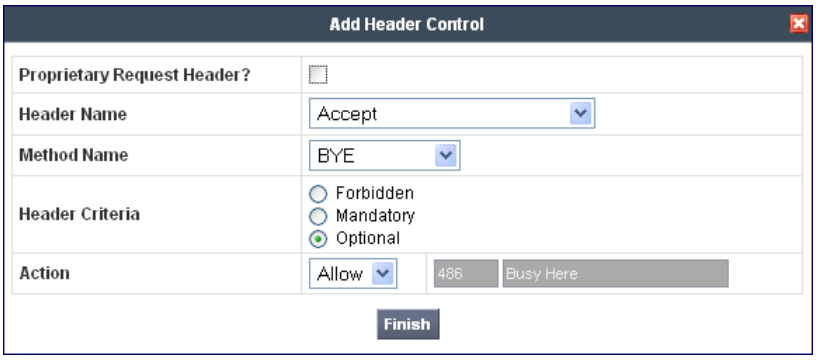


Figure 5-99 Add Header Control Pop-up Window.

3. Select the desired responses for each field (Table 5-15).

Table 5-15. Add Header Control Pop-up Window Field Descriptions.

Field	Description
Proprietary Request Header?	A checkbox indicating whether or not the header being defined is a non-standard SIP header. Check the box (☑) to designate a non-standard SIP header or leave the box blank (☐) to indicate a standard SIP header.
Header Name	The name of the proprietary SIP header. Make your selection from the corresponding drop-down list. This field will be grayed-out if the **Proprietary Request Header?** field is checked ☑.
Method Name	The context or call sequence in which the header is contained.
Header Criteria	Whether or not the presence of the header is **Forbidden**, **Mandatory**, or **Optional**.
Action	The action to be taken if the header is present in the SIP message designated in the **Method Name** field. Depending upon selection made in the **Header Criteria** field, available actions are: **Criteria** / **Action** **Forbidden**: • Remove header • Block with … **Mandatory**: • Bock with … **Optional**: • Allow If the **Block with …** Action is selected, then the two fields to the right are activated, allowing you to enter the response message to be sent in reply.

4. Select **Finish.**
   The selected values are displayed in the **Request Headers** tab display.

Editing Request Header Parameters

Use the following procedure to edit existing **Request Header** parameters.

1. Select the **Request Headers** parameter tab.
   The **Request Headers** parameters will be displayed in the Content Area.
2. Select the edit ( ) icon corresponding to the specific request header parameter set you want to edit.
   The **Edit Header Control** pop-up window is displayed (Figure 5-100).

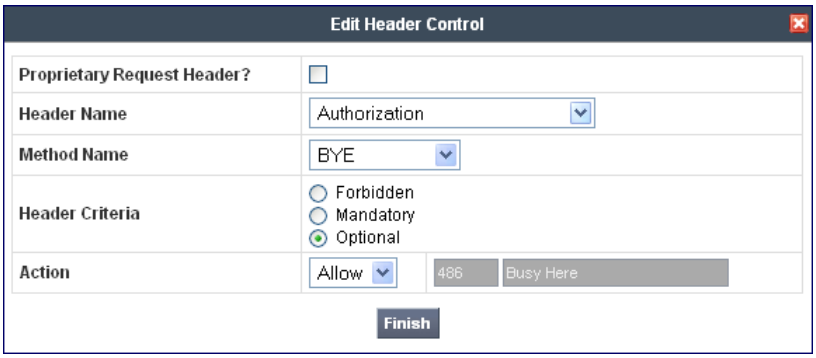


Figure 5-100 Edit Header Control Pop-up Window.

3. Edit the information in the pop-up window according to the information contained in Table 5-15.
4. Select **Finish**.

Response Headers Parameters Tab

Adding Response Header Parameters

Use the following procedure to add **In Header Control** and **Out Header Control** parameters for a **Signaling Rule** if none are already defined. **In Header Control** parameters are applied to the headers of SIP response messages destined for enterprise end-points. **Out Header Control** parameters are applied to the headers of SIP response messages destined for end-points external to the enterprise.

1. Select the **Response Headers** parameter tab.
   The **Response Headers** parameters will be displayed in the Content Area.
2. Select either the **Add In Header Control** or **Add Out Header Control** button.
   The **Add Header Control** pop-up window will be displayed (Figure 5-101).

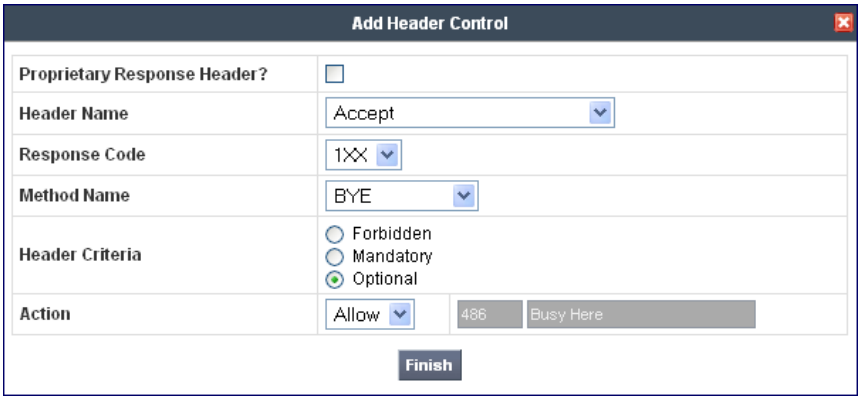


Figure 5-101 Add Header Control Pop-up Window.

3. Select the desired responses for each field using the corresponding checkbox, drop-down menus, and radio buttons (Table 5-16).

Table 5-16 Add Header Control Pop-up Window Field Descriptions.

Field	Description
Proprietary Response Header?	A checkbox indicating whether or not the header being defined is a non-standard SIP response header. Check the box (☑) to designate a non-standard SIP response header or leave the box blank (☐) to indicate a standard SIP response header.
Header Name	The standard SIP message header for which the signaling policy will apply. Make your selection from the corresponding drop-down list. This field will be grayed-out if the **Proprietary Response Header?** field is checked ☑.
Response Code	The code to be sent as the SIP response. Select the desired code from the drop-down box.
Method Name	SIP signaling message name (**CANCEL**, **INVITE**, **PUBLISH**, etc.). Make your selection from the corresponding drop-down list.
Header Criteria	Whether or not the presence of the header in the response field is **Forbidden**, **Mandatory**, or **Optional**.
Action	The action to be taken if the header is present in the SIP response. Available actions are: **Criteria** / **Action** **Forbidden** • Remove header • Change response to … **Mandatory** • Change response to … **Optional** • Allow If the **Change response to …** Action is selected, then the two fields to the right are activated, allowing you to enter the new response.

4. Select **Finish.**
   The selected values are displayed in the **Response Headers** tab (Figure 5-102), as shown in the example below.

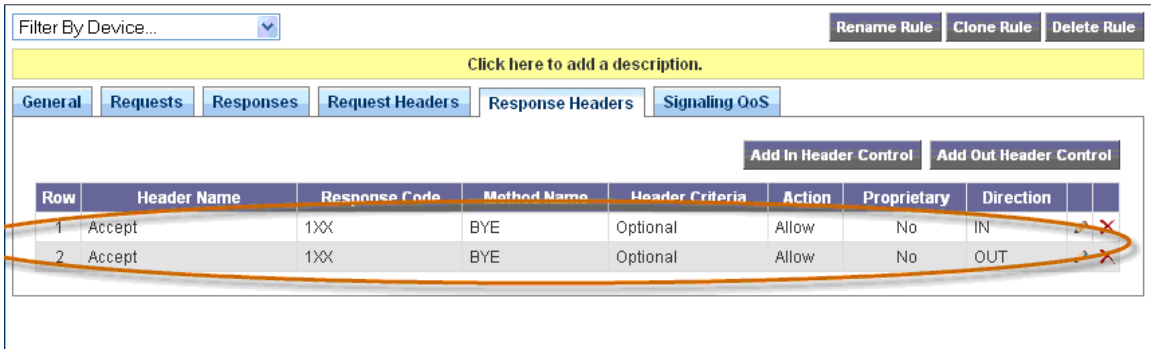


Figure 5-102 Updated Responses Headers Parameters Tab.

Editing Response Header Parameters

Use the following procedure to edit existing **Response Header** parameters.

1. Select the **Response Headers** parameter tab.
   The **Response Headers** parameters will be displayed in the Content Area.
2. Select the edit ( ) icon corresponding to the specific request header parameter set you want to edit.
   The **Edit Response Header Parameters** pop-up window is displayed (Figure 5-103).
3. Edit the information in the pop-up window according to the information contained in Table 5-16.
4. Select **Finish.**

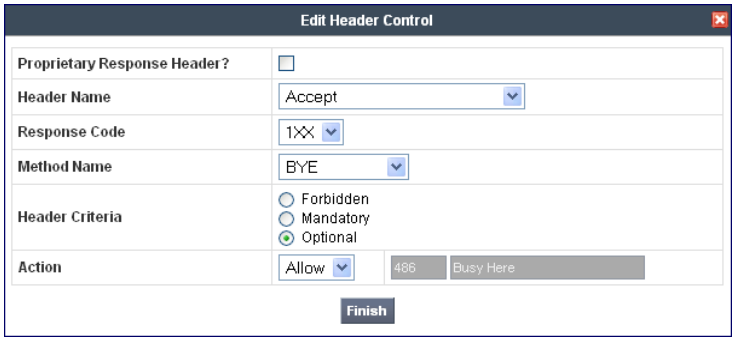


Figure 5-103 Edit Response Header Control Pop-up Window.

Signaling QoS Parameters Tab

Use the following procedure to edit the Signaling QoS parameter set.

1. Select the **Signaling QoS** parameter tab.
   The **QoS** parameters will be displayed in the Content Area.
2. Select **Edit.**
   The **Signaling QoS** pop-up window (Figure 5-104) is displayed.

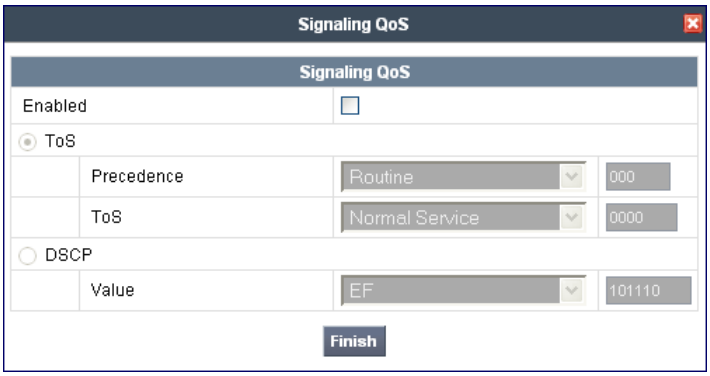


Figure 5-104 Signaling QoS Pop-up Window.

Edit the information in the pop-up window according to the information contained in

3. Table 5-12.
4. Select **Finish.**

Cloning an Existing Signaling Rule

Use the following procedure to make an exact copy (clone) of an existing **Signaling Rule.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Signaling Rules** function of the **Domain Policies** feature from the Task Pane. Existing **Signaling Rule** sets are displayed in the Application Pane. The parameters comprising a selected **Signaling Rule** set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-86.
3. In the Application Pane, select the **Signaling Rule** you want to clone (Figure 5-105). The parameters for the selected **Signaling Rule** will be displayed in the Content Area.
4. Select **Clone Rule.**
   The **Clone Rule** pop-up window is displayed (Figure 5-106).
5. Enter a name for the new **Signaling Rule** and select **Finish** to save your changes or **Cancel** to cancel the cloning operation and close the window without saving.
   A duplicate **Signaling Rule** set will be created with the new name and displayed in the Applications Pane (Figure 5-107).

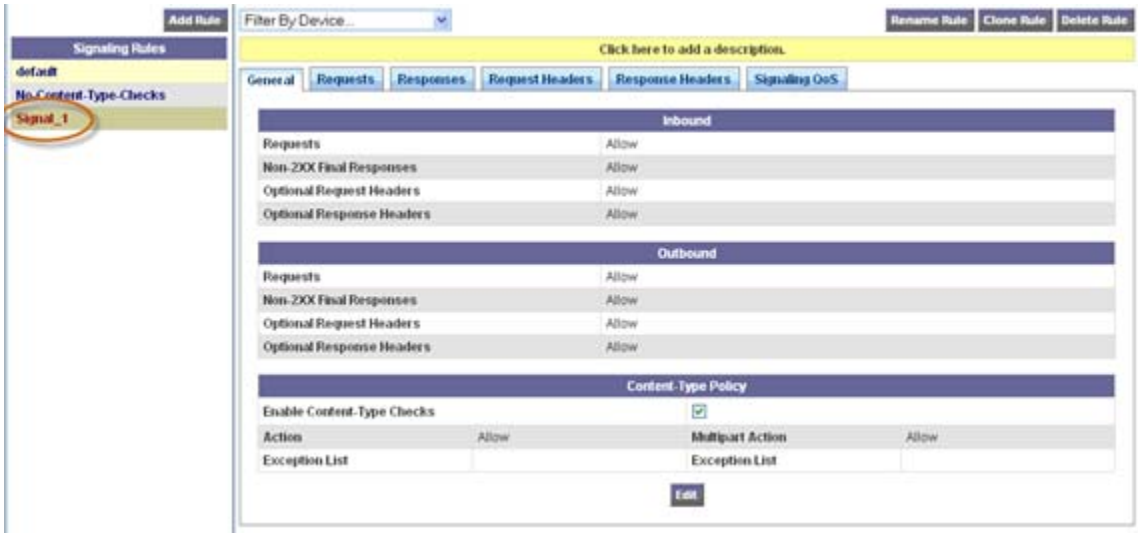


Figure 5-105 Selecting an Existing Signaling Rule.

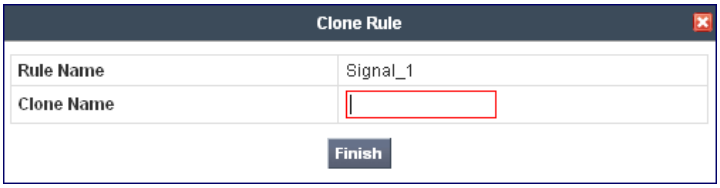


Figure 5-106 Clone Rule Pop-up Window.

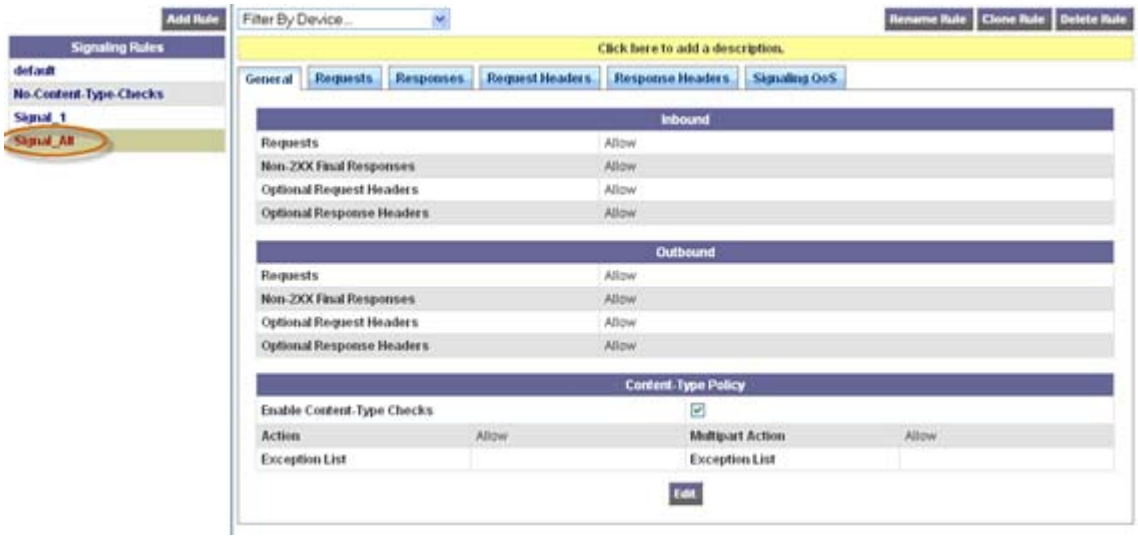


Figure 5-107 Updated Signaling Rules Display.

Renaming an Existing Signaling Rule

Use the following procedure to rename an existing **Signaling Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Signaling Rules** function of the **Domain Policies** feature from the Task Pane. Existing **Signaling Rule** sets are displayed in the Application Pane. The parameters comprising a selected **Signaling Rule** set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-86.
3. In the Application Pane, select the **Signaling Rule** you want to rename (Figure 5-105).
4. Select **Rename Rule**.
   The **Rename Rule** pop-up window is displayed (Figure 5-108).
5. Enter a new name for the **Signaling Rule** and select **Finish** to save your changes or **Cancel** to cancel the cloning operation and close the window without saving.
   The name of the **Signaling Rule** is changed.

Figure 5-108 Rename Rule Pop-up Window.

Deleting an Existing Signaling Rule

Use the following procedure to delete an existing **Signaling Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Signaling Rules** function of the **Domain Policies** feature from the Task Pane. Existing **Signaling Rule** sets are displayed in the Application Pane. The parameters comprising a selected **Signaling Rule** set are displayed in the Content Area of the E-SBC Control Center.
3. In the Application Pane, select the **Signaling Rule** you want to delete.
4. In the Content Area, select **Delete Rule**.
   A pop-up window is displayed similar to that shown below in Figure 5-109, asking you to confirm your request to delete the **Signaling Rule** set.
5. Click **OK**.
   The **Signaling Rule** is deleted.

Figure 5-109 Delete Confirmation Pop-up Window.

Time-of-Day (ToD) Rules

A **Time-of-day (ToD) Rule** allows you to determine when the domain policy it is assigned to will be in effect. ToD Rules provide complete flexibility to fully accommodate the enterprise by, not only determining when a particular domain policy will be in effect, but also to whom it will apply, and for how long it will remain in effect.

Creating a New ToD Rule

Use the following procedure to create a new **Time-of-Day Rule.**

Caution!

A default set of **Time-of-Day** rule named **default** is provided by Sipera. Editing this rule set is not recommended, as improper configuration may cause subsequent calls to fail.

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Time-of-Day Rules** function of the **Domain Policies** feature from the Task Pane. Existing Time-of-Day Rules are displayed in the Application Pane. The parameters comprising a selected Time-of-Day policy are displayed in the Content Area of the E-SBC Control Center. Select **Add Rule** in the Application Pane.
   The **Add Rule** pop-up window is displayed (Figure 5-111).

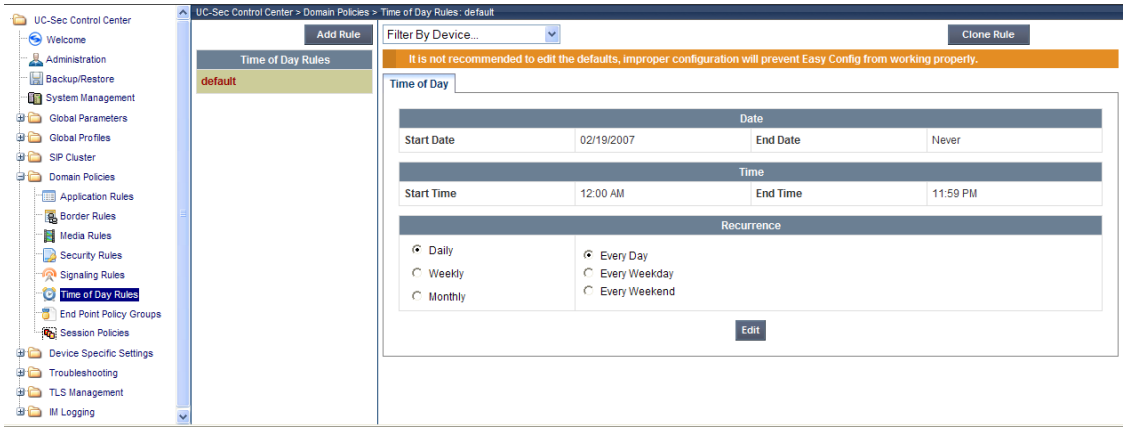


Figure 5-110 Time-of-Day Rules Display Screen.

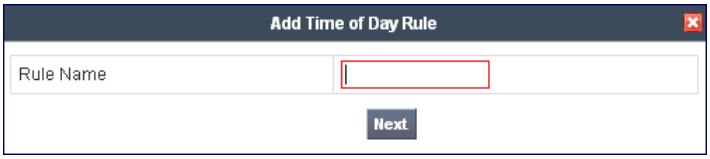


Figure 5-111 Add Rule Pop-up Window.

3. Enter a name for the ToD rule and press **Next.**
   The **Add ToD Parameters** pop-up window is displayed (Figure 5-112).

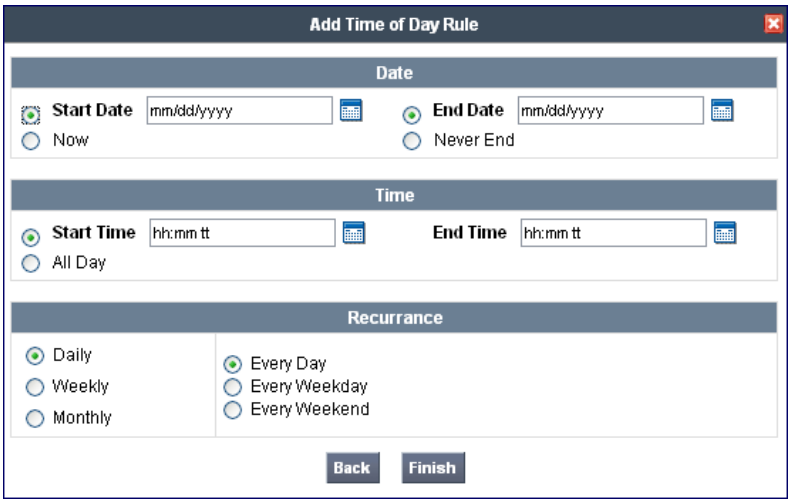


Figure 5-112 Add ToD Parameters Pop-up Window.

4. Enter the requested information into the appropriate fields.
   Table 5-17 describes each user-definable field displayed in the **Add Time of Day Rule** pop-up window.

Table 5-17 Add Time of Day Rule Pop-Up Window Field Descriptions.

Field	Description
	Date
Start Date	The day on which the ToD rule will automatically take effect. Click the **Show Calendar** icon to select the desired day.
Now	Indicates that the ToD rule is to take effect immediately.
End Date	The day on which the ToD rule will automatically end. Click the **Show Calendar** icon to select the desired day.
Never End	Indicates that the ToD rule is to remain in effect in perpetuity or until such time as an **End Date** is distinctly defined.
	Time
Start Time	The specific time on the designated day that the ToD rule will take effect. Click the **Show Calendar** icon to select the desired start time.
All Day	Indicates that the ToD policy is to remain in effect for the entire 24-hour period.
End Time	The specific time on the designated day that the rule will cease being applied. Click the **Show Calendar** icon to select the desired ending time.

Field	Description	
	Recurrence	
Daily, **Weekly**, or **Monthly**	When the ToD rule is to automatically be placed into effect.	
	Daily	Allows you to determine which "daily' cycle will be used for automatic activation: **Every Day** – the ToD rule will automatically take effect at the designated time on each weekday (weekends and holidays included). **Every Weekday** – the ToD rule will only automatically take effect on Monday through Friday. **Every Weekend** – the ToD rule will only automatically take effect on Saturday and Sunday.
	Weekly	Allows you to determine which weekly cycle the ToD rule will be used for automatic activation. You can select every week, every other week, etc. by selecting the appropriate cycle in the **Weeks** field. Also, you can select which particular day in the designated week the ToD rule will take effect by checking the appropriate checkbox.
	Monthly	Allows you to designate the specific day of a monthly cycle that the ToD policy will take effect.

5. Select **Finish.**
   The new Time-of-Day Rule is displayed in the Applications Pane and its parameters in the Content Area (Figure 5-113).

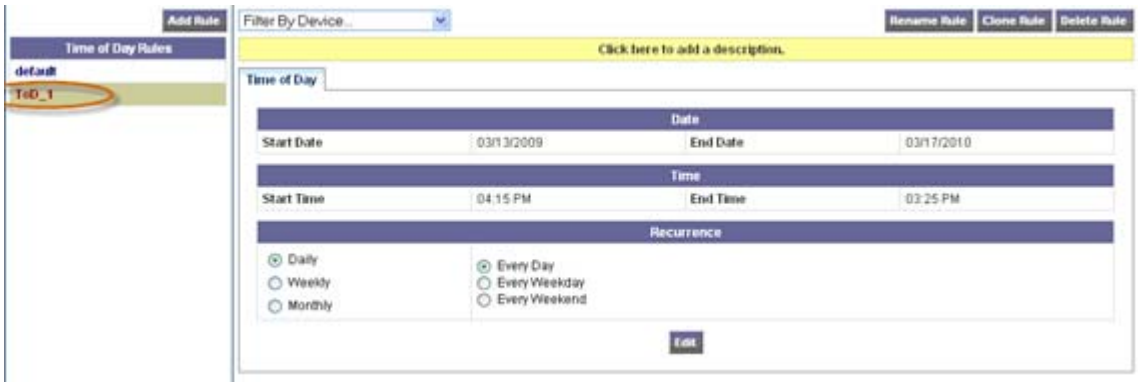


Figure 5-113 New ToD Rule.

Cloning an Existing ToD Rule

Use the following procedure to make an exact copy (clone) of an existing **Time-of-Day Rule.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Time-of-Day Rules** function of the **Domain Policies** feature from the Task Pane.

Existing **Time-of-Day Rules** are displayed in the Application Pane. The parameters comprising a selected **Time-of-Day** policy are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-110 Time-of-Day **Rules Display Screen.**

3. In the Application Pane, select the **Time-of-Day Rule** you want to clone (Figure 5-114).
   The parameters for that **Time-of-Day Rule** will be displayed in the Content Area.
4. Select **Clone Rule.**
   The **Clone Rule** pop-up window is displayed (Figure 5-115).

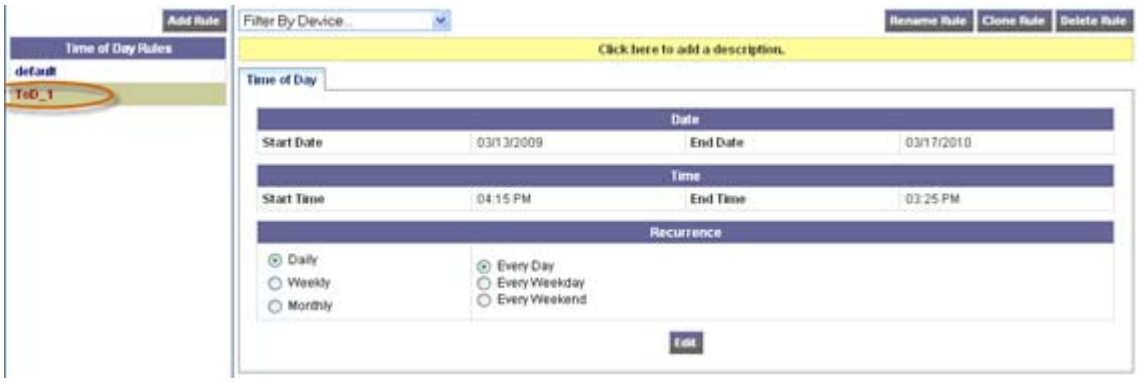


Figure 5-114 Selecting an Existing ToD Rule.

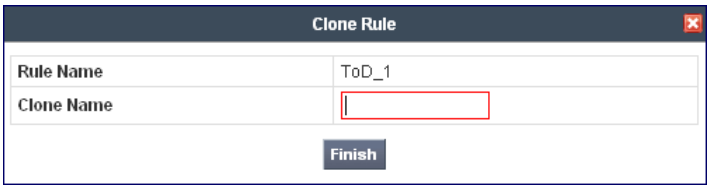


Figure 5-115 Clone Rule Pop-up Window.

5. Enter a name for the new **Time-of-Day Rule.**
6. Select **Finish** to save the new **Time-of-Day Rule** or **Cancel** to cancel the cloning process and close the window without saving.

Editing an Existing ToD Rule

Use the following procedure to edit an existing **Time-of-Day Rule.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Time-of-Day Rules** function of the **Domain Policies** feature from the Task Pane.
   Existing **Time-of-Day Rules** are displayed in the Application Pane. The parameters comprising a selected **Time-of-Day** policy are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-110 Time-of-Day **Rules Display Screen.**

   In the Application Pane, select the **Time-of-Day Rule** you want to edit (Figure 5-116).
   The parameters for that **Time-of-Day Rule** will be displayed in the Content Area.
3. Select **Edit.**

The **Edit Time-of-Day Rule** pop-up window is displayed (Figure 5-117).

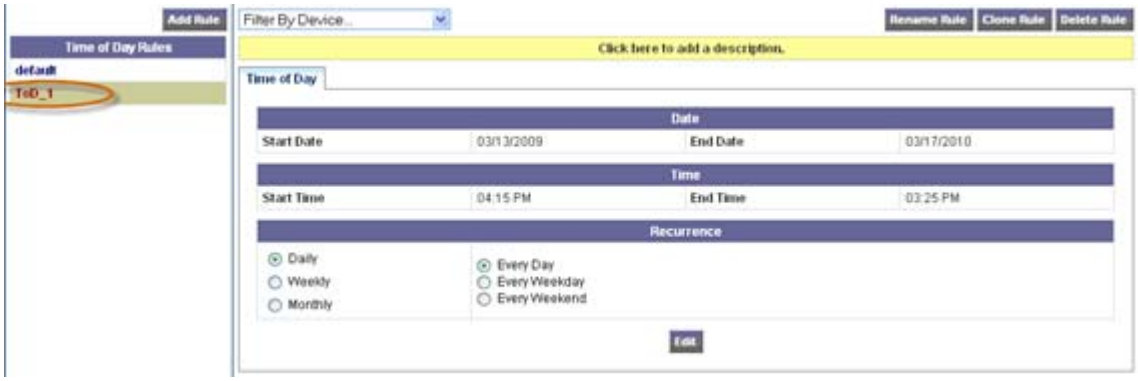


Figure 5-116 Selecting an Existing Time-of-Day Rule.

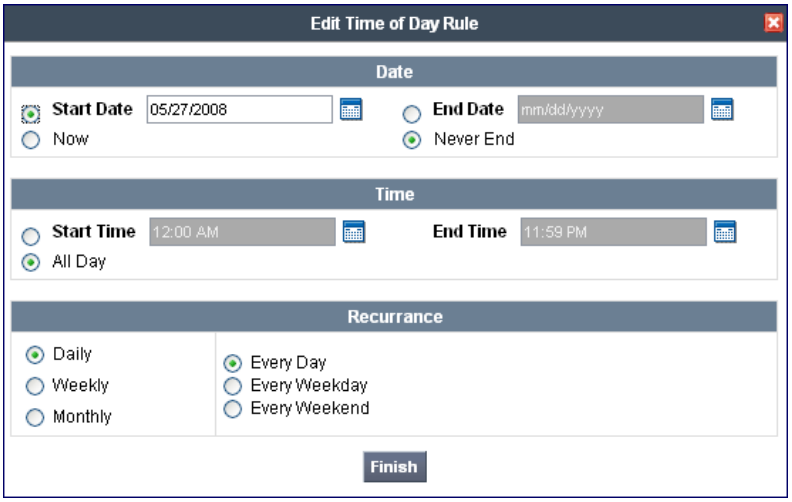


Figure 5-117 Edit Time-of-Day Rule Pop-up Window.

4. Edit the desired fields.
5. Select **Finish** to save your changes or **Cancel** ( ) to close the window without saving.

In addition to editing fields, you are also able to enter general descriptive text into the yellow-colored area just above the **Time-of-Day Info** tab. This information will be displayed whenever an **Admin** account that selects this rule.

Renaming an Existing ToD Rule

Use the following procedure to rename an existing **Time-of-Day Rule.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Time-of-Day Rules** function of the **Domain Policies** feature from the Task Pane. Existing **Time-of-Day Rules** are displayed in the Application Pane. The parameters comprising a selected **Time-of-Day** policy are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-110 Time-of-Day **Rules Display Screen.**

3. In the Application Pane, select the **Time-of-Day Rule** you want to rename (Figure 5-116).
   The parameters for that **Time-of-Day Rule** will be displayed in the Content Area.
4. Select **Rename Rule**.
   The **Rename Rule** pop-up window is displayed (Figure 5-118).
5. Enter a new name for the existing **Time-of-Day Rule** in the **New Name** field.
6. Select **Finish** to save the existing **Time-of-Day Rule** with the new name or **Cancel** to terminate the renaming process and close the window without saving.

Figure 5-118 Rename Rule Pop-up Window.

Deleting an Existing ToD Rule

Use the following procedure to delete an existing **Time-of-Day Rule**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Time-of-Day Rules** function of the **Domain Policies** feature from the Task Pane.
   Existing **Time-of-Day Rules** are displayed in the Application Pane. The parameters comprising a selected **Time-of-Day** policy are displayed in the Content Area of the E-SBC Control Center.
3. In the Application Pane, select the **Time-of-Day Rule** you want to delete (Figure 5-116).
   The parameters for that **Time-of-Day Rule** will be displayed in the Content Area.
4. In the Content Area, select **Delete Rule**.
   A pop-up window is displayed similar to that shown in Figure 5-119 asking you to confirm your request to delete the **Time-of-Day Rule**.
5. Click **OK**.
   The **Time-of-Day Rule** is deleted.

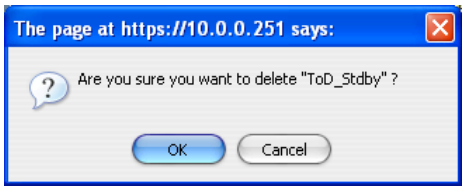


Figure 5-119 Delete Confirmation Pop-up Window.

End-Point Policy Groups

The End-Point Policy Group feature allows you to create *Policy Sets* and *Policy Groups*. A *Policy Set* is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and ToD. (Each of which was creating using the procedures contained in the previous sections.) A *Policy Group* is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of E-SBC security features to very specific types of SIP signaling messages traversing through the enterprise.

As various types of signaling traffic pass through the enterprise they are exhaustively inspected by the E-SBC security product and 'compared' against the criteria defined by which ever Policy Group is active at that time, as determined by its constituent ToD policy. The specific Policy Set the packets are compared to is determined by the order in which they are placed in the parent Policy Group; which is normally from most restrictive to least restrictive.

The packets are compared to each Policy Set in the Policy Group's prioritized list from top to bottom beginning with the most restrictive down to the least restrictive. As each individual packet's Policy Set match is found, it is further qualified by the Policy Set's Time-of-Day (ToD) rule and by the Policy Set number (priority number). When Policy Sets have ToD rules that match, the Policy Set number is used for the final selection, and the higher priority number wins. The selected Policy Set is applied to the packet and an action is taken.

When a 'match' is found, one of three possible actions is taken, depending upon the policies defined in the Policy Group: **ALLOW** (allow the packet to proceed to its destination without applying any security features), **DENY** (immediately block the packet), or **APPLY** (apply the security features defined by the Policy Set(s)).

Note

The user can add different Policy Sets with different ToD rules in the same End Point Policy Group.

Based on each ToD rule, a different security configuration can be applied to an incoming message.

Creating a New Policy Group

Use the following procedure to create a new **Policy Group.**

Caution!

A number of default Policy Groups whose name begins with '**default**' are provided by Sipera. Editing these rule sets is not recommended, as improper configuration may cause subsequent calls to fail.

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **End-Point Policy Groups** function from the **Domain Policies** feature from the Task Pane.
   Existing **End-Point Policy Groups** are displayed in the Application Pane. The End-Point Policy Sets comprising a selected **End-Point Policy Group** are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-120.

Note At least one Security Rule set must be defined before a Policy Group can be created. If a Security Rule does not exist, a pop-up window will be displayed telling you to create one.

3. Select **Add Policy Group** from the Applications Pane.
   The **Add Policy Group Name** pop-up window is displayed (Figure 5-121).

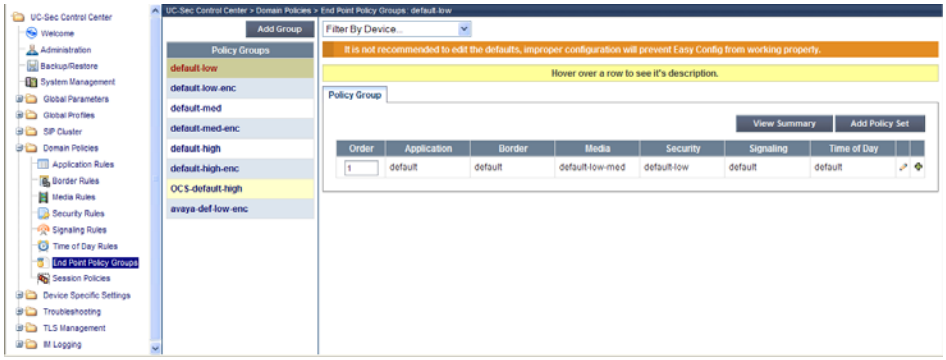


Figure 5-120 Policy Groups Display Screen.

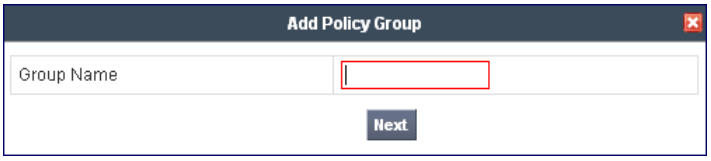


Figure 5-121 Add Policy Group Name Pop-up Window.

4. Provide a name for the new Policy Group and click **Next.**
   The **Add Policy Group** screen is displayed (Figure 5-122).

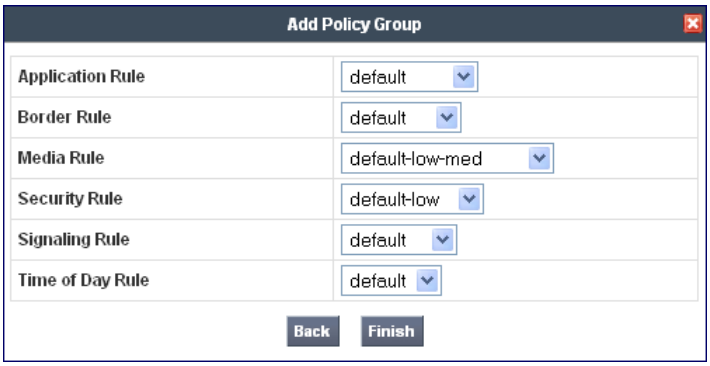


Figure 5-122 Add Policy Group Screen.

5. Enter the requested information using the drop-down menus corresponding to each field name in the window (Table 5-18).

   Selecting the **Cancel** icon cancels the operation and closes the window without creating a new Policy Group.

Table 5-18 Add Policy Group Parameters Screen Field Descriptions.

Field	Description
Application Rule	The name of the Application Rule that will determine which applications will have this Policy group applied.
Border Rule	The name of the Border Rule that will determine which applications will have this Policy group applied.
Media Rule	The name of the Media Rule that will be used to match media packets.
Security Rule	The name of the Security Rule that will determine which E-SBC security policies will be applied when this Policy Group is activated.
Signaling Rule	The name of the Signaling Rule that will be used to match SIP signaling packets.
Time-of-Day Rule	The ToD Rule set that will be used to determine when this Policy Group will be active.

6. Select **Finish.**
   The new **Policy Group** appears in the Application Pane (Figure 5-123).

Figure 5-123 New End-Point Policy Group Display.

Viewing an Existing Policy Group Summary

As previously stated, end-point policy groups are comprised of a group of end-point policy sets, all of which are specifically configured using a number of relevant parameters. These parameters can be viewed for any policy group in a single aggregate list which is displayed in a separate window. The procedure to view a policy group summary is provided below.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **End-Point Policy Groups** function from the **Domain Policies** feature from the Task Pane.

Existing **End-Point Policy Groups** are displayed in the Application Pane. The Policy Sets comprising a selected **Policy Group** are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-120.

3. From the Application Pane, select the **End-Point Policy Group** whose summary list you want to view (Figure 5-124).

The **Policy Sets** currently assigned to the selected **Policy Group** are displayed in the Content Area.

4. Select **View Summary**.

The **End-Point Policy Group Summary** is displayed in a new window (Figure 5-125).

Figure 5-124 Selecting an Existing Policy Group.

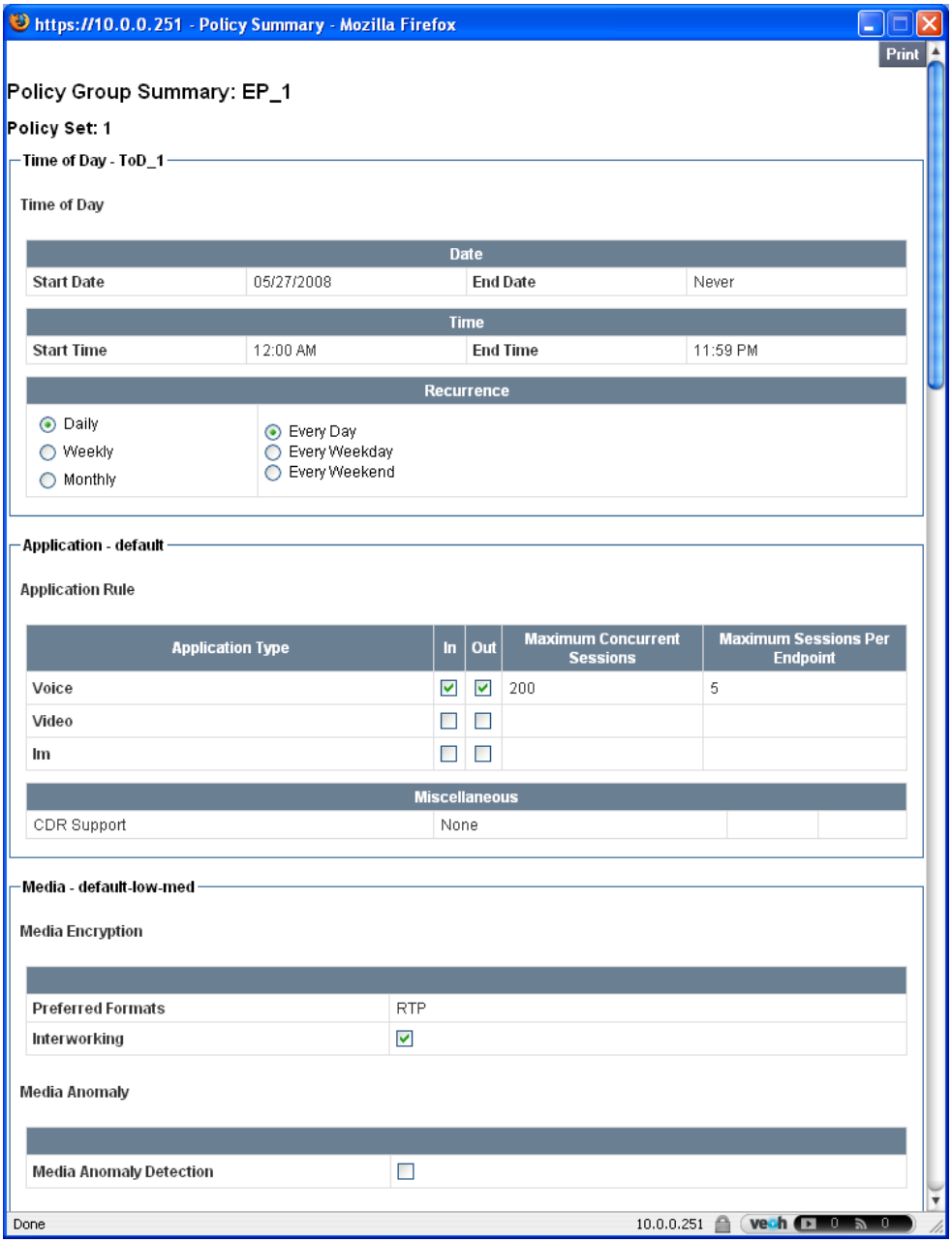


Figure 5-125 End-Point Policy Group Summary Report.

5. Use the scroll bar to view the entire report. Select **Print** to print the report or **Cancel** to close the window when done.

Editing an Existing End-Point Policy Group

Editing an End-Point Policy Group consists of: adding a Policy Set; reordering the precedence with which the constituent Policy Sets are executed within a Policy Group; editing an existing Policy Set; renaming an existing Policy Set; or deleting a specific Policy Set. Each of these procedures is described in the following sections.

Adding an End-Point Policy Set

Use the following procedure to add a **Policy Set** to an existing **Policy Group**. More than one Policy Set can be added to any Policy Group.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Policy Groups** function from the **Domain Policies** feature from the Task Pane.
   Existing **Policy Groups** are displayed in the Application Pane. The Policy Sets comprising a selected **Policy Group** are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-120.
3. From the Application Pane, select the **Policy Group** to which you want to add a Policy Set (Figure 5-124).
   The **Policy Sets** currently assigned to the selected **Policy Group** are displayed in the Content Area.
4. From the Application Pane, select **Add Policy Set**.
   The **Add Policy Set** pop-up window is displayed (Figure 5-126).

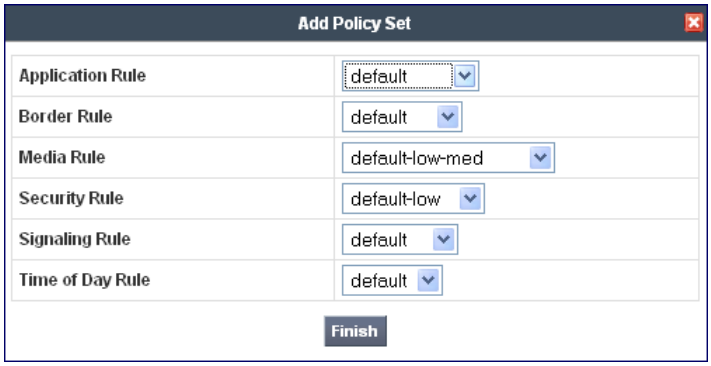


Figure 5-126 Add Policy Set Pop-up Window.

5. Select the desired pre-existing rule or policy for each remaining field using the corresponding radio button and drop-down lists.

   Selecting the Cancel icon cancels the operation and closes the window without creating a new Policy Set.

Table 5-19 Add Policy Set Pop-up Window Field Descriptions.

Field	Description
Application Rule	The name of the Application Rule that will determine which applications will have this Policy group applied.
Border Rule	The name of the Border Rule that will determine which applications will have this Policy group applied.
Media Rule	The name of the Media Rule that will be used to match media packets.
Security Rule	The name of the Security Rule that will determine which E-SBC security policies will be applied when this Policy Group is activated.
Signaling Rule	The name of the Signaling Rule that will be used to match signaling packets.
Time-of-Day Rule	The ToD Rule set that will be used to determine when this Policy Group will be active.

6. Select **Finish.**
   The new **Policy Set** appears in the Application Pane (Figure 5-127).

Note When multiple Policy Sets are assigned to any one Policy Group, the **Update Order** pushbutton is displayed in the top-left corner of the Content Area. This pushbutton is not displayed when a Policy Group contains only one Policy Set..

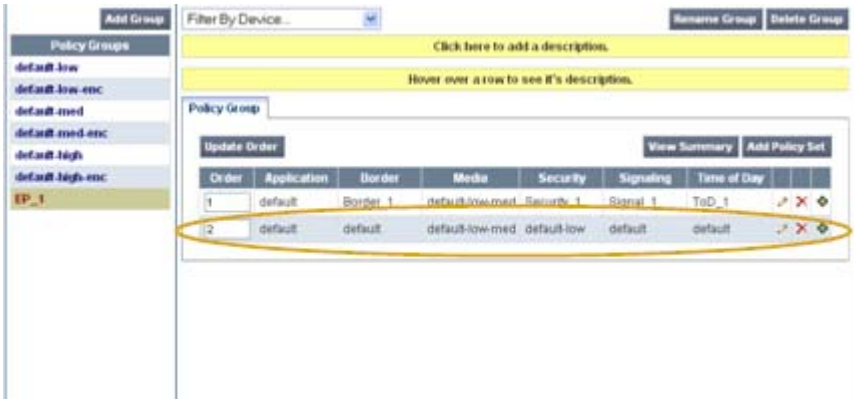


Figure 5-127 Updated End-Point Policy Set Display.

Reordering End-Point Policy Sets within a Policy Group

Use the following procedure to reorder the precedence with which constituent **Policy Sets** are executed within a **Policy Group.** As mentioned previously, The Policy Set number (priority position in the Policy Group's Policy Set list) is the deciding factor when ToD rules match on which Policy Set is applied to an incoming message.

1. Login to the E-SBC Control Center as the **Admin.**

2. Select the **End-Point Policy Groups** function from the **Domain Policies** feature from the Task Pane.
   Existing **End-Point Policy Groups** are displayed in the Application Pane. The Policy Sets comprising a selected **Policy Group** are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-128.

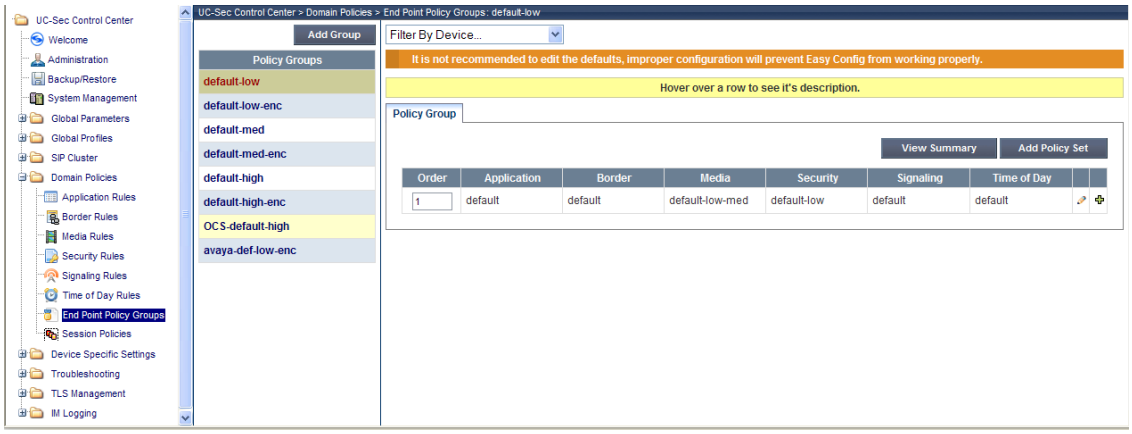


Figure 5-128 Policy Group Display Screen.

3. From the Application Pane, select the **Policy Group** whose **Policy Sets** you want to reorder (Figure 5-129).
   The constituent **Policy Sets** are displayed in the Content Area.

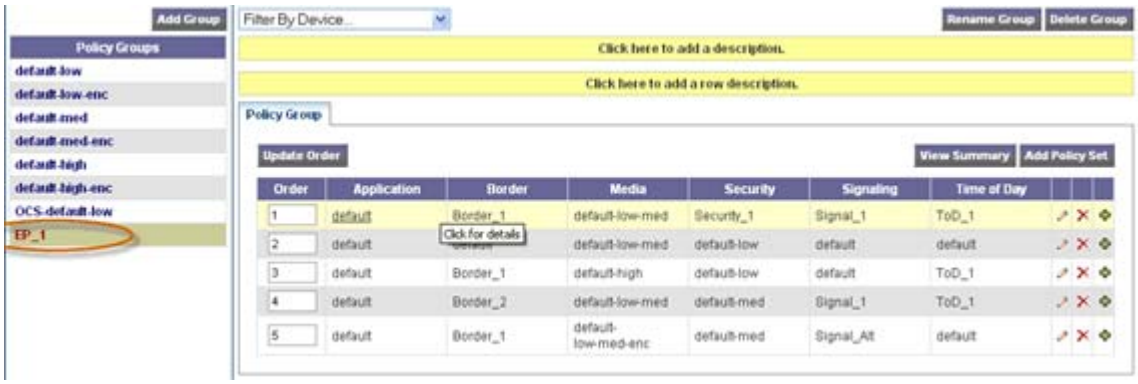


Figure 5-129 Selecting a Policy Group.

4. Change the number in the **Order** column to correspond to the order in which you want the **Policy Sets** to be executed (Figure 5-130).
5. Select **Update Order**.
   The **Policy Sets** are redisplayed in the Content Area to reflect the new order of precedence (Figure 5-131).

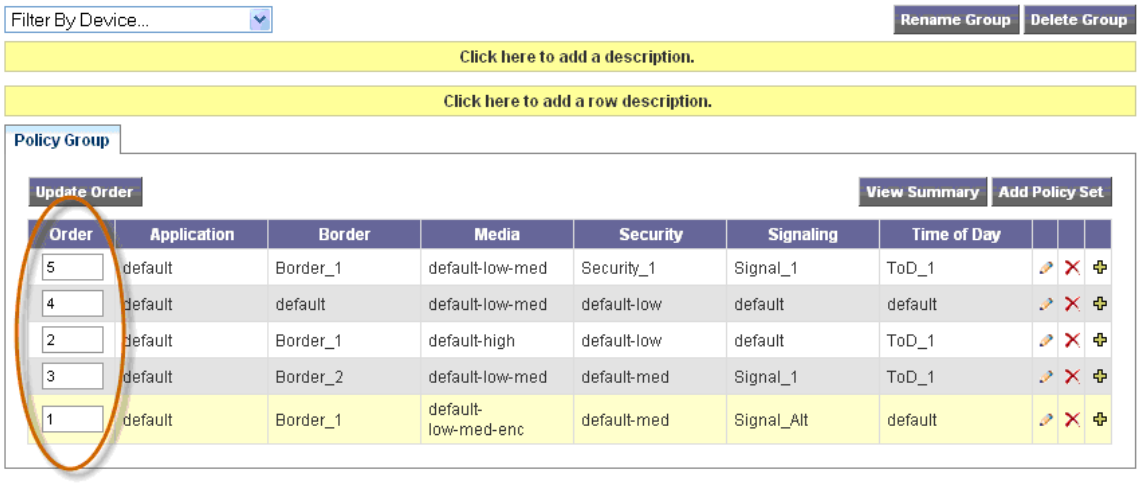


Figure 5-130 Selecting a New Order of Precedence for Existing Policy Sets.

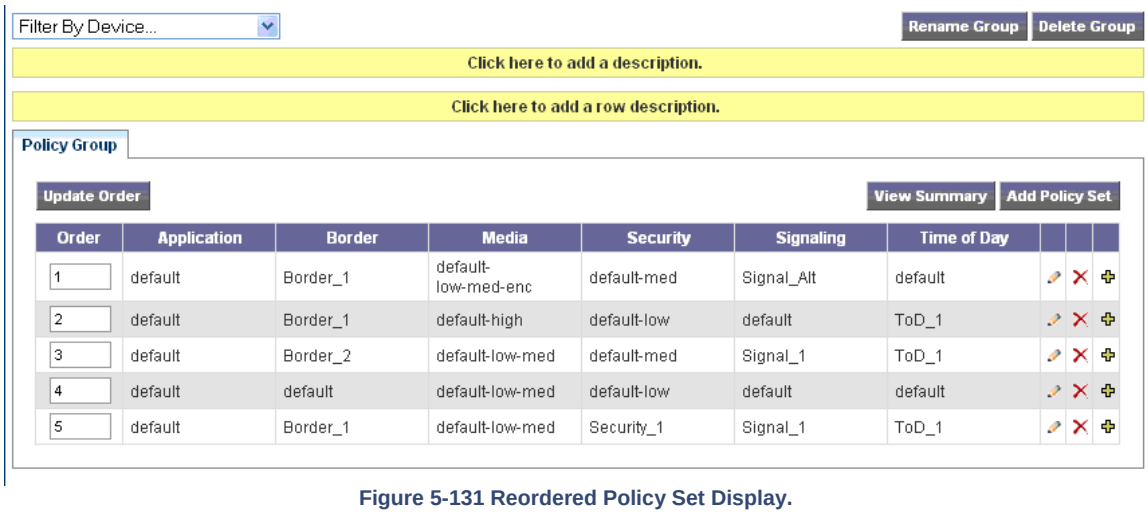


Figure 5-131 Reordered Policy Set Display.

Editing an End-Point Policy Set

Use the following procedure to edit an existing **End-Point Policy Set.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Policy Groups** function from the **Domain Policies** feature from the Task Pane. Existing **Policy Groups** are displayed in the Application Pane. The Policy Sets comprising a selected **Policy Group** are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-124.
3. From the Application Pane, select the **Policy Group** whose **Policy Sets** you want to edit (Figure 5-129).
   The constituent **Policy Sets** are displayed in the Content Area.
4. Click the **Edit** icon corresponding to the **Policy Set** you want to edit.
   The **Edit Policy Set** pop-up window is displayed (Figure 5-132).

5. Edit the desired fields and select **Finish** to save your changes, or **Cancel** to cancel the edit operation and close the window without saving. If necessary, refer back to Descriptions. Table for a description of each field.

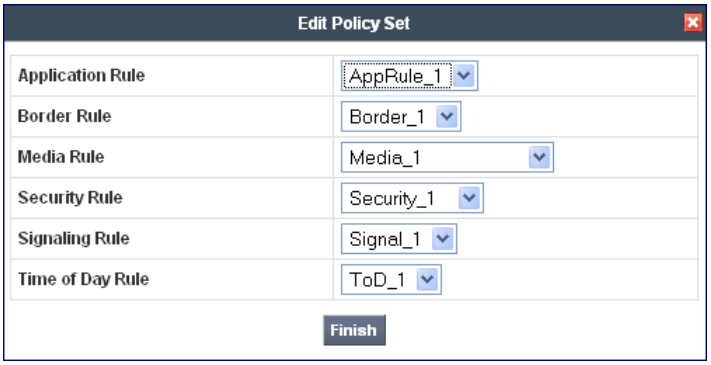


Figure 5-132 Edit Policy Set Pop-up Window.

Deleting an Existing End-Point Policy Set

Use the following procedure to delete an existing **End-Point Policy Set** from a **Policy Group.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Policy Groups** function from the **Domain Policies** feature from the Task Pane. Existing **Policy Groups** are displayed in the Application Pane. The Policy Sets comprising a selected **Policy Group** are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-128.
3. From the Application Pane, select the **Policy Group** whose **Policy Sets** you want to delete (Figure 5-129).
4. Click the **Delete** icon corresponding to the **Policy Set** you want to delete. A pop-up window similar to that shown in Figure 5-133 is displayed asking you to confirm the delete operation.

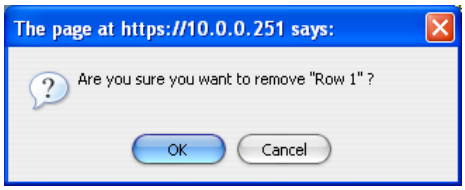


Figure 5-133 Delete Confirmation Pop-up Window.

5. Select **OK**. The **Policy Set** is deleted and the remaining **Policy Sets** are reordered and redisplayed in the Content Area.

Deleting an Existing End-Point Policy Group

Use the following procedure to delete an existing **End-Point Policy Group.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **End-Point Policy Groups** function from the **Domain Policies** feature from the Task Pane.
   Existing **End-Point Policy Groups** are displayed in the Application Pane. The Policy Sets comprising a selected **Policy Group** are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-128.
3. In the Applications Pane, select the **Policy Group** you want to delete (Figure 5-129).
4. From the Content Area, select **Delete Group.**
   A pop-up window similar to that shown in is displayed asking you to confirm the delete operation.
5. Select **OK.**
   The **End-Point Policy Set** is deleted.

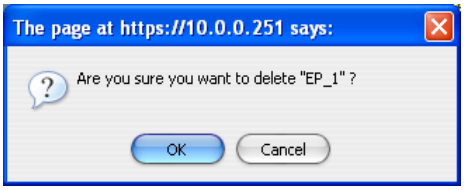


Figure 5-134 Delete Confirmation Pop-up Window.

Session Policies

Session Policies allow you to define RTP media packet parameters such as codec types (both audio and video) and codec matching priority. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the E-SBC security product.

Creating a New Session Policy

Use the following procedure to create a new **Session Policy.**

Caution! A default Session Policy is provided by Sipera. Editing this default rule set in not recommended, as improper configuration may cause subsequent calls to fail.

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Session Policies** function from the **Domain Policies** feature from the Task Pane.
   Existing **Session Policies** are displayed in the Application Pane. The parameters comprising a selected **Session Policy** set are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-135.

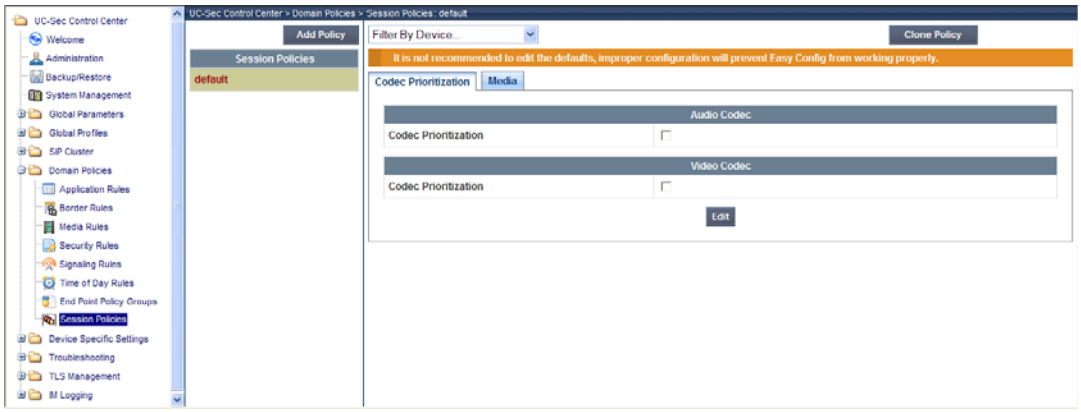


Figure 5-135 Session Policies Display.

3. Select **Add Policy** from the Applications Pane.
   The **Add Session Policy** pop-up window is displayed (Figure 5-136).

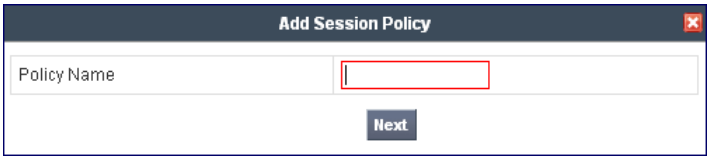


Figure 5-136 Add Session Policy Pop-up Window.

4. Enter a name for the new **Session Policy** and select **Next.**

The **Codec Prioritization** pop-up window is displayed (Figure 5-137).

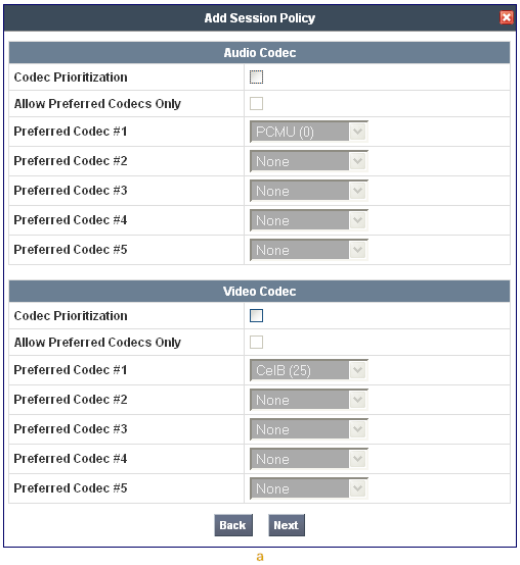


Figure 5-137 Codec Prioritization Pop-up Window.

5. Enter the requested information into the appropriate fields using the checkboxes and pull-down windows.

   Table 5-20 describes each user-definable field displayed in the **Codec Prioritization** pop-up window. Selecting the **Cancel** icon cancels the operation and closes the window without saving.

Table 5-20 Codec Prioritization Pop-up Window Field Descriptions.

Field	Description
	Audio Codec
Codec Prioritization	A checkbox that forces audio codecs to be matched according to the priority defined by the **Preferred Codec Priority 1** through **Preferred Codec Priority 5** fields.
Allow Preferred Codecs Only	A checkbox that will only match codecs listed in the previous **Preferred Codec Priority** fields. Audio codecs not listed will not be matched.
Preferred Codec Priority 1 through 5	Optional fields (required to be completed only if **Codec Prioritization** is checked) that contain the names of audio codecs you want specifically matched in a particular order.
	Video Codec
Codec Prioritization	A checkbox that forces video codecs to be matched according to the priority defined by the **Preferred Codec Priority 1** through **Preferred Codec Priority 5** fields.
Allow Preferred Codecs Only	A checkbox that will only match codecs listed in the previous **Preferred Codec Priority** fields. Audio codecs not listed will not be matched.
Preferred Codec Priority 1 through 5	Optional fields (required to be completed only if **Codec Prioritization** is checked) that contain the names of video codecs you want specifically matched in a particular order.

6. Select **Next.**
   The **Media Anchoring** pop-up window is displayed.

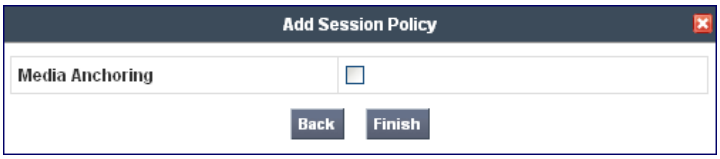


Figure 5-138 Media Anchoring Pop-up Window.

7. Click the checkbox (☑) to activate E-SBC Media Anchoring or leave blank (☐) to leave media anchoring disabled. Disabling *Media Anchoring*, as described in Chapter 1, keeps the media traffic within the Remote Branch Network (see Figure 1-2) if both calling parties reside inside the network.
8. Click **Next.**
   The **Media Forking** pop-up window is displayed.

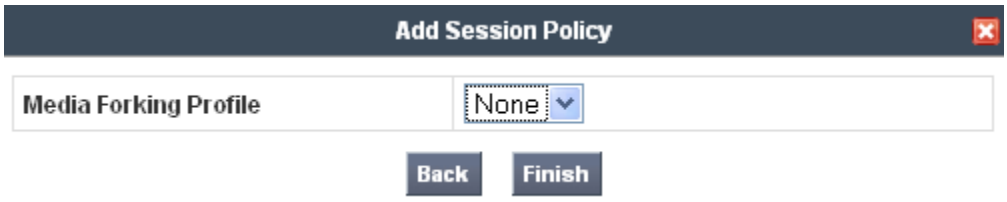


Figure 5-139 Media Forking Pop-up Window

9. Select **Finish.**

Cloning an Existing Session Policy

Use the following procedure to clone an existing **Session Policy.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Session Policies** function from the **Domain Policies** feature from the Task Pane.
   Existing **Session Policies** are displayed in the Application Pane. The parameters comprising a selected **Session Policy** set are displayed in the Content Area of the E-SBC Control Center.
3. Select **Clone Policy** from the Applications Pane.
   The **Clone Policy** pop-up window is displayed (Figure 5-140).

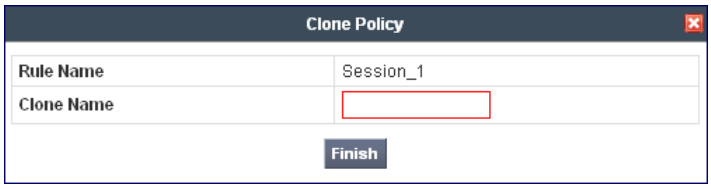


Figure 5-140 Clone Policy Pop-up Window.

4. Provide a name for the new policy in the field provided.
5. Select **Finish.**

Editing an Existing Session Policy

Session Policies are comprised of **Codec Prioritization** and **Media Anchoring** parameters. These can be easily edited by selecting the appropriate parameters tab and changing the desired fields. These procedures are described in the following sections.

Editing Codec Prioritization Parameters

Use the following procedure to edit **Codec Prioritization** parameters.

1. Select the **Session Policies** function from the **Domain Policies** feature from the Task Pane.

Existing **Session Policies** are displayed in the Application Pane. The parameters comprising a selected **Session Policy** set are displayed in the Content Area of the E-SBC Control Center.

2. From the Application Pane, select the **Session Policy** whose **Codec Prioritization** parameters you want to edit.
3. Select the **Codec Prioritization** tab.
4. Select **Edit**.
   The **Codec Prioritization** pop-up window is displayed (Figure 5-141).

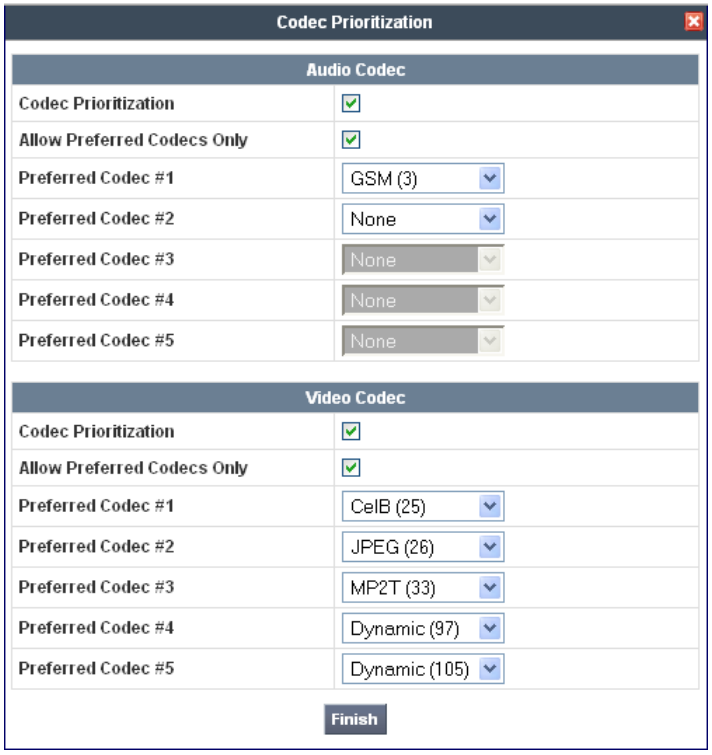


Figure 5-141 Codec Prioritization Pop-up Window.

5. Edit the desired fields and select **Finish** to save your changes or **Cancel** to cancel the operation and close the window without saving.

Editing Media Anchoring Parameters

Use the following procedure to edit **Media Anchoring** parameters.

1. Select the **Session Policies** function from the **Domain Policies** feature from the Task Pane.
   Existing **Session Policies** are displayed in the Application Pane. The parameters comprising a selected **Session Policy** set are displayed in the Content Area of the E-SBC Control Center.
2. From the Application Pane, select the **Session Policy** whose **Media Anchoring** parameters you want to edit.
3. Select the **Media Anchoring** tab.

4. Select **Edit**.
   The **Media Anchoring** pop-up window is displayed (Figure 5-142).

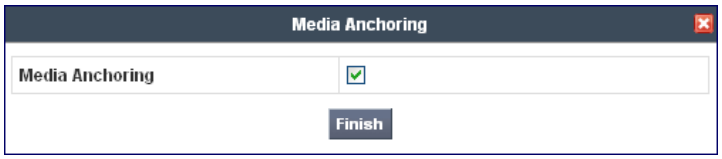


Figure 5-142 Media Anchoring Pop-up Window.

5. Change the state of the Media Anchoring feature by clicking the checkbox to activate the feature (☑) deactivate the feature (☐).
6. Select **Finish** when done.

Renaming an Existing Session Policy

Use the following procedure to rename an existing **Session Policy**.

1. Select the **Session Policies** function from the **Domain Policies** feature from the Task Pane.
   Existing **Session Policies** are displayed in the Application Pane. The parameters comprising a selected **Session Policy** set are displayed in the Content Area of the E-SBC Control Center.
2. From the Application Pane, select the **Session Policy** you want to rename (Figure 5-143).
3. Select the **Rename Policy** button.
   The **Rename Policy** pop-up window is displayed (Figure 5-144).

Figure 5-143 Selecting an Existing Session Policy.

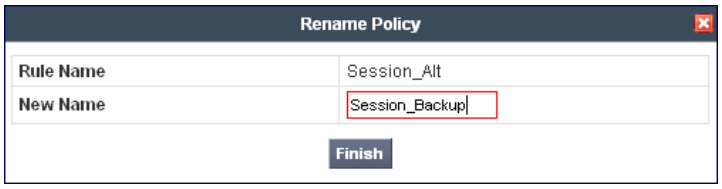


Figure 5-144 Rename Policy Pop-up Window.

4. Enter a new name for the existing **Session Policy** and select **Finish.**
   The existing **Session Policy** is redisplayed in the Application Pane with the new name.

Deleting an Existing Session Policy

Use the following procedure to delete an existing **Session Policy.**

1. Select the **Session Policies** function from the **Domain Policies** feature from the Task Pane.
   Existing **Session Policies** are displayed in the Application Pane. The parameters comprising a selected **Session Policy** set are displayed in the Content Area of the E-SBC Control Center.
2. From the Application Pane (Figure 5-143), select the **Session Policy** you want to delete.
3. Select the **Delete Policy** button.
   The **Delete Confirmation** pop-up window is displayed.
4. Select **OK.**
   The **Session Policy** is deleted.

Managing End-Point and Session Flows

The *End-Point Flows* and *Session Flows* features allow you to define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or from without. These features provide you with the complete and unparalleled flexibility to monitor, identify, and control very specific types of calls based upon these user-definable parameters. *End-Point Flows*, which profile SIP signaling parameters, are combined with *Session Flows*, which profile SDP media parameters, to completely identify and characterize a call placed through the network. Any number of End-Point and Session Flows may be defined.

There are two methods that can be used to create a new End-Point or Session Flow. The first method uses the **Add Flow** function of the **Flows** feature, wherein you manually define a signaling or media flow by configuring all the necessary parameters on a number of sequential display screens or pop-up windows. The second method, called **Cloning**, allows you to copy an existing flow and only change those parameters which would make it distinct. These methods are described in the following sections.

End-Point Flows

The following sections contain the procedures necessary to create, clone, view, edit, and delete Server End-Point Flows.

Note:	Some Sipera products provide two types of end-point flows, Subscriber and Server. The E-SBC product only uses Server End-Point Flows. Therefore, the Subscriber Flows tab on the End-Point Flows screen is not applicable and not used. Use only the Server Flows tab when configuring E-SBC deployments.

Creating a New Server End-Point Flow

Use the following procedure to manually create a new **Server End-Point Flow**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **End-Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
   The registered E-SBC security devices for which the new flow will be applied are listed in the Application Pane under the heading **E-SBC Devices**. A specifically ordered list of server flows for the selected E-SBC security device are displayed under the corresponding tab displays of the Content Area of the E-SBC Control Center.
3. From the Application Pane, select the E-SBC Device for which the new **Server End-Point Flow** will be created.
   The End-Point Flows currently defined for that E-SBC device are displayed in the Content Area.
4. Select the **Server Flows** tab.
5. From the Content Area, select **Add Flow**.
   The **Add Flow** pop-up window is displayed.

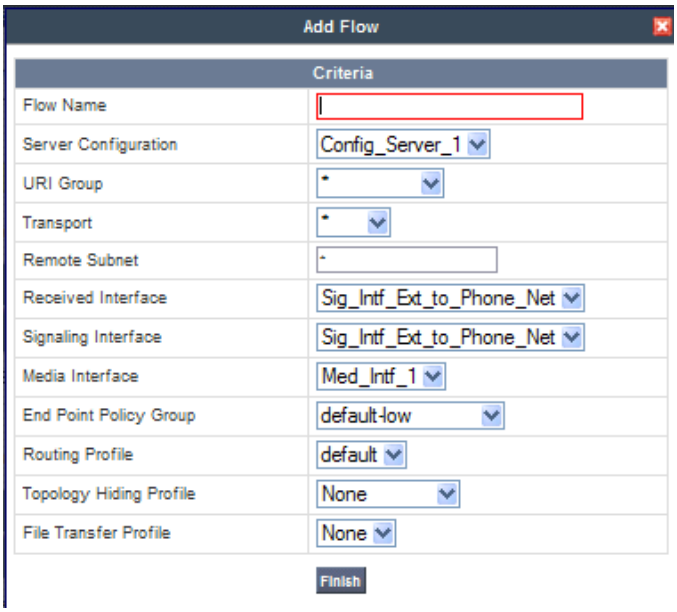


Figure 5-145 **Add Flow Pop-Up Window.**

6. Provide the requested information using the field boxes, drop-down menus, and radio buttons. Field descriptions are provided in Table 5-21.

   Selecting the **Cancel** icon cancels the operation and closes the window without creating a new end-point flow.

Table 5-21 Add Flow: Criteria Pop-up Window Field Descriptions.

Field	Description
	Criteria
Flow Name	The name assigned to this Server End-Point Flow.
Server Configuration	Drop-down menu from which you select the **Server Configuration Hiding Profile** to be used for this **Server End-Point Flow**.
URI Group	The domain of the call server or domain of the SIP trunk from which a call will originate, depending upon the direction of traffic flow.
Transport	The transport protocol type supported by the SIP server. Available selections are **TCP**, **UDP**, and **TLS**.
Remote Subnet	The subnet of the traffic source (e.g., 198.172.25.0/24).
Received Interface	Drop-down menu from which you select the **Received Interface** to be used for this **Server End-Point Flow**.
Signaling Interface	Drop-down menu from which you select the **Signaling Interface** to be used for this **Server End-Point Flow**.
Media Interface	Drop-down menu from which you select the **Media interface** to be used for this **Server End-Point Flow**. Select the internal or external media interface depending upon the direction of the flow of traffic.
End-Point Policy Group	Drop-down menu from which you select the **End-Point Policy Group** to be used for this **Server End-Point Flow**.
Routing Profile	Select the Routing Profile name from the drop-down list of the profile previously created by selecting **Global Profiles → Routing → Add Profile,** as described in Chapter 6, "System Configuration," in the subsection titled, "Routing Profiles."

Field	Description
Topology Hiding Profile	Select the Topology Hiding Profile name from the drop-down list of the profile previously created by selecting **Global Profiles** → **Topology Hiding** → **Add Profile,** as described in Chapter 7, "Security Configuration," in the subsection titled, "Topology Hiding ."
File Transfer Profile	Select the File Transfer Profile name from the drop-down list of the profile previously created by selecting **Device Specific Settings** → **Relay Services** → **File Transfer** (tab) → **Add Flow** and entering information in the **Add File Transfer Profile** pop-up screen.

7. Select **Finish.**
   The new **Server End-Point Flow** is displayed in the Content Area (Figure 5-146).

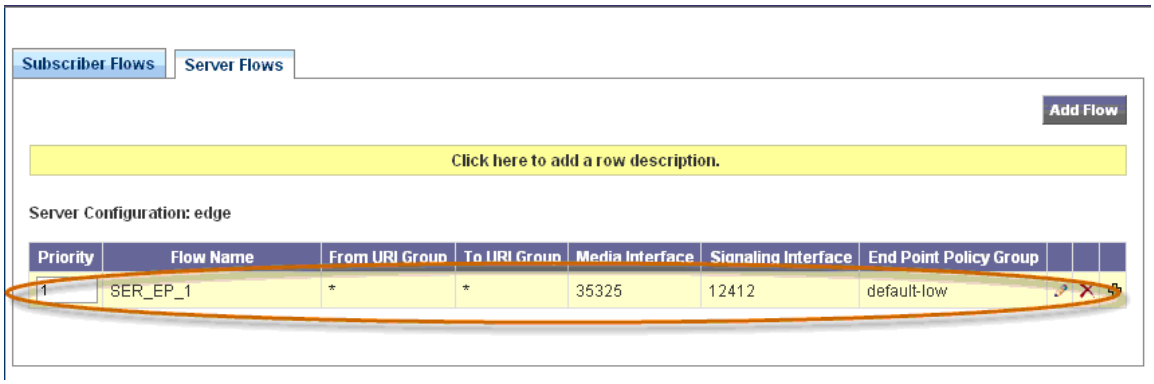


Figure 5-146 Updated Server End-Point Flow Display.

Cloning an Existing End-Point Flow

Additional End-Point Flows can be added to the E-SBC security repertoire by cloning existing **Server End-Point Flows** and editing the desired parameters to create new flow policies. The following sections contain the procedures necessary to clone existing End-Point Flows.

Note An end-point flow cannot be cloned from one E-SBC security device and applied to another E-SBC security device; a clone can only be assigned to the same E-SBC security device from which the original flow came.

Cloning an Existing Server End-Point Flow

Use the following procedure to manually create a new **Server End-Point Flow.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **End-Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
3. Select **Server Flows** tab.

The existing Server End-Point Flows are displayed in the Content Area of the E-SBC Control Center.

4. Select the **Clone** ( ) icon corresponding to the Server End-Point Flow you want to clone.
   The **Clone Flow: Criteria** pop-up window is displayed (Figure 5-147).
5. Add a new **Flow Name** to identify this cloned flow and edit any other parameters as desired.
6. Select **Finish.**
   The cloned **Server End-Point Flow** is displayed in the Content Area

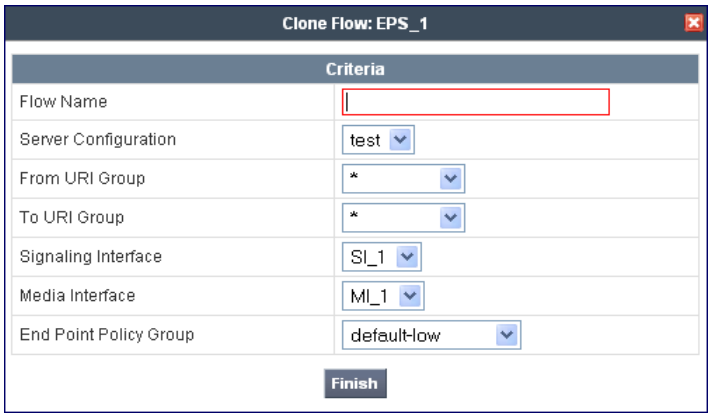


Figure 5-147 Clone Flow: Criteria Pop-up Window.

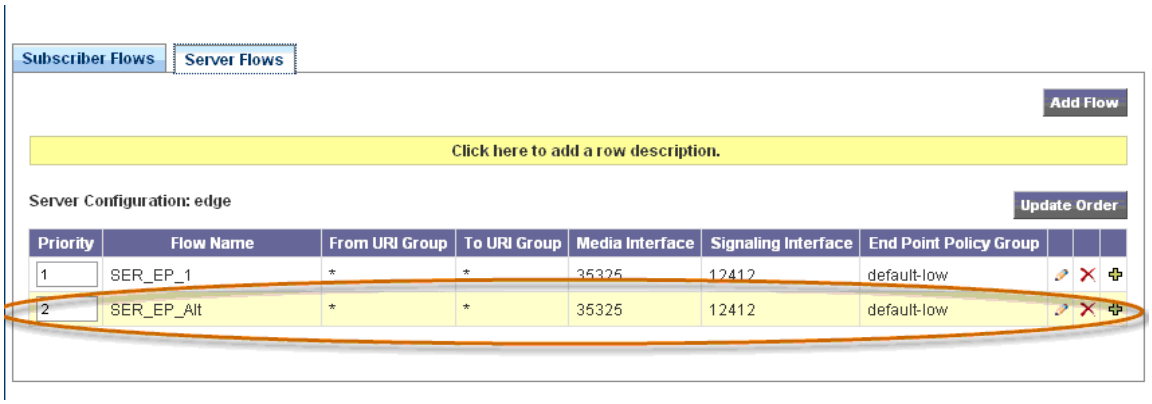


Figure 5-148 Updated Server End-Point Flow Display.

Editing Existing Server End-Point Flows

Use the following procedure to edit an existing **Server End-Point Flows.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **End-Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
3. Select the **Server Flows** tab.
4. Select the **Edit** ( ) icon corresponding to the flow you want to edit.

The **Edit Flow: Criteria** pop-up window is displayed (Figure 5-149).

5. Make your changes to the existing fields.

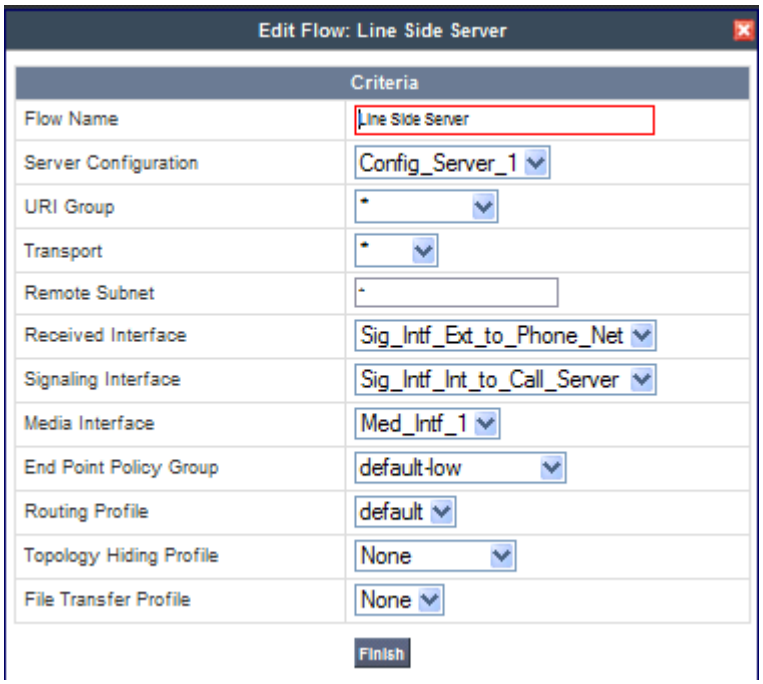


Figure 5-149 Edit Flow: Criteria Pop-up Window.

6. Select **Finish.**
   The **End-Point Flow** configuration is updated and saved.

Reordering the Precedence of End-Point Flows

Use the following procedure to reorder the precedence of existing **Server End-Point Flows.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **End-Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
3. Select the **Server Flows** tab.
4. Change the number in the **Order** column to reflect the order or precedence which you want the flows to be executed the (Figure 5-150).
5. Select **Update Order.**
   The **End-Point Flows** are redisplayed in the Content Area to reflect the new order of precedence (Figure 5-151).

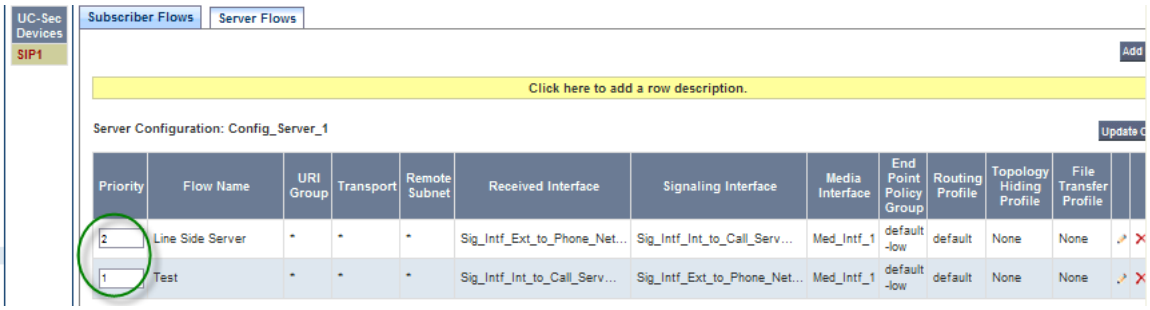


Figure 5-150 Selecting a New Order of Precedence for Existing End-Point Flows.

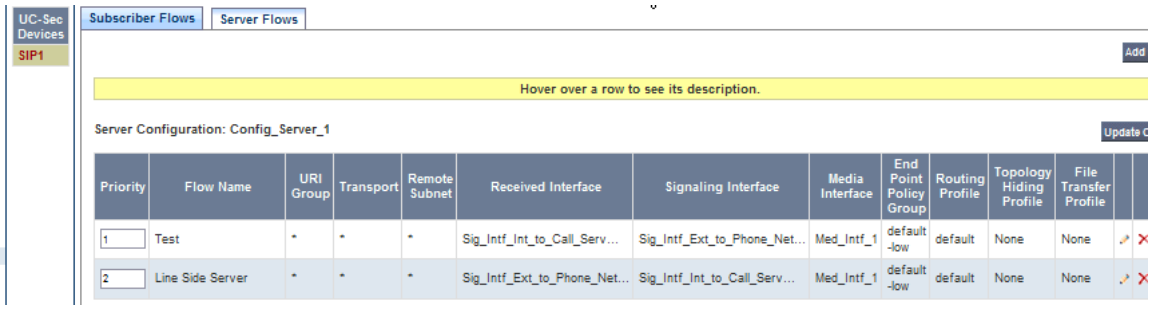


Figure 5-151 Reordered End-Point Flows.

Deleting an Existing End-Point Flow

Use the following procedure to delete an existing **Server End-Point Flow**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **End-Point Flows** function from the **Device Specific Settings** feature from the Task Pane.
3. Select either the **Subscriber Flows** or **Server Flows** tab.
4. Select the **Delete** (✕) icon corresponding to the **Server End-Point Flow** configuration you want to delete.
   The **Delete Confirmation** pop-up window is displayed (Figure 5-152).
5. Click **OK**.
   The **End-Point Flow** is deleted.

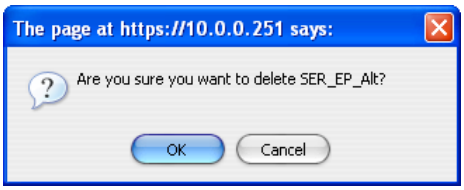


Figure 5-152 Delete Confirmation Pop-up Window.

Session Flows

The following sections contain the procedures necessary to create, clone, view, edit, and delete Session Flows.

Creating a New Session Flow

Use the following procedure to manually create a new **Session Flow**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Session Flows** function from the **Device Specific Settings** feature from the Task Pane.
   The registered E-SBC security devices for which the new flow will be applied are listed in the Application Pane under the heading **E-SBC Devices**. A specifically ordered list of **Session Flows** for the selected E-SBC security device are displayed in the E-SBC Control Center as shown in Figure 5-153.
3. From the Application Pane, select the E-SBC Device for which the new **Session Flow** will be created (Figure 5-154).
   The Session Flows currently defined for that E-SBC device are displayed in the Content Area.
4. Select **Add Flow**.
   The **Add Flow** pop-up window is displayed (Figure 5-155).

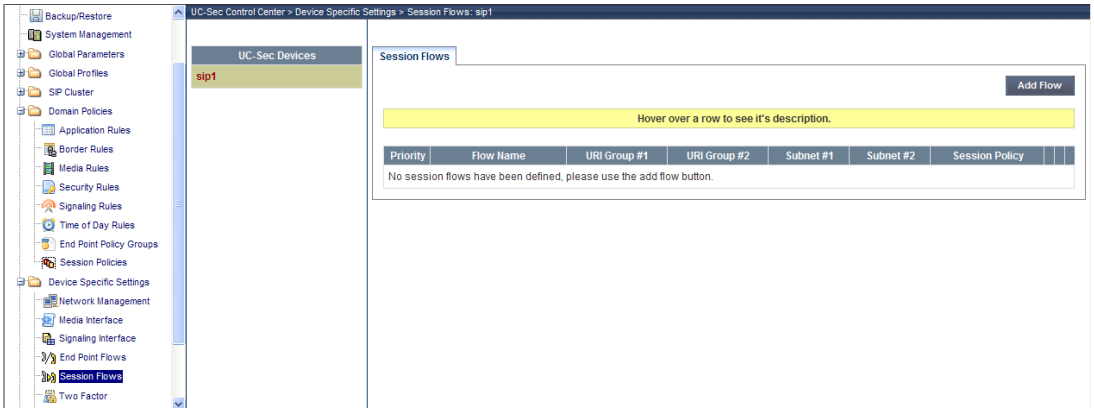


Figure 5-153 Session Flow Display.

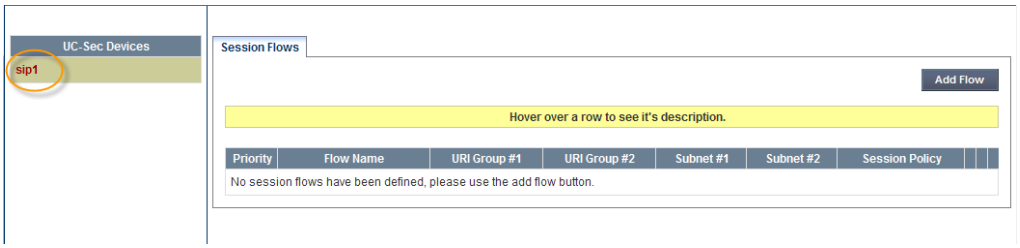


Figure 5-154 Selecting an E-SBC Device.

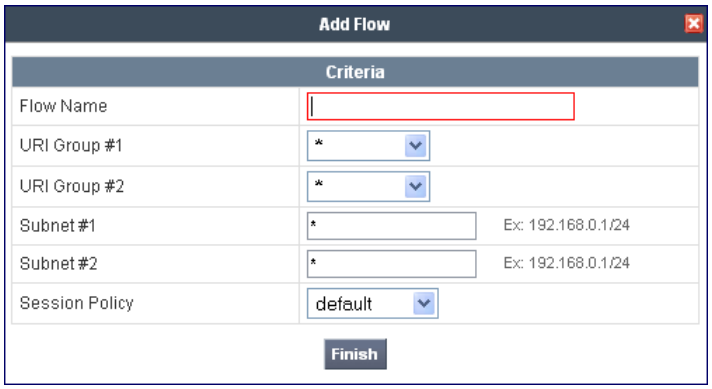


Figure 5-155 Add Flow Pop-up Window.

5. Provide the requested information using the field boxes, drop-down menus, and radio buttons. Field descriptions are provided in Table 5-22.

   Selecting the **Cancel** icon cancels the operation and closes the window without creating a new end-point flow.

Table 5-22 Add Flow Pop-up Window Field Descriptions.

Field	Description
	Criteria
Flow Name	The name assigned to this **Session Flow**.
URI Group #1	A drop-down list from which you select a currently defined SIP URI Group policy to identify the source of an originating call.
URI Group #2	A drop-down list from which you select a currently defined SIP URI Group policy to identify the destination of a call.
Subnet #1	The subnet address from which calls originate.
Subnet #2	The subnet address to which calls are destined.
Session Policy	The **Session Policy** profile to be used for this **Session Flow**.

5. Select **Finish.**
   The new **Session Flow** is added and displayed in the Content Area of the Control Center (Figure 5-156).

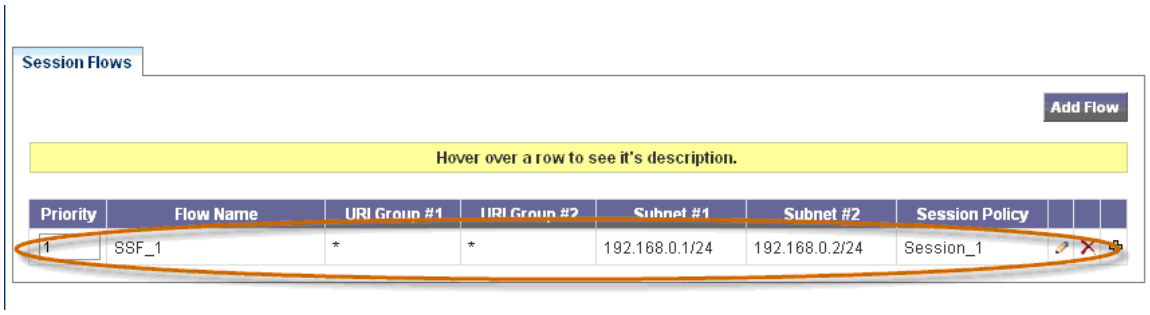


Figure 5-156 Updated Session Flow Display.

Cloning an Existing Session Flow

Additional **Session Flows** can be added to the E-SBC security repertoire by cloning existing **Session Flows** and editing the desired parameters to create new flow policies. The following sections contain the procedures necessary to clone existing **Session Flows.**

Note	A Session Flow cannot be cloned from one E-SBC security device and applied to another E-SBC security device; a clone can only be assigned to the same E-SBC security device from which the original flow came.

Use the following procedure to manually create a new **Server End-Point Flow.**

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Session Flows** function from the **Device Specific Settings** feature from the Task Pane.
   The registered E-SBC security devices for which the new flow will be applied are listed in the Application Pane under the heading **E-SBC Devices.** A specifically ordered list of **Session Flows** for the selected E-SBC security device are displayed in the E-SBC Control Center as shown in Figure 5-153.
3. From the Application Pane, select the E-SBC Device for which a **Session Flow** will be cloned (Figure 5-154).
   The Session Flows currently defined for that E-SBC device are displayed in the Content Area.
4. Select the **Clone** ( ) icon corresponding to the Session Flow you want to clone.
   The **Clone Flow** pop-up window is displayed (Figure 5-157).

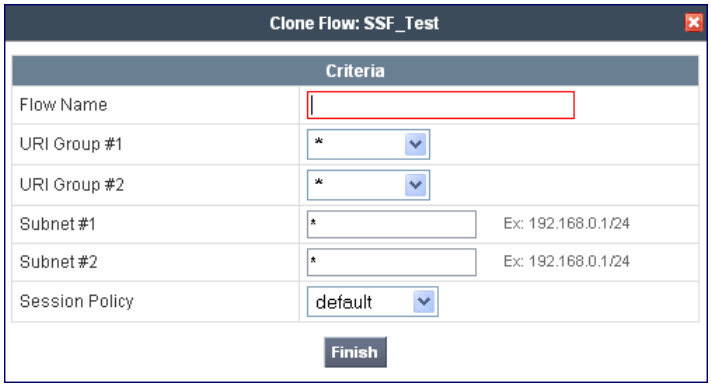


Figure 5-157 Clone Flow Pop-up Window.

5. Add a new **Flow Name** to identify this cloned flow and edit any other parameters as desired, according to the information contained in Table 5-22.
6. Select **Finish.**
   The cloned **Session Flow** is displayed in the Content Area (Figure 5-158).

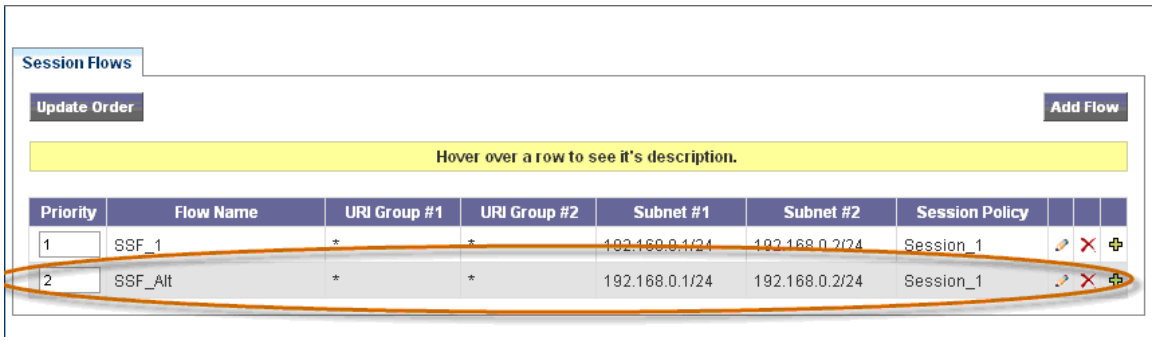


Figure 5-158 Updated Session Flow Display.

Editing Existing Session Flows

Use the following procedure to edit an existing **Server End-Point Flow**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Session Flows** function from the **Device Specific Settings** feature from the Task Pane.
   The registered E-SBC security devices for which the new flow will be applied are listed in the Application Pane under the heading **E-SBC Devices**. A specifically ordered list of **Session Flows** for the selected E-SBC security device are displayed in the E-SBC Control Center as shown in Figure 5-153.
3. From the Application Pane, select the E-SBC Device whose **Session Flow** you want to edit (Figure 5-154).
   The **Session Flows** currently defined for that E-SBC device are displayed in the Content Area.
4. Select the **Edit** ( ) icon corresponding to the flow you want to edit.
   The **Edit Flow** pop-up window is displayed (Figure 5-159).

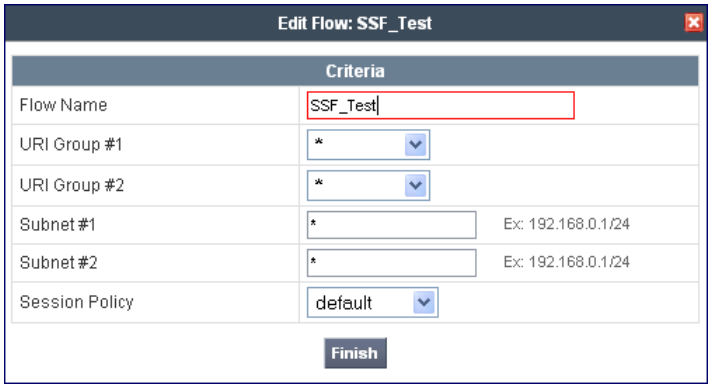


Figure 5-159 Edit Flow Pop-up Window.

5. Make your changes to the existing fields in the Edit Flow Pop-up window.
6. Select **Finish**.
   The edited **Session Flow** configuration is updated and saved.

Reordering the Precedence of Session Flows

Use the following procedure to reorder the precedence of existing **Session Flows**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Session Flows** function from the **Device Specific Settings** feature from the Task Pane.
3. From the Application Pane, select the E-SBC Device whose **Session Flow** whose precedence you want to reorder (Figure 5-154).
   The **Session Flows** currently defined for that E-SBC device are displayed in the Content Area.
4. Change the number in the **Order** column to reflect the order or precedence which you want the flows to be executed the (Figure 5-160).
5. Select **Update Order**.
   The **Session Flows** are redisplayed in the Content Area to reflect the new order of precedence (Figure 5-161).

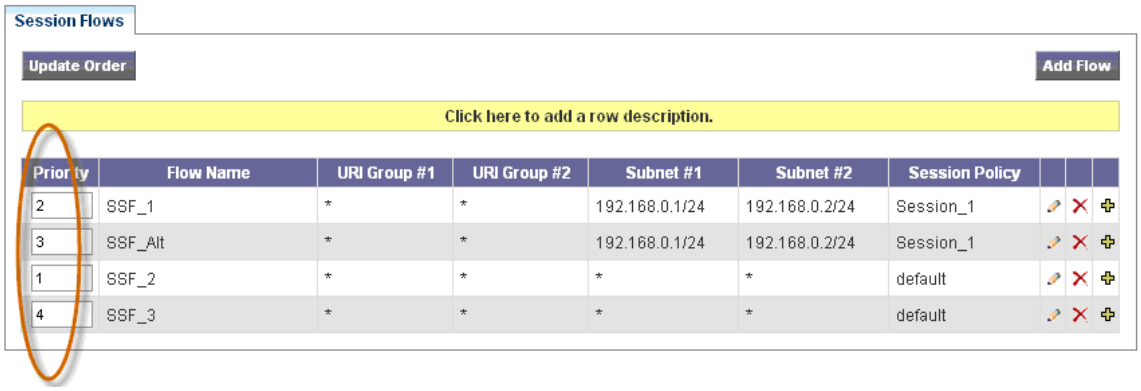


Figure 5-160 Selecting a New Order of Precedence for Existing Session Flows.

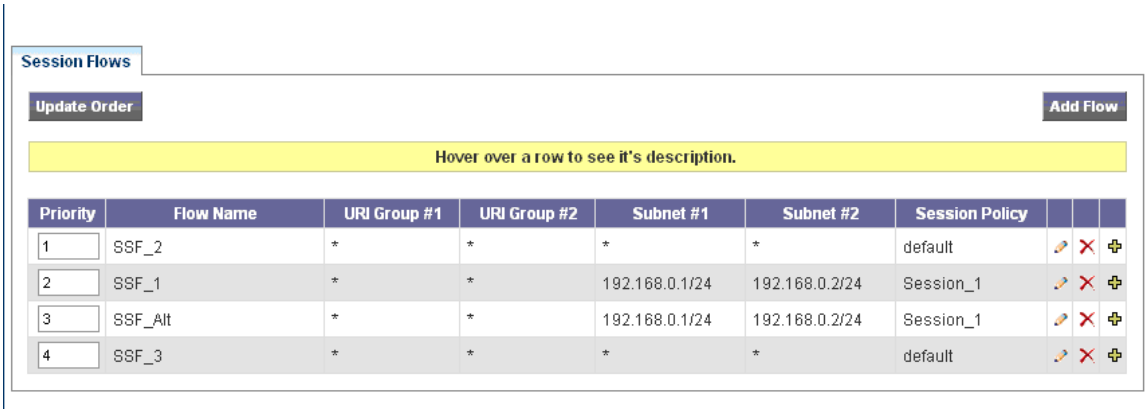


Figure 5-161 Reordered Session Flows.

Deleting an Existing Session Flow

Use the following procedure to delete an existing **Session Flow**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Session Flows** function from the **Device Specific Settings** feature from the Task Pane.
3. From the Application Pane, select the E-SBC Device whose **Session Flow** you want to delete (Figure 5-162).
   The **Session Flows** currently defined for that E-SBC device are displayed in the Content Area.

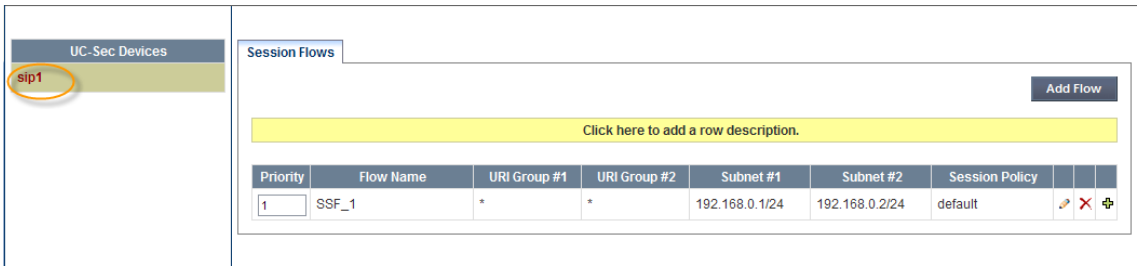


Figure 5-162 Selecting an E-SBC Device

4. Select the **Delete** (✕) icon corresponding to the **Session Flow** configuration you want to delete.
   The **Delete Confirmation** pop-up window is displayed.
5. Click **OK**.
   The **Session Flow** is deleted.

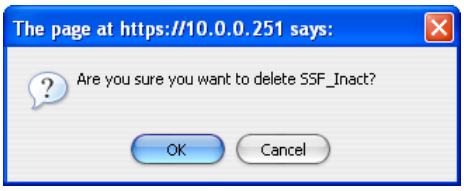


Figure 5-163 Delete Confirmation Pop-up Window.

Uniform Resource Identifier (URI) Groups

The **URI Group** feature allows you to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (**Allow**, **Block**, or **Apply Policy**) should be taken for a given call flow.

Creating a New URI Group

Use the following procedure to create a new SIP **URI Group**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **URI Groups** function from the **Global Parameters** feature from the Task Pane.

Figure 5-164 URI Groups Feature of Global Profiles

Existing **URI Groups** are displayed in the Application Pane. The various URIs that comprise that **URI Group** are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-165.

Figure 5-165 URI Group Display.

3. Select **Add Group** from the Application Pane.
   The **Add URI Group** pop-up window is displayed (Figure 5-166).
4. Provide a name for the new URI Group and press **Next** or **Cancel** to cancel the operation without saving.
   The next **Add URI Group** pop-up window is displayed (Figure 5-167).

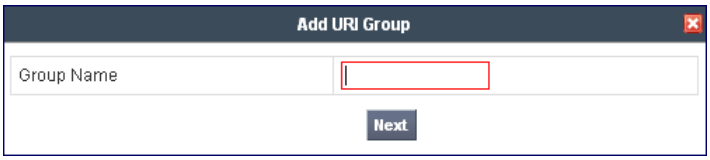


Figure 5-166 Add URI Group Pop-up Window.

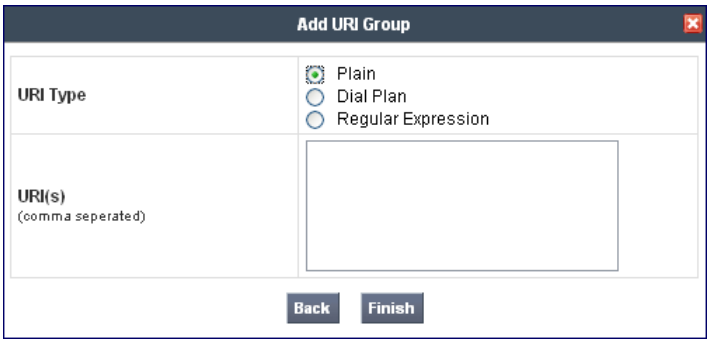


Figure 5-167 Subsequent Add URI Pop-up Window.

5. In the Add Uri Pop-up window, provide the requested information using the radio buttons and text box.

   Selecting the **Cancel** icon cancels the operation and closes the window without creating a new URI Group.

Table 5-23 Add URI Group Pop-up Window Field Descriptions.

Field	Description

URI Type	Radio button allowing you to select the type of URI expression you will enter into the **URI(s)** field. Available selections are:
	
	Plain Common SIP URI format:
	`*@192.168.15.12`
	`*@sipera.com`
	
	Dial Plan Valid SIP Dial Plan in the format:
	`9555XXXX@*`
	`9555NXXX@sipera.com`
	`011*@*`
	
	Regular Expression REGEX in the format:
	`[0-9]{3,5}\.user@domain\.com,`
	`(simple|advanced)\-user[A-Z]{3}@.*`

URI(s)	A text box into which you enter the desired URI(s), using the format selected in the **URI Type** field.

6. Click **Finish** to save the information or **Cancel** to cancel the operation and close the pop-up window without creating a new **URI Group.**
   The **URI Group** screen is displayed with the new URI Group listed in the Application Pane (Figure 5-168).

Figure 5-168 New URI Group Display.

Emergency Group

The **Emergency** URI group is an integral part of the system (not user-defined). Figure 5-169 below contains a sample **Emergency** group URI listing. The Emergency group is created to define special numbers that should not be restricted by any Domain Policies.

Note:	The SIP Options tab of the Advance Options screen further defines the management of numbers contained in the Emergency URI group. Refer to the section titled, “Managing SIP Options” in Chapter 6 of this document.

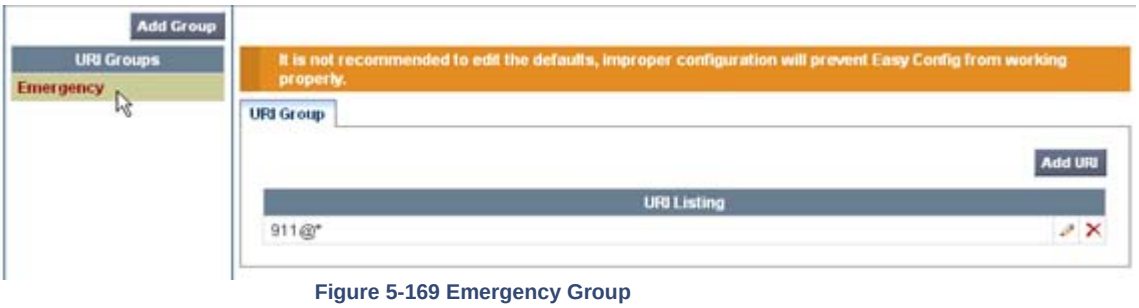


Figure 5-169 Emergency Group

Adding an Additional URI to an Existing URI Group

Use the following procedure to add an additional URI to an existing **URI Group**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **URI Groups** function from the **Global Profiles** feature from the Task Pane. Existing **URI Groups** are displayed in the Application Pane. The various URIs that comprise that **URI Group** are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-165.
3. From the Applications Pane, select the URI Group to which you want to add a URI.
   A list of SIP URIs currently assigned to the selected URI Group is displayed on the URI Group tab in the Content Area (Figure 5-170).
4. Select **Add URI**.
   The **Add URI** pop-up window is displayed.

5. Enter the desired URI(s) into the fields.

   Either select **Finish** to save the new information or **Cancel** to cancel the operation and close the pop-up window without adding the new URI information.

   The **URI Group** screen is displayed with the new URI Group listed in the Application Pane (Figure 5-172).

Figure 5-170 Selected URI Group Display.

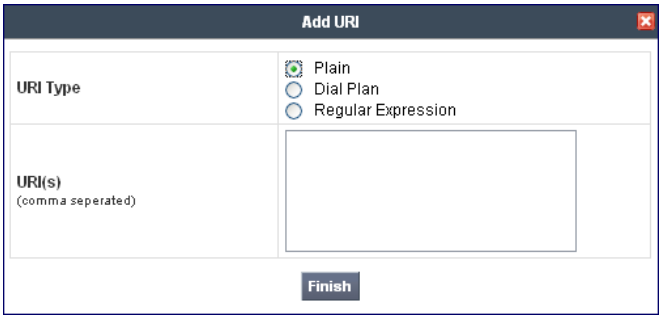


Figure 5-171 Add URI Pop-up Window.

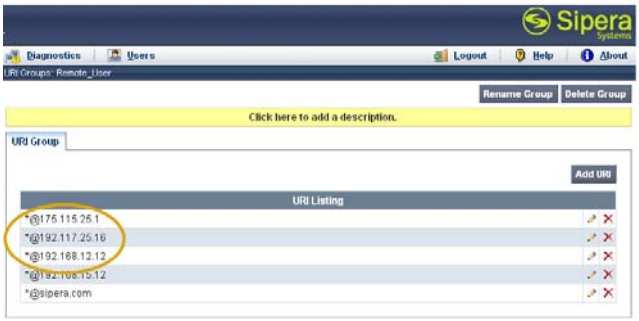


Figure 5-172 New URI Group Display.

Editing an Existing URI Group

Use the following procedure to edit an existing **URI Group**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **URI Groups** function from the **Global Profiles** feature from the Task Pane.
   Existing **URI Groups** are displayed in the Application Pane. The various URIs that comprise that **URI Group** are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-165.
3. From the Applications Pane, select the URI Group you want to edit.
   A list of SIP URIs that are currently assigned to selected URI Group is displayed on the URI Group tab (Figure 5-170) in the Content Area.
4. In the Content Area, click the **Edit** icon that corresponds to the URI you want to edit.
   The **Edit URI** pop-up window is displayed (Figure 5-173).

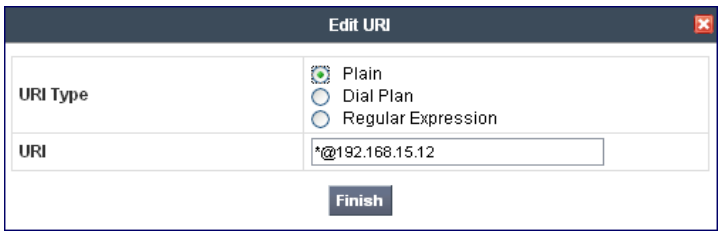


Figure 5-173 Edit URI Pop-up Window.

5. Edit the **URI** as desired and select **Finish** to save your changes or **Cancel** to revert to the previous values without saving.

Deleting a SIP URI from an Existing URI Group

Use the following procedure to delete a SIP URI from an existing **URI Group**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **URI Groups** function from the **Global Profiles** feature from the Task Pane.

   Existing **URI Groups** are displayed in the Application Pane. The various URIs that comprise that **URI Group** are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-165.

3. From the Applications Pane, select the **URI Group** from which you want to delete a SIP URI.
4. In the Content Area, click the **Delete** icon that corresponds to the URI you want to delete.
   A pop-up window is displayed similar to that shown in Figure 5-174 asking you to confirm your request to delete the SIP URI.

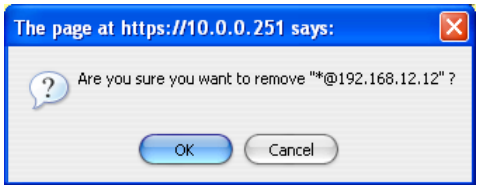


Figure 5-174 Delete Confirmation Pop-up Window.

5. Select **OK**.
   The SIP URI is deleted from the **URI Group**.

Renaming an Existing URI Group

Use the following procedure to rename an existing **URI Group**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **URI Groups** function from the **Global Profiles** feature from the Task Pane.
   Existing **URI Groups** are displayed in the Application Pane. The various URIs that comprise that **URI Group** are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-165.
3. In the Content Area, select **Rename URI Group**.
   The **Rename URI Group** pop-up window is displayed (Figure 5-175).

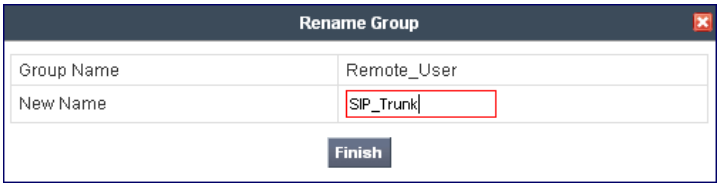


Figure 5-175 Rename URI Group Pop-up Window.

4. Enter a new name for the existing **URI Group** in the **New Name** field.
5. Select **Finish** to save the existing **URI Group** with the new name or **Cancel** to terminate the renaming process and close the window without saving.

Deleting an Existing URI Group

Use the following procedure to delete an existing SIP **URI Group**.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **URI Groups** function from the **Global Profiles** feature from the Task Pane.
   Existing **URI Groups** are displayed in the Application Pane. The various URIs that comprise that **URI Group** are displayed in the Content Area of the E-SBC Control Center as shown in Figure 5-165.
3. In the Content Area, select **Delete Group**.
   If this URI Group is associate with a security policy or call flow, then a pop-up window similar to that shown in Figure 5-176 is displayed.
4. Go to the section in this chapter called *Managing End-Point and Session Flows* and remove any existing associations. Return to step 3 above.
   A pop-up window is displayed similar to that shown in Figure 5-177 asking you to confirm your request to delete the SIP URI Group.

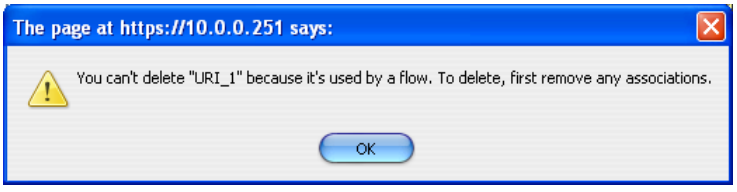


Figure 5-176 Association Notification Pop-up Window.

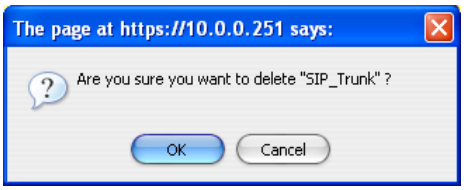


Figure 5-177 Delete Confirmation Pop-up Window.

5. Select **OK**.
   The **URI Group** is deleted.

System Configuration 6

Basic Configuration Overview

The E-SBC Control Center (EMS) allows you to configure and manage the system-related security features of the E-SBC security products deployed in an enterprise VoIP network. These are:

- Backup / Restore System Information
- Manage E-SBC Security Devices
  - Provision installed E-SBC security devices
  - Establish secure shell sessions
  - Shutdown and reboot individual E-SBC devices
  - Restart E-SBC applications
  - View, edit, and delete E-SBC device configurations
- Configure Advanced Options
  - Manage Subsystem Logs
  - CDR Listing
  - Feature Control
  - SIP options
  - Signaling port ranges
- Manage Global Parameters
  - RADIUS Authentication
  - SNMP Settings
  - Routing Profiles
  - Trace Settings
  - Syslog
- Manage Device-Specific Settings
  - Signaling Interface
  - Media Interface

This section provides an overview of the overall basic configuration process, including the following:

- E-SBC Architecture
- Basic Configuration Quick-Start Steps Checklists
  - Reconfigure E-SBC
  - Enabling Interfaces
  - Configuring URI Groups
  - Configuring Routing Profiles
  - Configuring Interworking
  - Adding Servers
  - Adding TLS Certificates
  - Adding TLS Server Profiles
  - Adding Domain Policy Groups
  - Adding Signal Interfaces
  - Adding Media Interfaces
  - Adding Server Flows
  - Adding Session Flows

Note: **This section only provides brief basic configuration checklists.**

For detailed procedures regarding each of the topics in this overview section, refer to the appropriate sections in the chapters listed below:

Chapter 5 — "Domain Policy Administation"
Chapter 6 — "System Configuration" (this chapter)
Chapter 7 — "Security Configuration"
Chapter 8 — "Network Configuration"

Architecture

Figure 6-1 provides an illustration the E-SBC platform and associated network architecture.

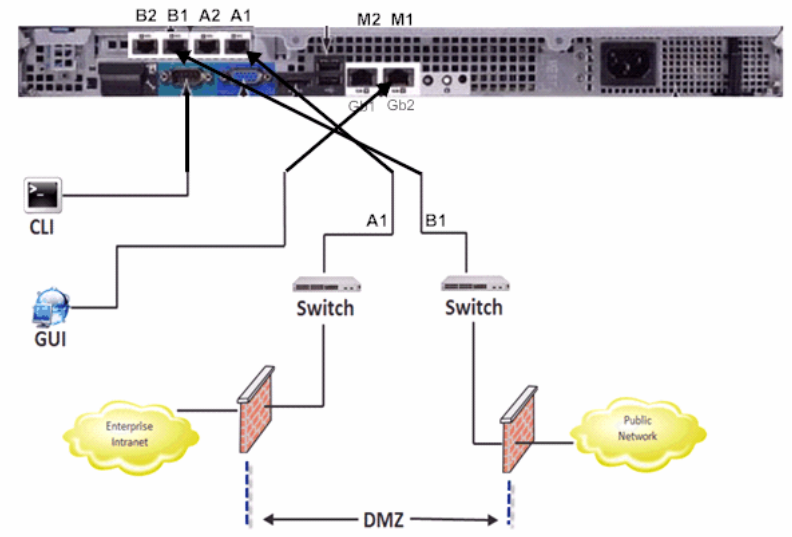


Figure 6-1 E-SBC Architecture

Basic Configuration Quick-Start Steps Checklists

Figure 6-2 below shows the basic configuration steps along with their associated Task Plane menu Feature selections where these steps are performed.

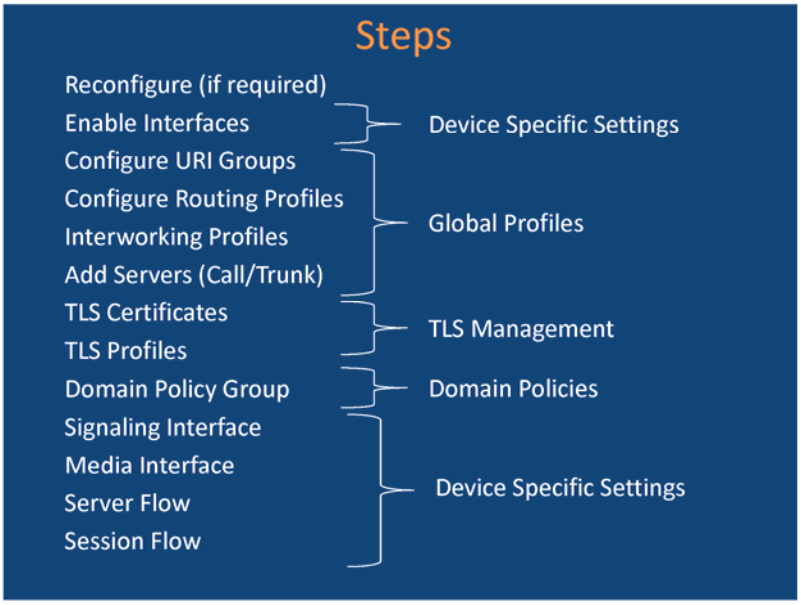


Figure 6-2 Basic Overall Configuration Steps

Reconfigure E-SBC Checklist

Note:	E-SBC reconfiguration is only required if you are going to change the management (M1) IP.

Reconfigure E-SBC by performing the following:

1. Uninstall the E-SBC device from the GUI.
2. Initiate a secure shell (SSH) connection to the E-SBC (ipcs/SIPera_123).
3. Run the reconfigure script: **/usr/local/ipcs/icu/scripts/ipcs-reconfigure**
4. Reprovision the E-SBC in the GUI.

Enabling Interfaces Checklist

Note:	Assume IP addresses for all ports have been assigned during installation or reconfiguration.

Enable Interfaces by performing the following:

1. Select: **Device Specific > Network Management > Interface Configuration**
2. Enable**: A1, B1**

Configuring URI Groups Checklist

Note:	Configure URI Groups to define dialed phone numbers for routing purposes.

Configure URI Groups by performing the following:

1. Select: **Global Profiles > URI Groups**
2. Explain existing URI Groups

URI Group Configuration Example

3. Add Group
4. Name = URI-*xxxx*
5. Add URI Group (select Dial Plan)
6. 9*XXXX*@.*
7. Finish

Configuring Routing Profiles Checklist

Note:	Configure Routing Profiles to define the route for a particular URI.

Configure Routing Profiles by performing the following:

1. Select: **Global Profiles > Routing**
2. Explain existing Routes

Routing Profile Configuration Example

3. Add Profile
4. Name = Route-*xxxx*
5. URI Group = URI-*xxxx*
6. Next Hop Server 1 = *xxxx*
7. Outgoint Transport = UDP

Configuring Interworking Checklist

Note:	Configure Interworking Profiles to manipulate headers, etc. for compatibility.

Configure Interworking Profiles by performing the following:

1. Select: **Global Profiles > Server Interworking**
2. Explain existing Interworking Profiles
    a. SIP Trunk Interworking

Interworking Configuration Example

3. Add Profile
    a. Name = Interwork-*xxxx*
    b. Describe the screens
    c. Click all **Next** and **Finish** buttons

Adding Servers Checklist

Note:	Configure to add Call Servers and Trunk Servers (SIP Trunk).

Add servers by performing the following:

1. Select: **Global Profiles** > **Server Configurations**
2. Explain existing configurations

Add Server Configuration Example

3. Add Profile
4. Name = Server-*xxxx*
5. Type = Call Server
6. Addresses = *xxxx*
7. Transports = TCP, UDP port 5060
8. Interworking Profile = Interwork-*xxxx*

Adding TLS Certificates Checklist

Note:	TLS Certificates are only needed if line side phones are encrypted.

Add TLS Certificates by performing the following:

1. Select: **TLS Management** > **Certificates**

TLS Certificate Configuration Example

2. Generate CSR
3. Install a certificate
4. More steps involved (see details in Chapter 8, “Network Configuration.”)

Adding TLS Server Profiles Checklist

Note: Create a new TLS Server Profile to allow encrypted phones to connect.

Configure TLS Server Profiles by performing the following:

1. Select: **TLS Management > Server Profiles**
2. Explain existing profile

TLS Server Profile Configuration Example

3. Add Profile
4. Name = TLS-*xxxx*
5. Finish

Adding Domain Policy Groups Checklist

Note: Policy Groups contain our policy sets and rules.

Configure URI Groups by performing the following:

1. Select: **Domain Policies > End Point Policy Groups**
2. Explain existing Policy Groups and Policy Sets

Policy Group Configuration Example

3. Add Group
4. Name = Policy-*xxxx*
5. Choose default rules
6. Finish

Adding Signal Interfaces Checklist

Note: Signal Interfaces define the type of signaling on the ports.

Configure Signaling Interfaces by performing the following:

1. Select: **Device Specific Settings > Signaling Interface**
2. Explain existing Signaling Interfaces

Signaling Interface Configuration Example

3. (Refer to further details in the appropriate section in Chapter 6 (this chapter).

Adding Media Interfaces Checklist

Note: Media Interfaces define the type of signaling on the ports.

Configure Media Interfaces by performing the following:

1. Select: **Device Specific Settings > Media Interface**
2. Explain existing Media Interfaces

Media Interface Configuration Example

3. (Refer to further details in the appropriate section in Chapter 6 (this chapter).

Adding Server Flows Checklist

Note: Server Flows allow us to categorize trunk-side signaling and apply a policy.

Configure Server Flows by performing the following:

1. Select: **Device Specific Settings > Endpoint Flows > Server Flows**
2. Explin existing flows

Server Flow Configuration Example

3. Name = Server Flow-*xxxx*
4. Server = Server-*xxxx*
5. Finish

Adding Session Flows Checklist

Note:	**Session Flows allow us to categorize media traffic and apply a policy.**

Configure Session Flows by performing the following:

1. Select: **Device Specific Settings > Session Flows**
2. Explain existing flows

Session Flow Configuration Example

3. Session Policies (codec negotiation and media anchoring) are available by selecting: **Domain Policies > Session Policies**

Backup / Restore System Information

The **Backup/Restore** feature provides the ability to backup (make a *snapshot*) of the EMS security configuration to a user-definable location that is secure and physically-separate from the E-SBC equipment chassis for later retrieval or restoration.

Note:	A configuration backup can be taken manually and restored as needed. Scheduled backup operations are currently not supported.

Designating a Snapshot Server

Before the Backup/Restore feature can be used, a server must first be designated as a *snapshot server* to hold the backup files, from which they can be retrieved when necessary.

Use the following procedure to designate a snapshot server.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select **Backup/Restore** from the Task Pane.
   The **Backup/Restore** screen will be displayed in the Content Area, defaulting to the **Snapshots** tab display (Figure 6 - 1).
3. Select the **Snapshot Servers** tab.
   The **Snapshot Servers** screen will be displayed in the Content Area (Figure 6-2).

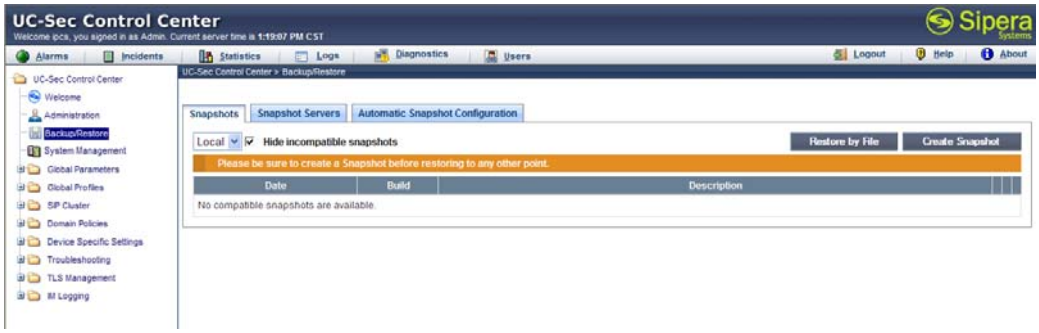


Figure 6 - 1 Typical Backup/Restore Screen

Figure 6-2 Backup/Restore Screen - Snapshot Servers Tab Display

4. Select **Add Server.**
   The **Add Snapshot Servers** pop-up window will be displayed (Figure 6-3).

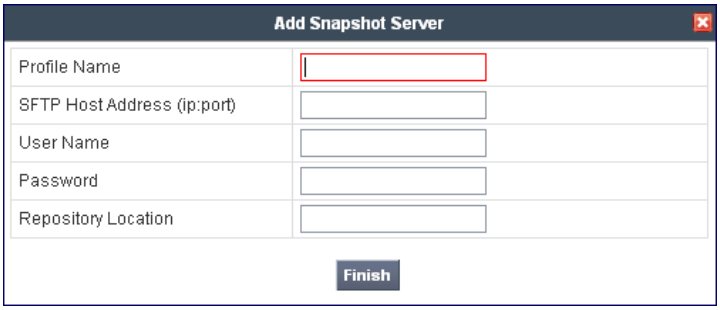


Figure 6-3 Add Snapshot Server Pop-up Window

5. Add the requested information into the fields provided according to the information contained in Table 6-1.

Table 6-1. Add Snapshot Server Pop-up Window Field Descriptions.

Field	Description
Profile Name	A descriptive name that will be used to refer to the snapshot server being configured.
SFTP Host Address (ip:port)	The physical IP address and port number of the snapshot server to which backup files (snapshots) will be transferred via secure FTP (SFTP).
User Name	The **User Name** of the administrative account which is authorized to make system backups.
Password	The password assigned to authenticate the administrative accounted identified in the previous field.
Repository Locations	The physical path (directory) on the snapshot server where the backup files will be stored to and retrieved from.

6. Select **Finish.**
   The **Snapshot Server** will be created and displayed in the Content Area (Figure 6-4).

Figure 6-4 Updated Backup/Restore Screen - Snapshot Servers Tab Display

Making a System Snapshot (Backup)

1. Login to the E-SBC Control Center as the **Admin.**
2. Select **Backup/Restore** from the Task Pane.
   The **Backup/Restore** screen will be displayed in the Content Area, defaulting to the **Snapshots** tab display.
3. Select create **Snapshot Servers.**

   The **Create Snapshot** pop-up window will be displayed (Figure 6-5).
4. Enter a name to designate this snapshot (backup) file and click **Finish**.
   A snapshot (backup) of the EMS security configuration is made and saved to the designated snapshot server. A banner will be displayed on the **Create Snapshot** pop-up window informing you that the snapshot has been successfully created (Figure 6-6). When the process has completed, the newly created snapshot will be displayed in the Content Area of the **Snapshots** screen (Figure 6-7).

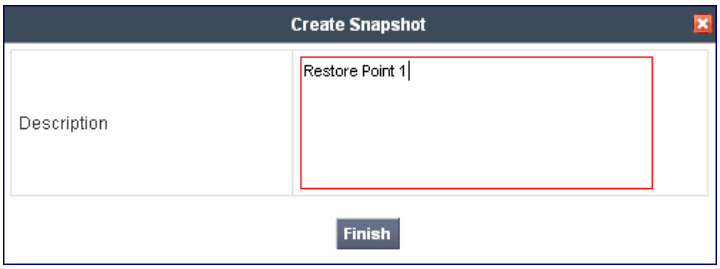


Figure 6-5. Create Snapshot Pop-up Window.

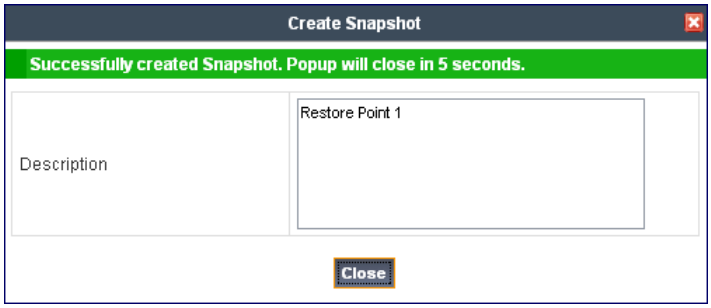


Figure 6-6. Snapshot Notification Banner.

Figure 6-7. Updated Backup/Restore Screen - Snapshots Tab Display.

Restoring a System Snapshot (Backup)

Two methods are provided for restoring a snapshot to the EMS server; one is manual and the other is automatic. The manual method involves two steps but gives you more control over how the snapshot files will restore the EMS while the automated method simply restores the backup files without further intervention on your part.

Caution!

The process of restoring a snapshot (backup) file (both manual and automatic) takes the EMS off-line while the files are being transferred and the device reconfigured.

This means that no E-SBC detection or mitigation features will be available for the entire duration of the backup procedure, making your system vulnerable to intrusions and attacks.

It is strongly recommended that restoration procedures only be done during times of relative system inactivity or during normally scheduled periods of maintenance.

Manual Method

The manual method of restoring a snapshot to the EMS is a two-step process whereby the snapshot is first retrieved from the snapshot server to your local workstation and then uploaded to the EMS for re-configuration. Use the following two procedures in succession to restore an EMS to a previous snapshot configuration: *Retrieving a Snapshot File* and *Restoring a Snapshot File*.

Retrieving a Snapshot File

Use the following procedure to retrieve a snapshot file from the snapshot server and store it locally on your workstation for subsequent restoration on the EMS.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select **Backup/Restore** from the Task Pane.
   The **Backup/Restore** screen will be displayed in the Content Area, defaulting to the **Snapshots** tab display.
3. Using the drop-down menu in the Content Area, select the snapshot server that contains the snapshot file you want to retrieve (Figure 6-8).
   All the snapshot files that are contained on the selected snapshot server will be displayed in the Content Area.
4. Select the snapshot file you want to retrieve by clicking the corresponding **Download Restore Point** icon.
   A dialog pop-up window similar to that shown in Figure 6-9 will be displayed.
5. Select the **Save to Disk** radio button and click **OK**.
   Another dialog pop-up window similar to that shown in Figure 6-10 will be displayed.
6. Designate a destination to save the snapshot file and select **Save**.
   The snapshot file will be saved in the designated location.

Figure 6-8. Selecting a Snapshot Server.

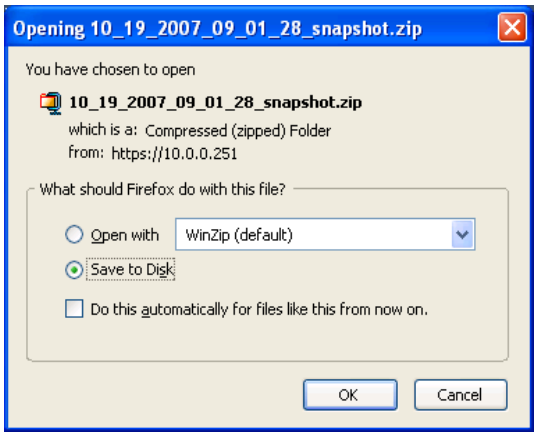


Figure 6-9. Designating a Snapshot File Action.

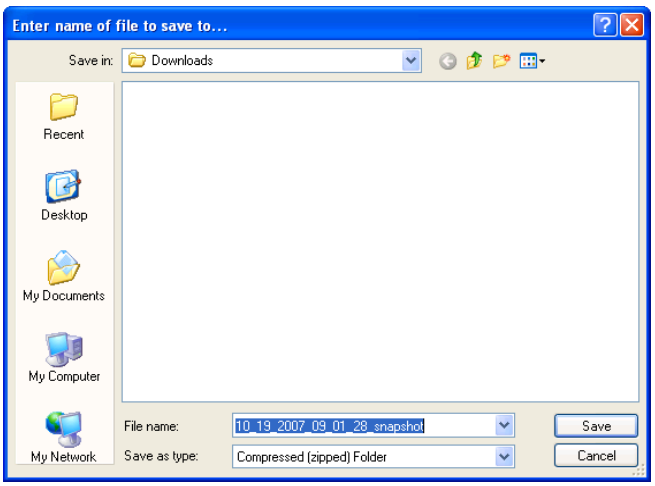


Figure 6-10. Directory Dialog Pop-up Window.

Restoring a Snapshot File

Once the snapshot file has been retrieved from the snapshot server and saved on your local workstation, it may now be uploaded to the EMS server where it will be uncompressed and used to reconfigure the EMS to a previous state.

Note:	**Any device whose management IP does not EXACTLY match the management IP contained in the snapshot will become inaccessible, INCLUDING THE EMS.**

Use the following procedure to upload the snapshot from your local workstation to the EMS server and reconfigure the EMS.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select **Backup/Restore** from the Task Pane.
   The **Backup/Restore** screen will be displayed in the Content Area, defaulting to the **Snapshots** tab display.
3. Select **Restore by File**.
   The **Restore by File** pop-up window will be displayed (Figure 6-11).

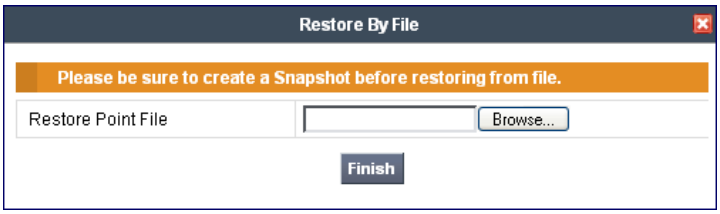


Figure 6-11. Restore by File Pop-up Window.

4. Select **Browse.**
   A **File Upload** dialog pop-up widow similar to that shown in Figure 6-12 will be displayed.
5. Select the desired snapshot file and select **Open.**
   The selected snapshot file is entered into the **Restore Point File** field of the **Restore by File** pop-up window (Figure 6-13).
6. Select **Finish.**
   A warning pop-up window will be displayed similar to that shown in Figure 6-14, asking you to confirm that you want to proceed with the restoration procedure.
7. Select **OK.**
   The EMS will be taken off-line and the snapshot file transferred to the EMS server, where it will be uncompressed and used to reconfigure the EMS software to a previous configuration.

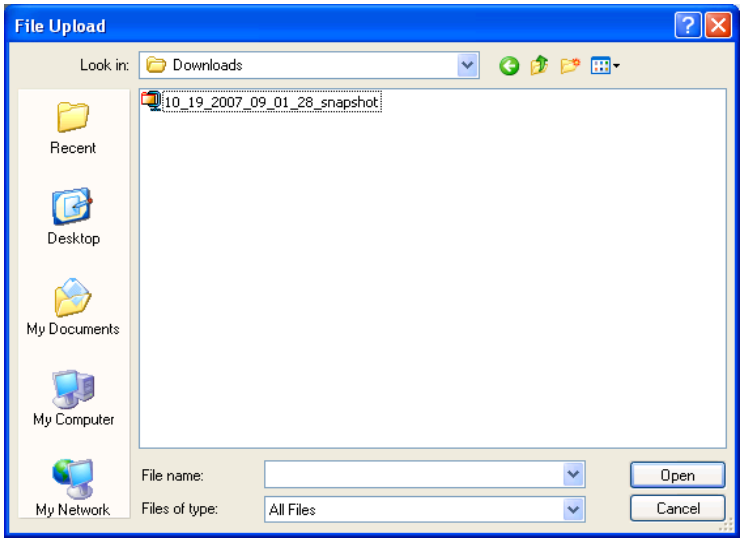


Figure 6-12. File Upload Dialog Pop-up Window.

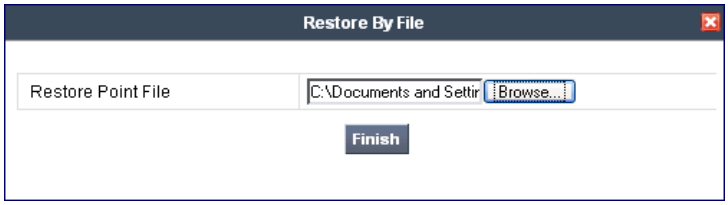


Figure 6-13. Updated Restore by File Pop-up Window.

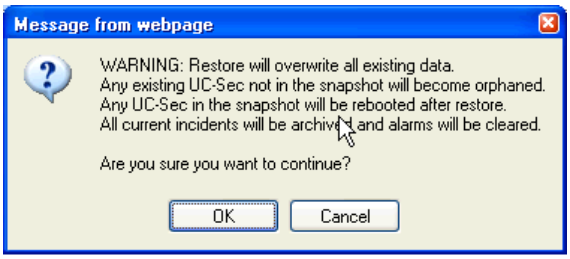


Figure 6-14. Restoration Warning Pop-up Window.

Automatic Method

The automatic method of restoring a snapshot to the EMS is a single-step process which restores the EMS to the previous configuration (snapshot) without further intervention on your part.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select **Backup/Restore** from the Task Pane.
   The **Backup/Restore** screen will be displayed in the Content Area, defaulting to the **Snapshots** tab display.
3. Using the drop-down menu in the Content Area, select the snapshot server that contains the snapshot file you want to retrieve (Figure 6-8).
   All the snapshot files that are contained on the selected snapshot server will be displayed in the Content Area.
4. Select the snapshot file you want to restore to the EMS by clicking the corresponding **Download Restore from this Point** icon.
   A warning pop-up window will be displayed similar to that shown in Figure 6-15, asking you to confirm that you want to proceed with the automatic restoration procedure.
8. Select **OK**.
   The EMS will be taken off-line and reconfigured with the snapshot file.

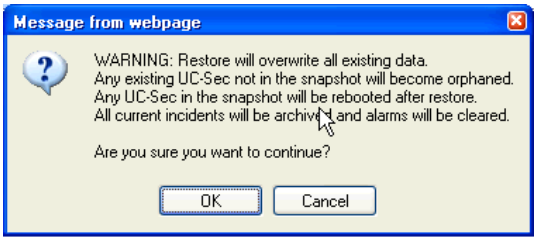


Figure 6-15. Restoration Warning Pop-up Window.

Deleting a System Snapshot (Backup)

Use the following procedure to delete an existing system snapshot.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select **Backup/Restore** from the Task Pane.

The **Backup/Restore** screen will be displayed in the Content Area, defaulting to the **Snapshots** tab display.

3. Select the **Delete** icon that corresponds to the snapshot you want to delete.
   A **Delete Confirmation** pop-up window is displayed, asking you to confirm your selection (Figure 6-16).

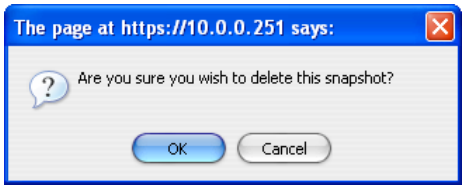


Figure 6-16. Delete Confirmation Pop-up Window.

4. Select **OK**.
   The snapshot file is deleted.

Automatic Snapshot Configuration

Use the following procedure for automatic snapshot configuration.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select **Backup/Restore** from the Task Pane.
   The **Backup/Restore** screen will be displayed in the Content Area, defaulting to the **Snapshots** tab display (Figure 6 - 1).
3. Select the **Automatic Snapshot Configuraion** tab.
   The **Automatic Snapshot Configuration** screen will be displayed in the Content Area (Figure 6-17).

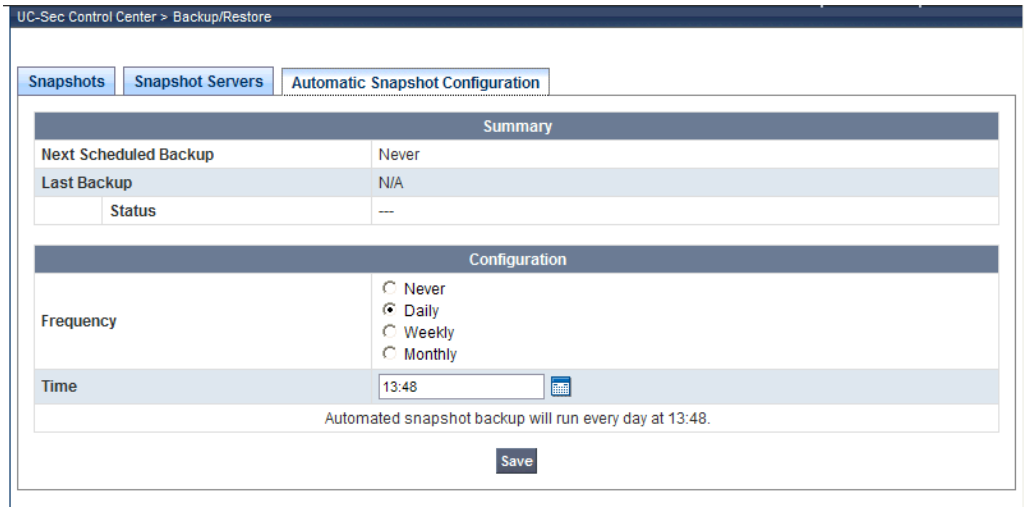


Figure 6-17. Automatic Snapshot Configuration Screen.

Note:	In the **Summary** area of the Automatic Snapshot Configuration tab, the configuration for a previously saved backup will be displayed if one existed, otherwise the default setting of **Never** will be displayed.

4. The Automatic Snapshot Configuration feature is easy to use, just select a frequency (i.e., Daily, Weekly, or Monthly) and select a time to start in the Time field, as shown in the example in Figure 6-18 below.

Note:	When the **Weekly** or **Monthly** Frequency option is selected, a group of **Day(s)** checkboxes (i.e., **Su**, **Mo**, **Tu**, **We**, **Th**, **Fr**, and **Sa**) is displayed. When the **Monthly** Frequency option is selected, an additional row of checkboxes is displayed for **Occurrence** (i.e., **1st**, **2nd**, **3rd**, **4th**, and **Last**). Clicking on the small calendar icon to the right of the **Time** field displays an **Edit Time** dialog box for entering the time and before clicking on the **Save** and **Close** buttons.

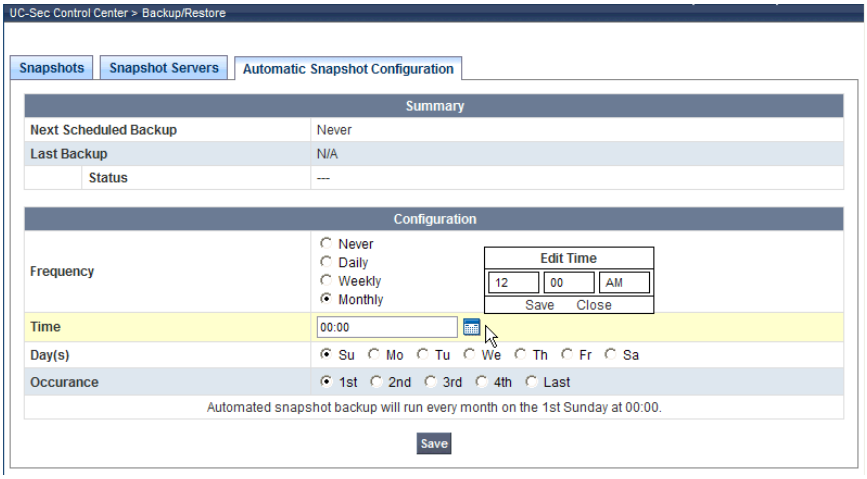


Figure 6-18. Automatic Snapshot Configuration Screen (cont).

Managing Deployed E-SBC Security Devices

In addition to configuring newly installed E-SBC security devices (Chapter 4, *Device Configuration*), the **System Management** feature also allows you to perform a number of additional functions which help you to effectively manage your network. The additional functions that can be performed using the **System Management** feature are:

- Establish secure shell sessions
- Shutdown and reboot individual E-SBC security devices
- Restart E-SBC applications
- Swap E-SBC devices
- View, edit, and delete E-SBC device configurations

Establishing a Secure Shell Session

Use the following procedure to establish a secure shell (SSH) communications session with an E-SBC security device.

1. Login to the E-SBC Control Center as the **Admin.**
   The System Management screen will be displayed in the Content Area, defaulting to the Installed tab display (Figure 6-20).
2. Select the **System Management** feature from the Task Pane (**Figure 6-19**).

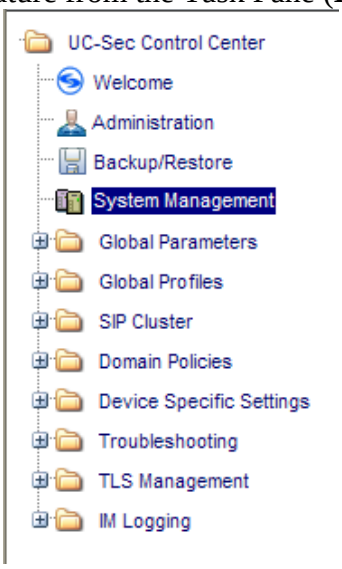


Figure 6-19. System Management Screen Selection

3. Click the **SSH** icon corresponding to the E-SBC security device to which you want to establish an SSH session.
   The **SSH Connection Profile** pop-up window will be displayed (Figure 6-22).

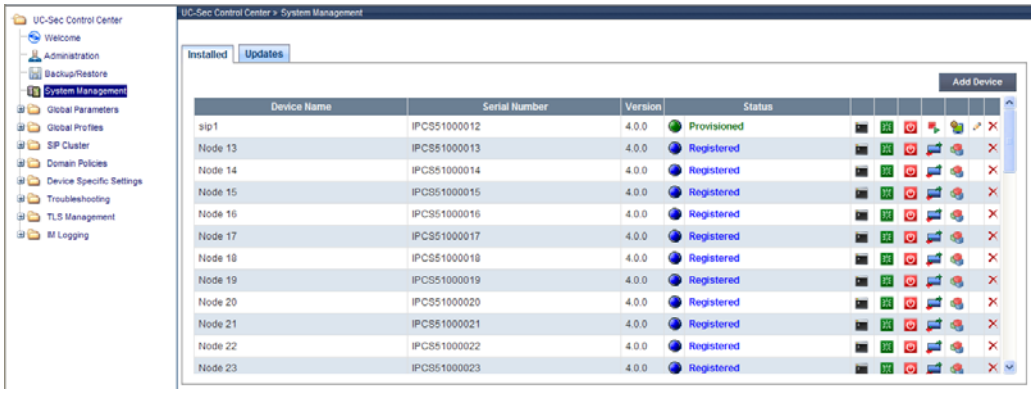


Figure 6-20. System Management Screen - Installed Tab Display.

Note: The Provisioned state, shown previously for some devices in (Figure 6-20) is an intermediate state between the initial Registered state and the final Commissioned state shown in Figure 6-21. A device should only be in either the Registered state or Commissioned state at any given time, remaining in the Provisioned state for a short period of time during the transition from Registered to Commissioned state.

Depending upon the state of a device, some options may not be available, such as the Edit Device icon that is not an available option for devices in the Registered state.

The System Management screen also provides HA status, including Primary or Secondary designations, for devices configured for HA, as shown in Figure 6-21 below.

Device Name	Serial Number	Version	Status
NWU-HA (DOWN)	IPCS51005122	3.6.0.Q48	Commissioned
NWU-HA (Primary)	IPCS51005123	3.6.0.Q48	Commissioned

Figure 6-21. System Management Screen HA Status Information

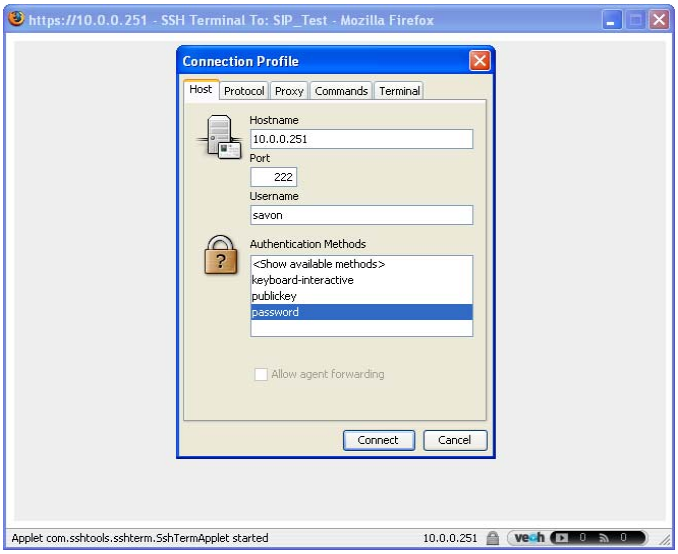


Figure 6-22. SSH Connection Profile Pop-up Window.

4. Enter the user name into the **Username** field and select password as the **Authentication Method.**
5. Select **Connect.**
   The **SSH Password Authentication** pop-up window will be displayed (Figure 6-23).
6. Enter the requested password and select **OK.**
   The SSH session is established (Figure 6-24).
7. Refer to Chapter 10, *Command Line Interface* for more information on using the command line interface (CLI) and related commands.

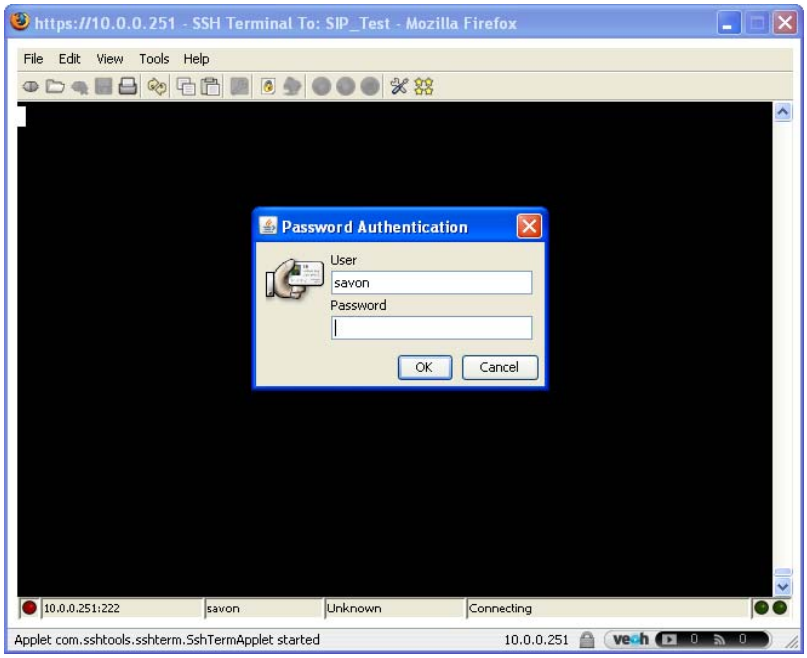


Figure 6-23. SSH Password Authentication Pop-up Window.

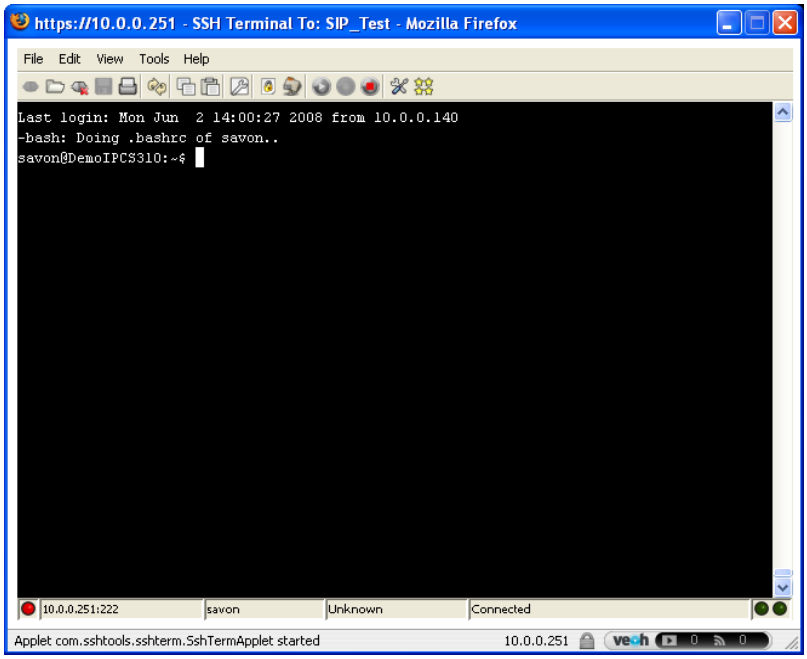


Figure 6-24. Active SSH Communications Session.

Shutdown and Reboot an E-SBC Security Device

Use the following procedures to shutdown or reboot an individual E-SBC security device.

Shutdown

1. Login to the E-SBC Control Center as the **Admin**.

2. Select the **System Management** feature from the Task Pane (Figure 6-19).
   The System Management screen will be displayed in the Content Area, defaulting to the Installed tab display (Figure 6-20).
3. Click the **Shutdown Device** icon corresponding to the E-SBC security device you want to shutdown.
   A pop-up window similar to that shown in Figure 6-25 will be displayed asking you to confirm your selection.

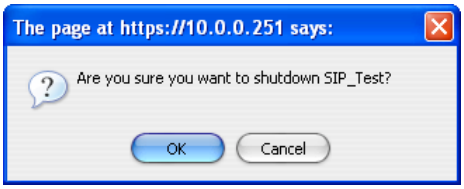


Figure 6-25. Shutdown Confirmation Pop-up Window.

4. Click **OK**.
   A notification pop-up window similar to that shown in Figure 6-26 will be displayed when the device has been successfully shutdown.

Figure 6-26. Successful Shutdown Notification Pop-up Window.

Reboot

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **System Management** feature from the Task Pane (Figure 6-19).
   The System Management screen will be displayed in the Content Area, defaulting to the Installed tab display.
3. Click the **Reboot Device** icon corresponding to the E-SBC security device you want to reboot.
   A pop-up window similar to that shown in Figure 6-27 will be displayed asking you to confirm your selection.

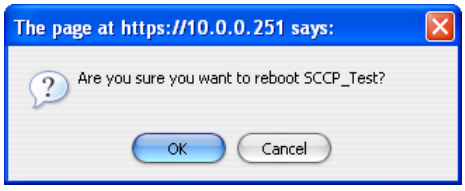


Figure 6-27. Reboot Confirmation Pop-up Window.

4. Click **OK**.

A notification pop-up window similar to that shown in Figure 6-28 will be displayed when the device has been successfully rebooted.

Figure 6-28. Successful Reboot Notification Pop-up Window.

Restarting an E-SBC Application

Use the following procedure to restart a stopped E-SBC application.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **System Management** feature from the Task Pane (Figure 6-19).
   The System Management screen will be displayed in the Content Area, defaulting to the Installed tab display.
3. Click the **Restart Application** icon corresponding to the E-SBC security device whose application you want to restart.
   A pop-up window similar to that shown in Figure 6-29 will be displayed asking you to confirm your selection.

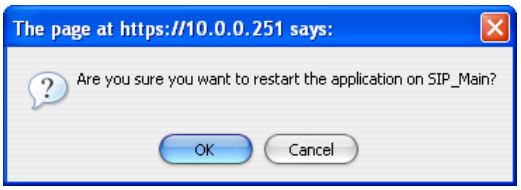


Figure 6-29. Restart Application Confirmation Pop-up Window.

4. Click **OK**.
   A notification pop-up window similar to that shown in Figure 6-30 will be displayed when the device has been successfully restarted.

Figure 6-30. Successful Restart Notification Pop-up Window.

Managing E-SBC Device Configurations

Use the following procedures to view, edit, and delete individual E-SBC security device configurations.

View Configuration

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **System Management** feature from the Task Pane (Figure 6-19).
   The **System Management** screen will be displayed in the Content Area, defaulting to the **Installed** tab display (Figure 6-31).
3. Click the **View Config** icon corresponding to the E-SBC security device whose configuration you want to view.
   A **Device Configuration** pop-up window similar to that shown in Figure 6-32 will be displayed for you to view.

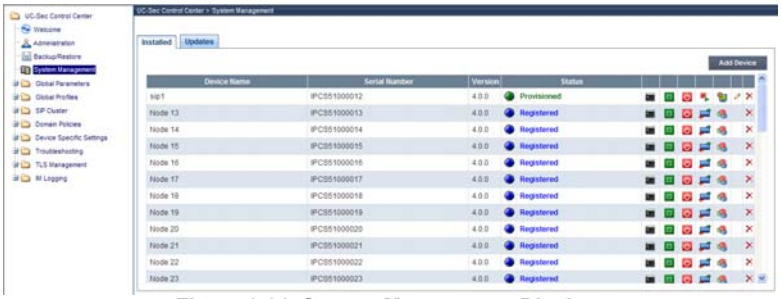


Figure 6-31. System Management Display.

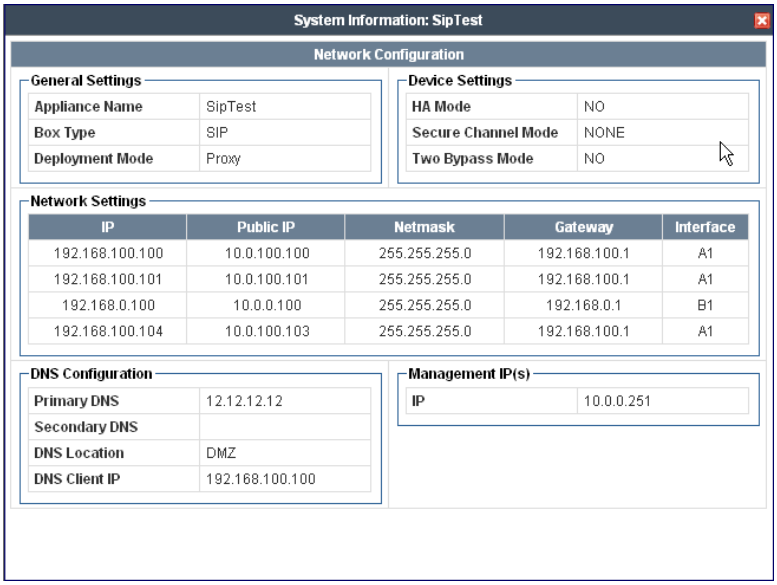


Figure 6-32. E-SBC Device Configuration Window

4. Click the **Cancel** icon when you are finished viewing the configuration information.
   The **Device Configuration** pop-up window will be closed.

Edit Configuration

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **System Management** feature from the Task Pane (Figure 6-19).
   The **System Management** screen will be displayed in the Content Area, defaulting to the **Installed** tab display (Figure 6-31).
3. Click the **Edit Device** icon corresponding to the E-SBC security device whose configuration you want to edit.
   The **Edit Device Configuration** pop-up window will be displayed (Figure 6-33).

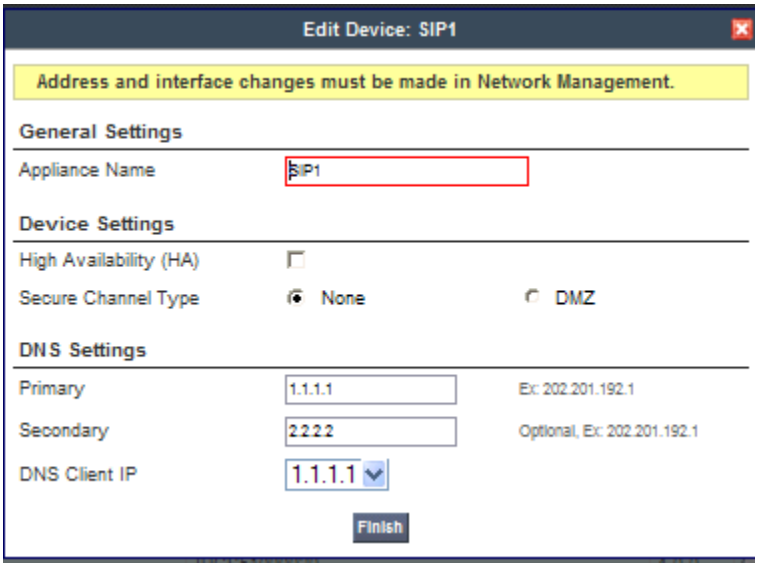


Figure 6-33. Edit Device Pop-up Window

4. Make the necessary changes or click the **Cancel** icon to close the window without saving your changes.
5. Select **Finish**.
   The changes are saved to the E-SBC configuration file. If you want to make additional changes to the E-SBC configuration, see Chapter 8, *Network Configuration*.

Delete Configuration

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **System Management** feature from the Task Pane (Figure 6-19).
   The **System Management** screen will be displayed in the Content Area, defaulting to the **Installed** tab display (Figure 6-31).
3. Click the **Delete Device** icon corresponding to the E-SBC security device whose configuration you want to delete.
   A confirmation pop-up window similar to that shown in Figure 6-34 will be displayed asking you to confirm your selection.

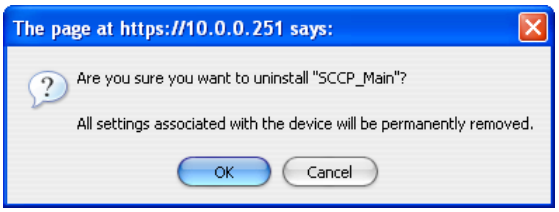


Figure 6-34. Delete Confirmation Pop-up Window.

4. Click **OK**.
   The E-SBC device configuration is deleted and the **System Management** screen is updated and redisplayed with the deleted device removed from the list.

System Management Updates

1. Login to the E-SBC Control Center as the **Admin**.
   Select the **System Management** feature from the Task Pane (Figure 6-19).
   The **System Management** screen will be displayed in the Content Area, defaulting to the **Installed** tab display (Figure 6-31).
2. Click the **Updates** tab to display System Management Updates screen (Figure 6-35).
   From the Updates screen, you can select an upgrade package and initiate a system upgrade.

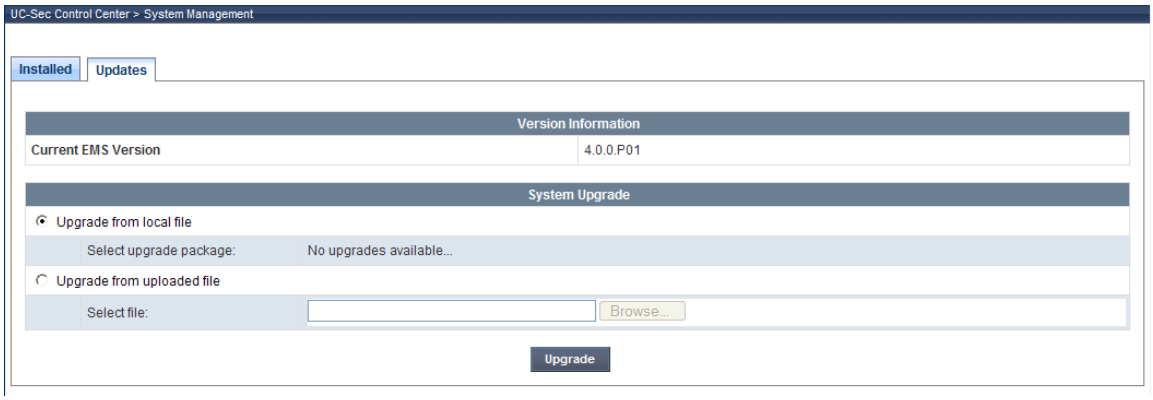


Figure 6-35. System Management Updates Screen

Configuring Advanced Options

The **Advanced Options** function of the **Troubleshooting** feature allows you to: enable or disable E-SBC subsystem execution logs; enable or disable E-SBC security features; configure SIP signaling message options; and designate signaling and media port ranges. In addition, you can view system-generated Call Detail Records (CDRs).

Enabling / Disabling E-SBC Logging Level

The **Subsystem Logs** tab of the **Advanced Options** function allows you to enable (or disable) certain E-SBC subsystem event logs: **Message, Information,** and **Warning**. Use the following procedure to manage the debug log files.

1. Login to the E-SBC Control Center as the **Admin**.

2. Select the **Advanced Options** function of the **Troubleshooting** feature from the Task Pane (Figure 6-36).

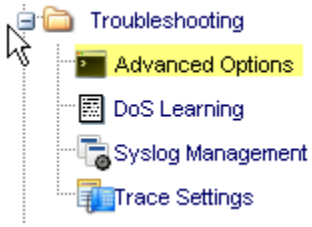


Figure 6-36. Advanced Options Function

A list of installed E-SBC security devices is displayed in the Application Pane under the heading **E-SBC Devices**. The Subsystem Logs tab (Figure 6-37 for E-SBC and Figure 6-38 for EMS).

Note When the **Advanced Options** feature is selected in the Task Pane, the Content Area defaults to the **Subsystem Logs** tab.

Figure 6-37. Advanced Options: Subsystem Logs Display (E-SBC View).

Figure 6-38. Advanced Options: Subsystem Logs Display (EMS View).

3. From the Application Pane, select the E-SBC device for which you want to manage log files.
   The **Advanced Options** screen defaults to the **Subsystem Logs Level** tab display.
4. Check ☑ or uncheck ☐ the box corresponding to the type of execution log you want to **Enable** (checked) or **Disable** (unchecked).
5. Select **Save** when you are finished.

Viewing a CDR File

The **CDR Listing** tab of the **Advanced Options** function allows you view system-generated Call Detail Records (CDRs). A CDR is a file that contains specific information about recent system call activity such as call sources, call destinations, call duration, etc. and is stored in a comma-separated values (CSV) file that can be downloaded and viewed at will using the following procedure.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Advanced Options** function of the **Troubleshooting** feature from the Task Pane (Figure 6-36).
   A list of installed E-SBC security devices is displayed in the Application Pane under the heading **E-SBC Devices** (Figure 6-37).
3. From the Application Pane, select the SIP-specific E-SBC device whose CDR files you want to view (Figure 6-39).

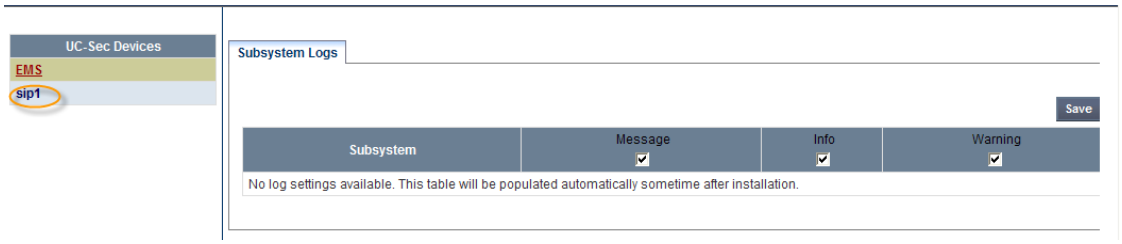


Figure 6-39. Selecting an E-SBC Security Device.

4. Select the **CDR Listing** tab.

   A list of available CDR files is displayed in the Content Area for the selected E-SBC security device (Figure 6-40).

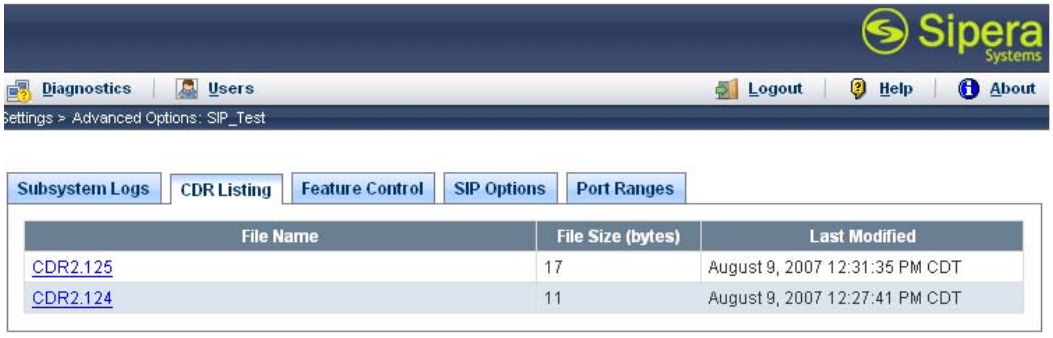


Figure 6-40. CDR Listing Tab Display.

5. Select the CDR file you want to view.
   A dialog box similar to that shown in Figure 6-42 is displayed.
6. Click the **Open with** radio button and select **EXCEL.EXE** as the program to use in viewing the CDR file (Figure 6-43).
7. Click **OK**.
   The CDR file is opened to display a log similar to that shown in Figure 6-44.

Note: The types of CDRs listed here are defined in the Application Rules screen in Miscellaneous area in the Edit Application Rule pop-up window. Refer to the section titled, “Application Rules,” in Chapter 5 of this document.

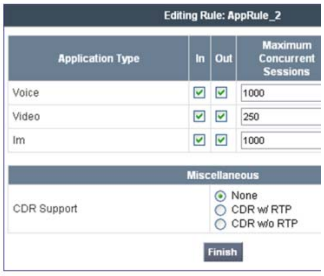


Figure 6-41. CDR Support Definition in Application Rules

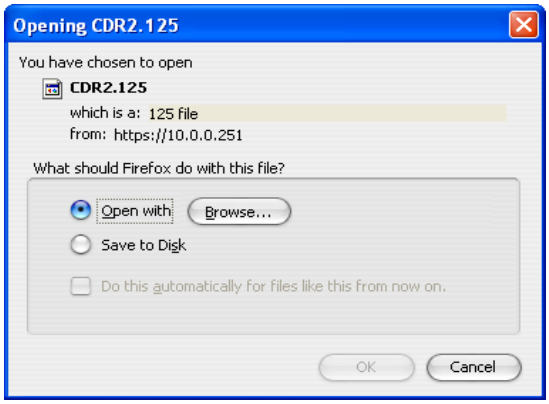


Figure 6-42. Open CDR Dialog Pop-up Window.

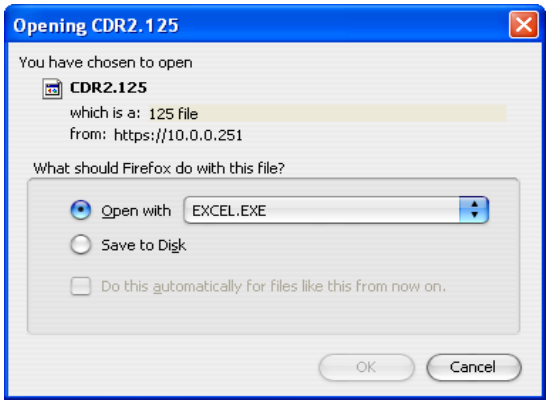


Figure 6-43. Selecting a Program to View the CDR File.

State	From	To	Source IP Addres	Time Stamp	Media Type	End Point Type	End Point Policy Name	Call Id	CDR Id	Session Id	Data
Initiated	sip:2435@sipera.co	sip:5002@sipera.co	10.10.51.252	Mon May 12 18:14:24 200	AUDIO	EP_SUBSCRIBER	default-med-enc	3c2678	1	533	
Initiated	sip:2435@sipera.co	sip:5002@sipera.co	172.16.51.51	Mon May 12 18:14:24 200	AUDIO	EP_CS	default-low	10e2ed	2	533	
Initiated	sip:2435@sipera.co	sip:5002@sipera.co	192.168.151.62	Mon May 12 18:14:24 200	AUDIO	EP_CS	default-low	10e2ed	1	534	
Initiated	sip:2435@sipera.co	sip:5002@sipera.co	172.16.51.52	Mon May 12 18:14:24 200	AUDIO	EP_SUBSCRIBER	default-med-enc	b9a2be	2	534	
Initiated	sip:2435@sipera.co	sip:5002@sipera.co	192.168.151.62	Mon May 12 18:14:24 200	AUDIO	EP_CS	default-low	10e2ed	1	535	
Initiated	sip:2435@sipera.co	sip:5002@sipera.co	172.16.51.52	Mon May 12 18:14:24 200	AUDIO	EP_SUBSCRIBER	default-med-enc	35a3b6	2	535	
Established	sip:2435@sipera.co	sip:5002@sipera.co	10.10.51.252	Mon May 12 18:14:26 200	AUDIO	EP_SUBSCRIBER	default-med-enc	3c2678	1	533	
Established	sip:2435@sipera.co	sip:5002@sipera.co	172.16.51.51	Mon May 12 18:14:26 200	AUDIO	EP_CS	default-low	10e2ed	2	533	
Established	sip:2435@sipera.co	sip:5002@sipera.co	192.168.151.62	Mon May 12 18:14:26 200	AUDIO	EP_CS	default-low	10e2ed	1	535	
Established	sip:2435@sipera.co	sip:5002@sipera.co	172.16.51.52	Mon May 12 18:14:26 200	AUDIO	EP_SUBSCRIBER	default-med-enc	35a3b6	2	535	
Terminated	sip:2435@sipera.co	sip:5002@sipera.co	10.10.51.252	Mon May 12 18:14:28 200	AUDIO	EP_SUBSCRIBER	default-med-enc	35a3b6	2	535	
Terminated	sip:2435@sipera.co	sip:5002@sipera.co	172.16.51.51	Mon May 12 18:14:28 200	AUDIO	EP_CS	default-low	10e2ed	1	535	
Terminated	sip:2435@sipera.co	sip:5002@sipera.co	172.16.51.52	Mon May 12 18:14:28 200	AUDIO	EP_SUBSCRIBER	default-med-enc	3c2678	1	533	
Initiated	sip:5002@sales.sip	sip:5001@sales.sip	10.10.51.252	Mon May 12 18:14:31 200	AUDIO	EP_SUBSCRIBER	default-med-enc	3c2678	1	537	
Initiated	sip:5002@sales.sip	sip:5001@sales.sip	172.16.51.51	Mon May 12 18:14:31 200	AUDIO	EP_CS	default-low	800bfd	2	537	

Figure 6-44. CDR File Display Example

In the CDR file display, the value in the **State** column (i.e., **Initiated**, **Established**, or **Terminated**) identifies the state of the call process at the time specified in the **Time Stamp** column on the associated information line.

The information in the **State** column and the **Time Stamp** column can be used in calculating the billing time for each call as illustrated below.

Definitions

State	Time Stamp
Initiated	*<the start time of the call>*
Terminated	*<the end time of the call>*
Established	*<the time that the call is established and the conversation can begin>*

Calculations

<Terminated Time> minus <Initiated Time> = <Total Time>

<Terminated Time> minus <Established Time> = <Billable Time>

Enabling / Disabling E-SBC Security Features

The **Feature Control** tab of the **Advanced Options** function allows you to enable (or disable) system-wide E-SBC security features. Use the following procedure to manage the activation of these features.

Note:	The E-SBC-specific security features enable/disable settings described next, are accessible by selecting: **Troubleshooting → Advanced Options** The security features enable/disable settings defined here apply specifically to each E-SBC Device that is currently selected in the Application Pane. These settings only enable or disable one or more security features for the selected E-SBC Device. The actual thresholds for each one of these security features are globally defined for all E-SBC Devices within the network by selecting: **Global Parameters → DoS/DDoS** See the Chapter 7 section , "DoS Security Features," for more details.

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Advanced Options** function of the **Troubleshooting** feature from the Task Pane (Figure 6-36).
   A list of installed E-SBC security devices is displayed in the Application Pane under the heading **E-SBC Devices** (Figure 6-37).
3. From the Application Pane, select the SIP-specific E-SBC device whose security features you want to manage (Figure 6-39).
4. Select the **Feature Control** tab in the Content Area.
   The **Feature Control** screen is displayed (Figure 6-45).
5. In the **Enable / Disable** column, check ☑ or uncheck ☐ the box corresponding to the security feature you want to **Enable** (checked) or **Disable** (unchecked). Enabling a feature directs the E-SBC security device to detect the indicated anomaly (DoS, DDoS, etc.) or perform the corresponding service (IM Logging, Random Early Drop (RED), etc.).

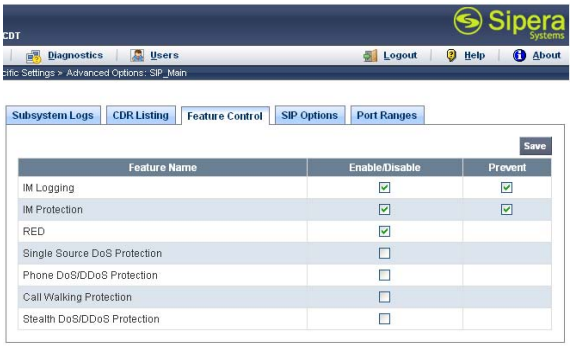


Figure 6-45. Feature Control Tab Display.

6. Select **Save** when you are finished.

Managing SIP Options

The **Feature Control** tab of the **Advanced Options** function allows you to enable and disable DNS caching. Use the following procedure to manage these features.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Advanced Options** function of the **Troubleshooting** feature from the Task Pane (Figure 6-36).
   A list of installed E-SBC security devices is displayed in the Application Pane under the heading **E-SBC Devices** (Figure 6-37).
3. From the Application Pane, select the E-SBC device whose security features you want to manage (Figure 6-39).
4. Select the **Feature Control** tab in the Content Area, and make the appropriate selections.
5. Select the SIP Options tab.
   The **SIP Options** screen is displayed (Figure 6-46).

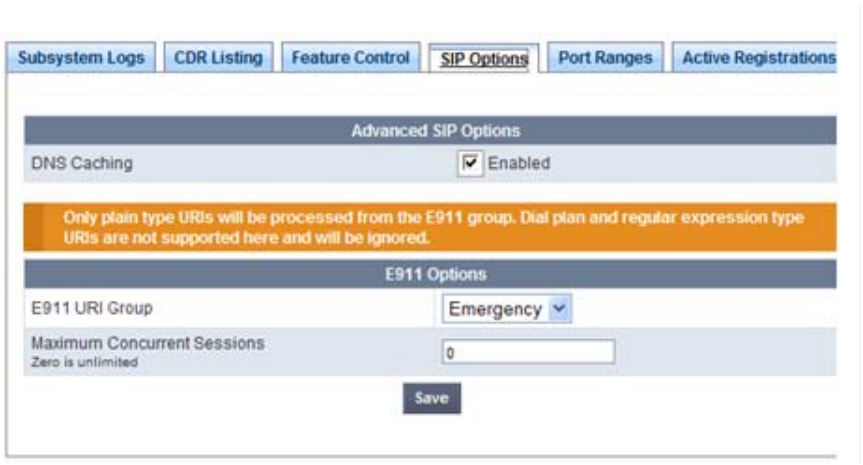


Figure 6-46. SIP Options Tab Display.

6. Make your selections based upon the information contained in Table 6-2 and click **Save**.
   Your selections are saved.

Table 6-2. SIP Options Tab Display Field Descriptions.

Field	Description
DNS Caching	Checkbox enabling (☑) or disabling (☐) DNS Caching.
E911 URI Group	Selecting **Emergency** enables the numbers contained in the **Emergency** URI group to be free from any dial-out restrictions which may be imposed by Domain Policies. The **Emergency** URI group is an integral part of the system (not user-defined) that defines special numbers that should not be restricted by any Domain Policies.
Maximum Concurrent Sessions	The number of allowed concurrent dial-out sessions. Entering a value of zero (0) allows unlimited sessions.

Note:	The Emergency URI group is defined in the URI Groups function of the Global Profiles feature (described in the section titled, “Managing Global Parameters” in Chapter 6 of this document. The Emergency URI group can be edited to add/delete numbers by following the procedure described in the section titled, “Editing an Existing URI Group” in chapter 5 of this document.

Port Options

The **Port Ranges** tab of the **Advanced Options** function allows you to set the range of ports on which internal signaling and media traffic will be received and sent. Use the following procedure to manage this feature.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Advanced Options** function of the **Troubleshooting** feature from the Task Pane (Figure 6-36).
   A list of installed E-SBC security devices is displayed in the Application Pane under the heading **E-SBC Devices** (Figure 6-37).
3. From the Application Pane, select the E-SBC device whose security features you want to manage (Figure 6-39).
4. Select the **Port Ranges** tab in the Content Area.
   The **Port Ranges** screen is displayed (Figure 6-47).

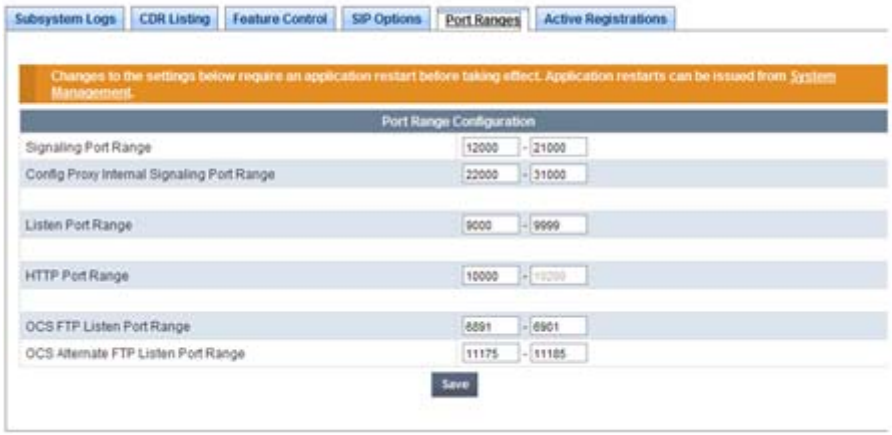


Figure 6-47. Port Ranges Tab Display

Notes:	**Signaling Port Range** – (Direction = Away from E-SBC) This port range is used by E-SBC to initiate connections for outgoing SIP requests from E-SBC towards a SIP Server (Call Server or Trunk Server). **Config Proxy Internal Signaling Port Range** – (Direction = Away from E-SBC) This port range is used by E-SBC to initiate connections from E-SBC toward Configuration Servers (i.e., Configuration Servers of the following types: HTTP, HTTP Proxy, HTTPS, LDAP, TFTP, and SCEP.

Listen Port Range – (Direction = Toward E-SBC) This port range is used in PORTID Mode (see the Chapter 8 section, "*Managing SIP Server Configurations*" E-SBC listens on these ports for requests from a SIP Server (usually a Call Server) during non-persistent phone-related communications (e.g., calls, signaling) where a link does not stay up indefinitely.

HTTP Port Range – (Direction = Away from E-SBC) This port range is used by Tinyproxy to initiate connections for E-SBC towards the upstream server or any other http server based on the routing for non-persistent non-phone-related communications (e.g., web services, media) where a link does not stay up indefinitely.

OCS FTP Listen Port Range and **OCS Alternate FTP Listen Port Range** – **For OCS use only.** (Direction = Toward E-SBC) This port range is used for OCS FTP. OCS clients operate with two fixed port ranges (one range with starting port 6891 and an alternate range with starting port 11175), therefore E-SBC provides two separate range parameter fields (**OCS FTP Listen Port Range** and **OCS Alternate FTP Listen Port Range**) to accommodate an OCS deployment.

For SIP deployments, ***Internal*** (toward Call Server) signaling interfaces and media interfaces and ***External*** (toward Trunk Server) signaling interfaces and media interfaces are created and defined using the **Signaling Interface** and **Media Interface** functions of the **Device Specific Settings** feature from the Task Pane.

Fixed Ports – (Direction = Toward E-SBC) Note that the fixed Ports for TCP, UDP, or TLs defined under **Device Specific Settings > Signaling Interface** should not be assigned a port number that falls within a Signaling Port Range. A fixed Port for TCP, UDP, or TLS is a shared Listen Port for multiple calls incoming to E-SBC from a Trunk Server or Call Server.

5. Enter the beginning and ending port numbers for each of the fields listed and click **Save.**
   Your selections are saved.

Enabling HA

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **System Management** feature in the Task Pane (Figure 6-36).
   A list of installed E-SBC security devices is displayed in the Content Pane under the **Installed** tab.

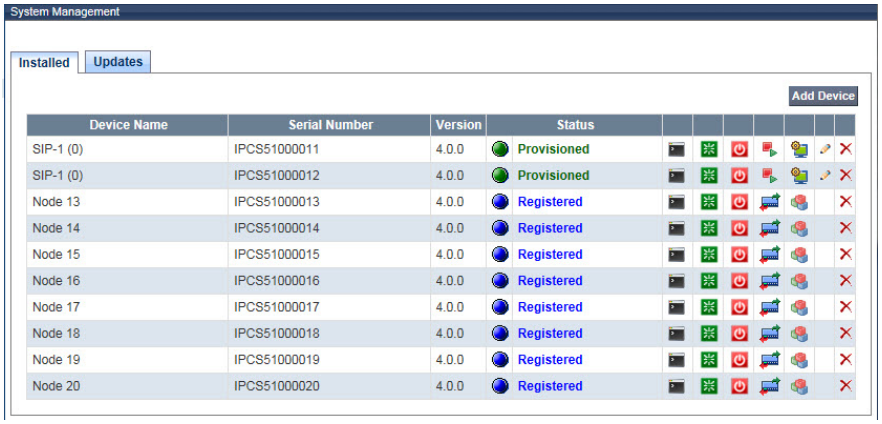


Figure 6-48. System Management Installed Tab

3. Click the Edit Device icon corresponding to the E-SBC security device whose configuration you want to edit. The Edit Device Configuration pop-up window will be displayed.
4. Select the High Availability (HA) checkbox.
5. Select a Device Pair from the pull-down list.
6. Click on the **Finish** button to save and exit.

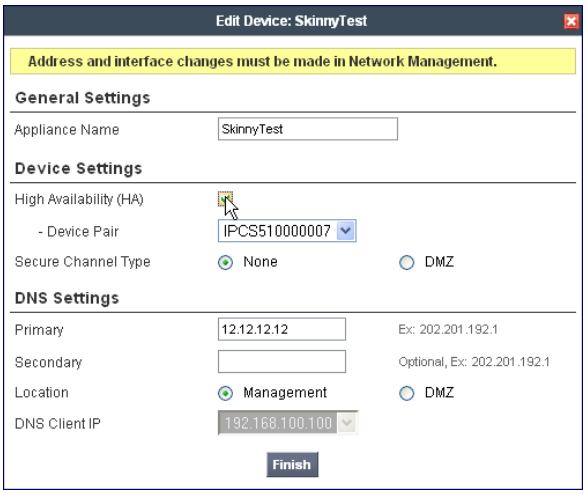


Figure 6-49. Edit Device Configuration Pop-up Window

Configuring HA Heartbeat Interval and Max Retries

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Advanced Options** function of the **Troubleshooting** feature from the Task Pane (Figure 6-36).
   A list of installed E-SBC security devices is displayed in the Application Pane under the heading **E-SBC Devices** (Figure 6-37).
3. From the Application Pane, select the E-SBC device whose security features you want to manage (Figure 6-39).
4. Select the **HA Pairs** tab in the Content Area.
   The Edit HA Pairs Option pop-up window is displayed.

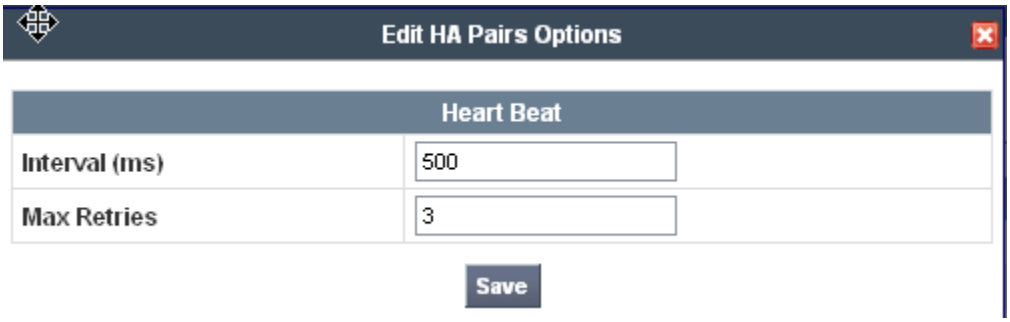


Figure 6-50. HA Pairs Tab

6. Enter the appropriate values for Heart Beat Interval (ms) and maximum retries, and click the **Save** button to save and exit.

Managing Global Parameters

The **Global Parameters** feature allows you to provision Simple Network Management Protocol (**SNMP**) parameters to enhance alarm reporting. By supporting each of the three current versions of **SNMP** (v1, v2, and v3), this feature allows you to take advantage of the most up-to-date security and remote configuration capabilities available to efficiently manage network events (alarms).

In addition to managing SNMP parameters, the **Global Parameters** feature also allows you to manage **Syslog** and **RADIUS** parameters, as well as designate the secure channel source and destination ports and provision authorized user agents (end-points).

Managing RADIUS Authentication Parameters

Use the following procedure to manage RADIUS authentication parameters.

Adding a New RADIUS Server

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **RADIUS** (authentication) function of the **Global Parameters** feature from the Task Pane (Figure 6-51).

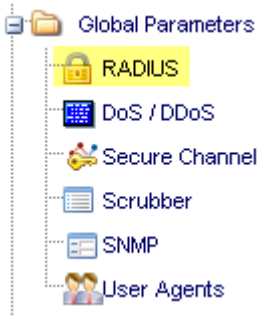


Figure 6-51. Selecting the RADIUS Authentication Function

3. The **Radius** screen is displayed (Figure 6-52).
4. Select **Add Server**.

   The **Add RADIUS Server** pop-up window is displayed (Figure 6-53).
5. Enter the requested information into the appropriate fields.
   Table 6-3 describes each user-definable field displayed in the **Add RADIUS Server** pop-up window.

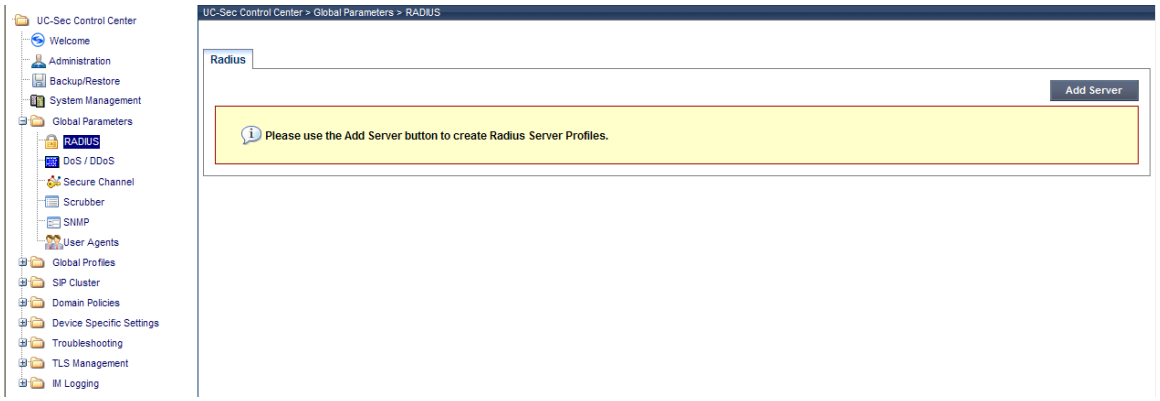


Figure 6-52. RADIUS Tab Display.

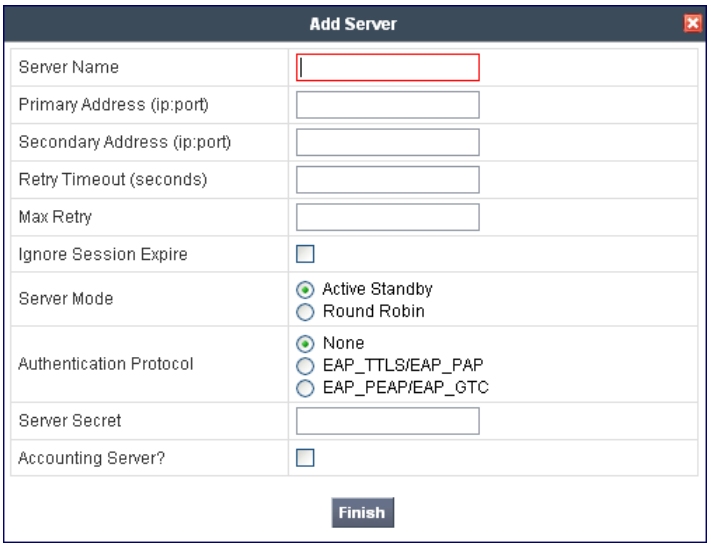


Figure 6-53. Add RADIUS Server Pop-up Window.

Table 6-3. Add RADIUS Server Pop-up Window Field Descriptions.

Field	Description
Server Name	A descriptive name used to identify this RADIUS server.
Primary Address (ip:port)	The IP address and port number of the server designated as the primary RADIUS server.
Secondary Address (ip:port)	The IP address and port number of the server designated as the primary RADIUS server.
Retry Timeout (seconds)	The maximum amount of time (in milliseconds) allowed for a successful authentication to be completed. If no successful authentication is completed within this amount of time, the connection is automatically terminated and an incident is generated.
Max Retry	The maximum number of times a user can attempt to authenticate before the connection is terminated.

Field	Description
Ignore Session Expire	Checkbox used to indicate whether or not the RADIUS session will terminate upon receipt of the SESSION EXPIRE message. Checking this box (☑) will cause the E-SBC to maintain the current session upon receipt of the SESSION EXPIRE message. Leaving the box blank (☐) will cause the E-SBC to terminate the current RADIUS session upon receipt of the SESSION EXPIRE message.
Server Mode	The method the E-SBC security device will use to select which RADIUS server it will choose to authenticate a user. Two selections are currently supported: **Active Standby** and **Round Robin**.
Authentication Protocol	The authentication protocol to be used for RADIUS authentication. Available options are: **None**, **EAP_TTLS/EAP_PAP**, and **EAP_PEAP/EAP_GTC**.
Server Secret	The shared secret maintained between the E-SBC security device and the active RADIUS server against which communications between the two will be encrypted.
Accounting Server	Checkbox indicating whether or not this RADIUS server is also to be designated as an Accounting Server, able to receive CDRs. Checking this box (☑) indicates this RADIUS server is also an Accounting Server and can receive CDRs. Leaving the box blank (☐) indicates this RADIUS server is ***not*** also an Accounting Server and will ***not*** receive CDRs.

6. Select **Finish.**
   The new RADIUS server is displayed in the Content Area (Figure 6-54).

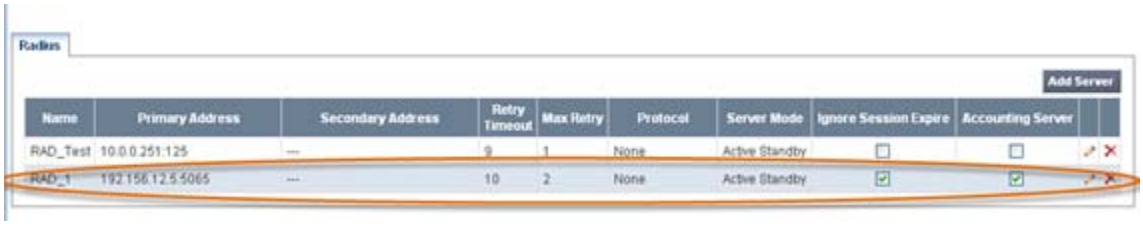


Figure 6-54. Updated RADIUS Tab Display.

Editing an Existing RADIUS Server Profile

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **RADIUS** (authentication) function of the **Global Parameters** feature from the Task Pane (Figure 6-51).
   The **Radius** screen is displayed (Figure 6-52).
3. Select the **Edit** icon corresponding to the server profile you want to edit.
   The **Edit RADIUS Server** pop-up window is displayed (Figure 6-55).

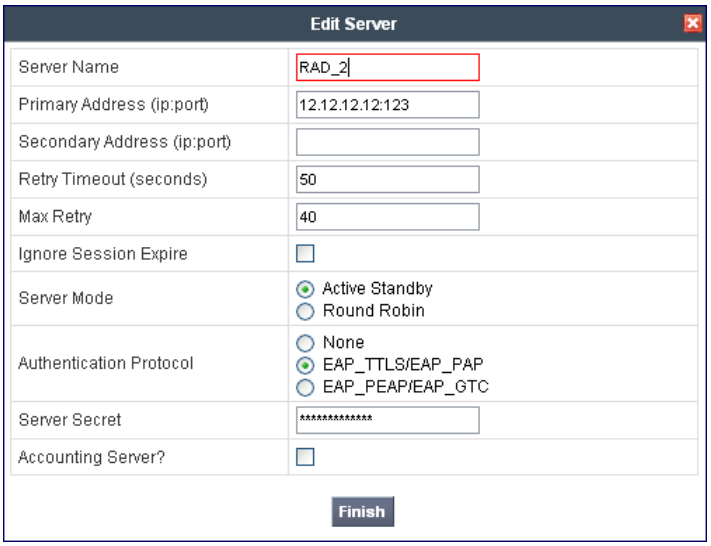


Figure 6-55. Edit RADIUS Server Pop-up Window.

4. Make your changes to the existing fields, referring back to Table 6-3 if necessary.
5. Select **Finish.**
   The RADIUS server configuration is updated and saved.

Deleting an Existing RADIUS Server Profile

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **RADIUS** (authentication) function of the **Global Parameters** feature from the Task Pane.
   The **Radius** screen is displayed.
3. Select the **Delete** icon corresponding to the server profile you want to delete.
   A confirmation pop-up window similar to that shown in Figure 6-56 will be displayed.

Figure 6-56. Delete Confirmation Pop-up Window.

6. Select **OK.**
   The selected RADIUS server configuration is deleted and the **RADIUS** tab display is updated (Figure 6-57).

Figure 6-57. Updated RADIUS Server Tab Display.

Signaling Forking Overview

The Signaling Forking feature allows the E-SBC device to bifurcate signaling packets according to a designated Signaling Forking Profile (see description in this section). This solution addresses problems faced by call recorders deployed for quality assurance and compliance. The Signaling Forking feature enables, for security and compliance purposes, the monitoring and recording of calling behavior, call attempts, and other related user actions involving signaling.

The Signaling Forking Profile sets up conditions for sending a duplicate stream of signaling packets to a call recorder.

Note:	Without the E-SBC device, ports of all phones would need to be spanned to the signaling recorder. Spanning all ports becomes a tedious task. With the E-SBC device in the picture, the spanning of all ports is not required.

Adding a Signaling Forking Profile

Note:	Signaling Forking and Media Forking are two separate functions that must be configured separately. Configuring your site for Signaling Forking does not automatically configure it for Media Forking, and configuring your site for Media Forking does not automatically configure it for Signal Forking.

1. Login to the E-SBC control center as the Admin.
2. Select: **Device Specific Settings** > **Network Management** and then select the **Interface Configuration** tab to display the Interface Configuration screen, similar to the example shown below.

   In the Interface Configuration screen click on the **Toggle State** button to toggle the state to **Enable** the Interface that needs to fork signaling traffic.

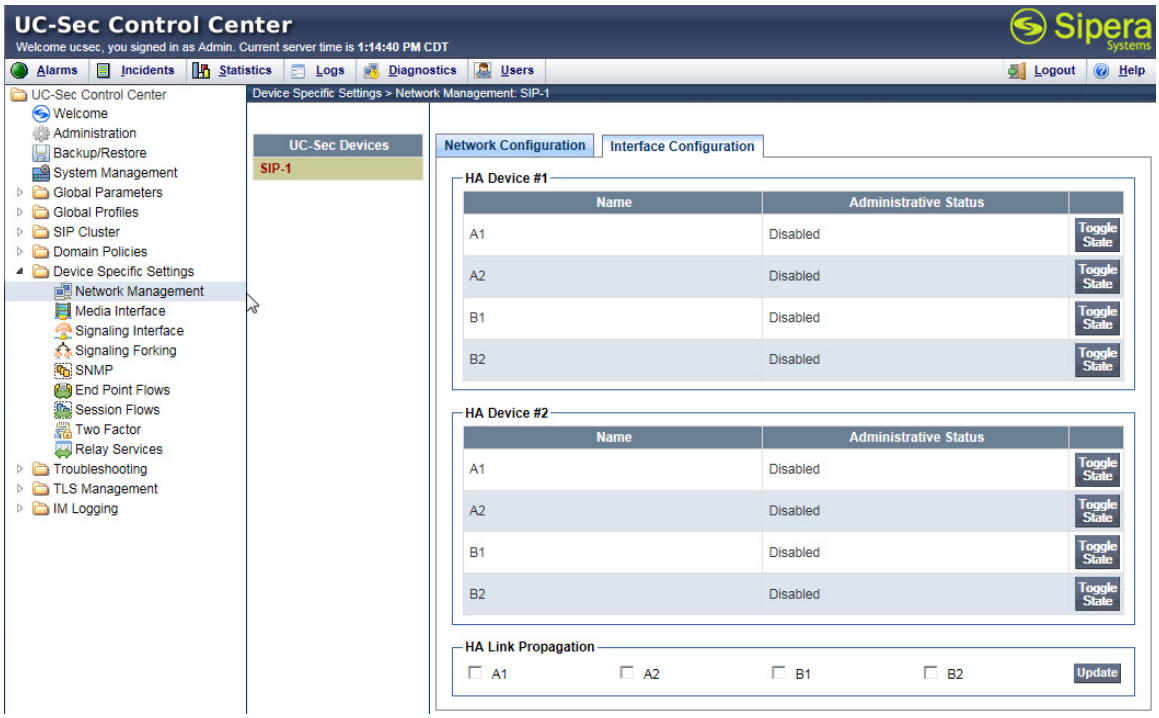


Figure 6-58 **Interface Configuration Screen**

As shown in Figure 6-59, select the **Signaling Forking** function under the **Device Specific Settings** from the task pane to display the Signaling Forking screen (Figure 6-60).

Figure 6-59 Selecting the Signaling Forking Function

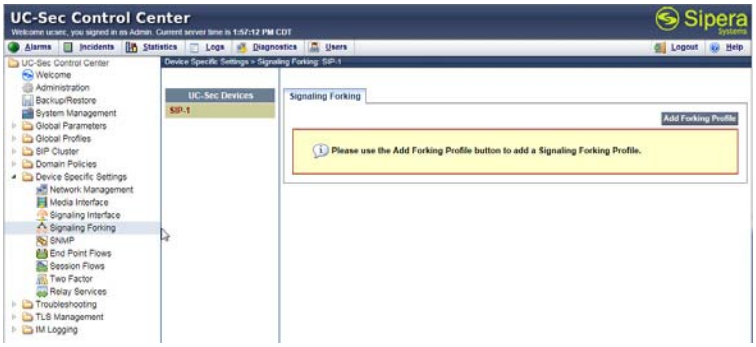


Figure 6-60 Selecting Signaling Forking Screen

3. Click the **Add Forking Profile** button in the upper-right portion of the Signaling Forking screen, to display the Add Forking Profile screen for configuring the appropriate settings as shown in the example in Figure 6-61 below.

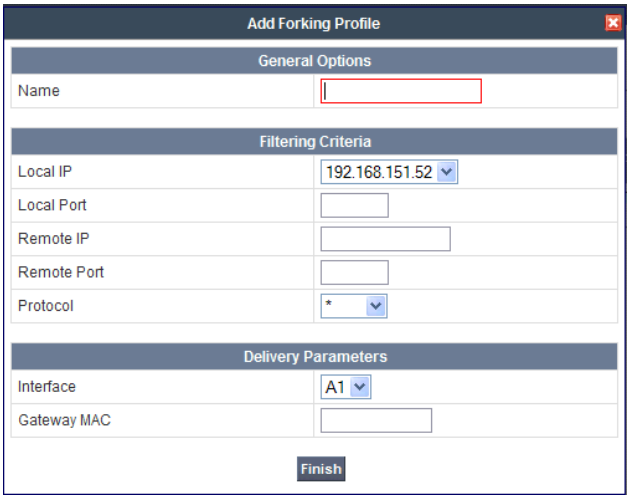


Figure 6-61 Add Forking Profile Screen

4. Make all of the appropriate selections and entries, which are listed and described in the table below, and then click **Finish** to display a Signaling Forking Profile Information screen similar to the example shown in Figure 6-62.

Table 6-4 Add Forking Profile Screen Field Descriptions.

Field	Description
Name	Signaling Forking Profile Name
Local IP	Select which signaling Interface IP signaling traffic needs to be mirrored
Local Port	Configure the signaling traffic local port information on which E-SBC handles signaling traffic
Remote IP	Configure the remote client/server IP from/to which signaling traffic needs to mirrored
Remote Port	Configure the signaling traffic Remote port information from/to which E-SBC handles signaling traffic
Transport	Configure the signaling traffic transport.
Interface	Select the Local Interface which is used for Spanning the Signaling Traffic
Gateway MAC Addresses	Enter the correct Destination MAC

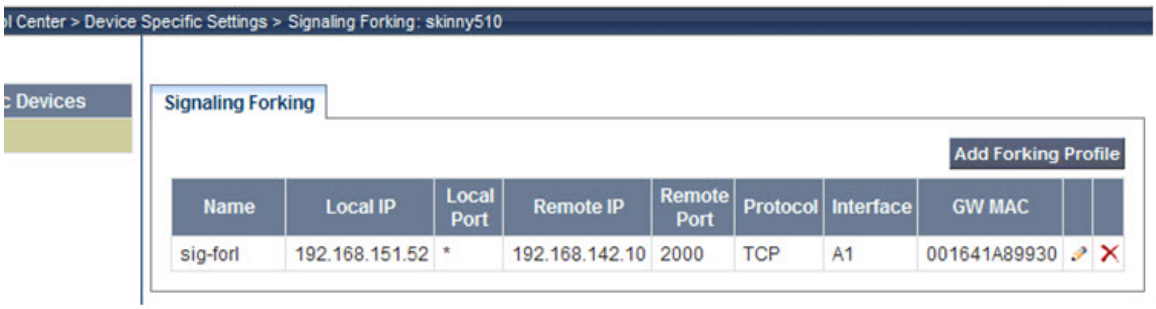


Figure 6-62 Signaling Forking Profile Information Screen

SNMP Settings

Provisioning SNMP parameters (v1/v2 and v3) is essentially comprised of granting certain users access to the **SNMP** information. Use the following procedure to create the access accounts.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **SNMP Settings** function of the **Global Parameters** feature from the Task Pane. The **SNMP** screen is displayed, which defaults to showing the contents of the **SNMP v1/v2** tab (Figure 6-63). The Content Area contains two user-selectable tabs (**SNMP v1/v2** and **SNMP v3**) which provide access to global SNMP parameters.
3. Proceed to the section *Managing SNMP v1/v2 Access* to configure user access for **SNMP v1/v2** information. Proceed to *Managing SNMP v3 Access* to configure user access for **SNMP v3** information.

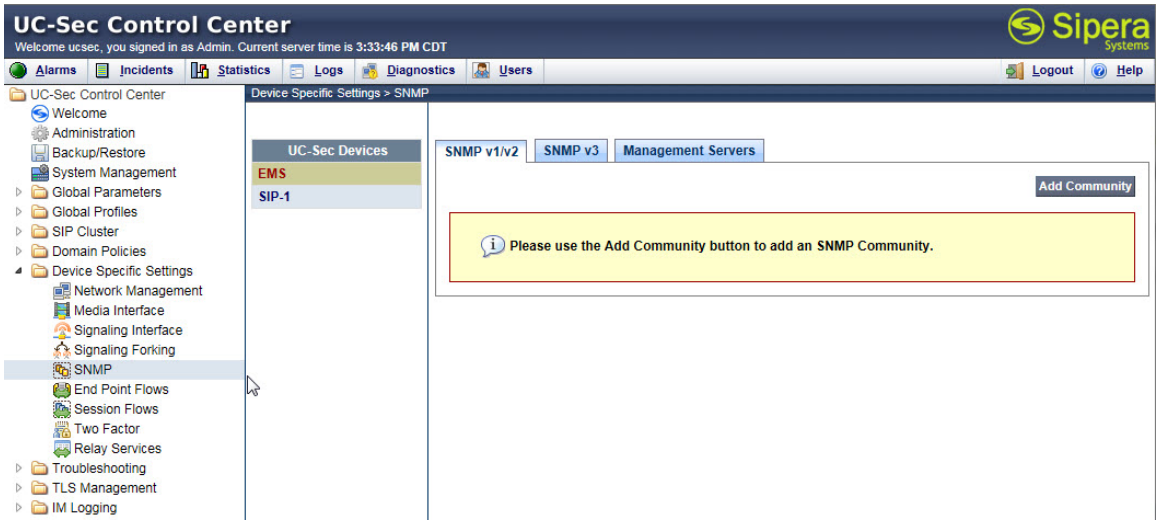


Figure 6-63. SNMP v1/v2 Tab Display.

Managing SNMP v1/v2 Access

Adding a New SNMP v1/v2 Community

Use the following procedure to configure user access for SNMP v1/v2 information.

1. In the Content Area, select the **SNMP v1/v2** tab.
2. Select **Add Community.**
   The **Add SNMP Community** pop-up window is displayed (Figure 6-64).

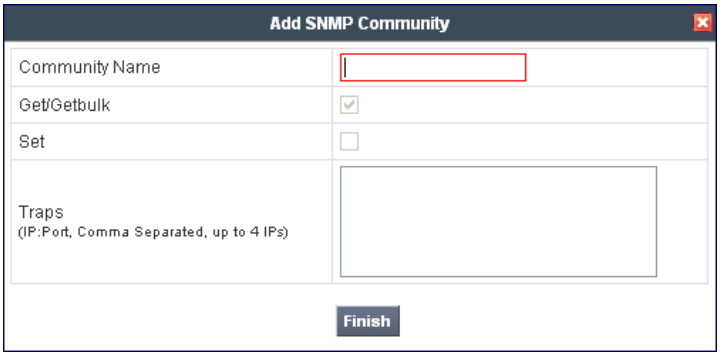


Figure 6-64. Add SNMP Community Pop-up Window.

3. In the **Community Name** field, enter the name of the community that will have access to the SNMP v1/v2 information.

Note:	The Get/Getbulk and Set checkboxes are grayed out and unavailable. In the Traps edit field, you can enter a list of up to four comma-separated SNMP trap receivers, each consisting of an IP address, colon, and port number in the format: IP_Address:Port_Number,IP_Address:Port_Number

This will be the SNMP user password for that account.

Note

The **Get/Getbulk** and **Set** fields are pre-set by Sipera Systems and are not user configurable.

4. Select **Save.**
   The new community will be displayed on the **SNMP v1/v2** tab (Figure 6-65).

Figure 6-65. Updated SNMP v1/v2 Display.

Editing an Existing SNMP v1/v2 Community

Use the following procedure to edit an existing SNMP v1/v2 community.

1. In the Content Area, select the **SNMP v1/v2** tab.
2. Select the **Edit** icon corresponding to the community you want to edit. The **Edit SNMP Community** pop-up window is displayed (Figure 6-66).

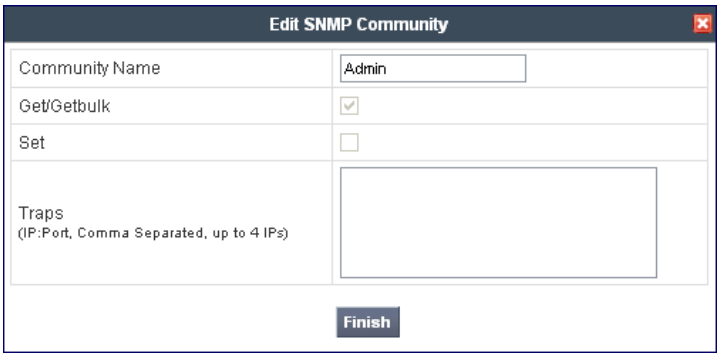


Figure 6-66. Edit SNMP Community Pop-up Window.

3. Edit the **Community Name** and **Traps** fields as desired and select **Save.** The new field values are saved and the SNMP v1/v2 tab display is updated (Figure 6-67).

Figure 6-67. Updated SNMP v1/v2 Tab Display.

Deleting an Existing SNMP v1/v2 Community

Use the following procedure to delete an existing SNMP v1/v2 community.

1. In the Content Area, select the **SNMP v1/v2** tab.
2. Select the **Delete** icon corresponding to the SNMP community you want to delete. A confirmation pop-up window is displayed asking you to confirm your selection (Figure 6-68).

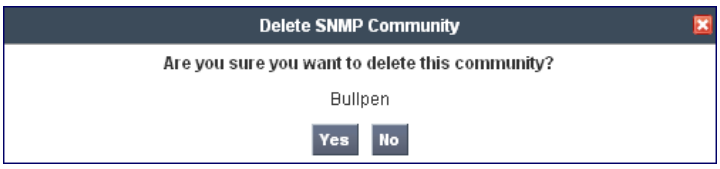


Figure 6-68. Delete Confirmation Pop-up Window.

3. Edit the **Community Name** field and select **Save.**

The **Community Name** is changed and the SNMP Setting screen is updated with the new information.

4. Select the **Yes**.
   The selected SNMP community is deleted and the **SNMP v1/v2** display is updated.

Managing SNMP v3 Access

Adding SNMP v3 Access

Use the following procedure to configure user access for SNMP v3 information.

1. In the Content Area, select the **SNMP v3** tab.
2. Select **Add User**.
   The **Add SNMP User** pop-up window is displayed (Figure 6-69).

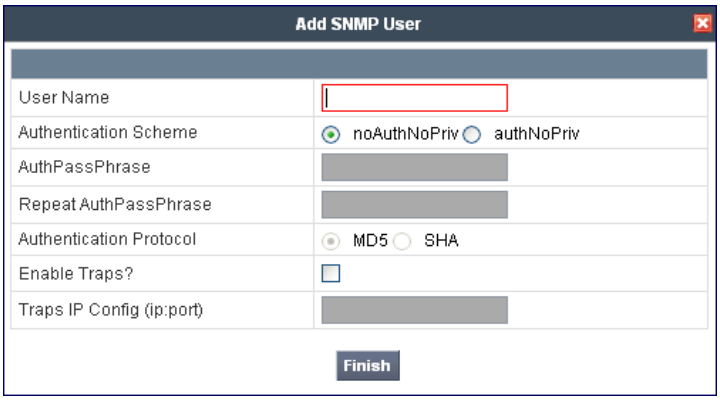


Figure 6-69. Add SNMP User Pop-up Window.

3. Referring to Table 6-5, enter the requested information into the appropriate fields in the Add SNMP User screen shown in Figure 6-69.

Table 6-5. SNMP v3 Configuration: Add User Pop-up Window Field Descriptions.

Field	Description
User Name	The assigned name/designation of the user being granted access to SNMP v3 data.
Authentication Scheme	The scheme to be used to authenticate the user prior to granting access to SNMP data. **noAuthNoPriv** — The user will not be authenticated and SNMP data will not be encrypted. **authNoPriv** — The user will be authenticated, but SNMP data will not be encrypted.
AuthPassPhrase	The user password for authentication.
Repeat AuthPassPhrase	The **AuthPassPhrase** entered again for verification.

Field	Description
Authentication Protocol	The type of authentication algorithm to be used to encrypt the user password (**AuthPassPhrase**). An authentication protocol: ensures data integrity, protects against data modification, provides data origin authentication, and protects against masquerade attacks. The types authentication protocol currently supported are: **MD5** Message Digest Algorithm. **SHA** Secure Hash Algorithm.
Enable Traps?	Enable the use of unsolicited SNMP messages to signal significant system events (alarms).
Traps IP Config (ip:port)	The IP address and port on which SNMP traps will be received.

4. Select **Finish** to create the new SNMP v3 user access and close the pop-up window or select **Cancel** to close the pop-up window without saving.
   The **SNMP v3** screen is updated to display the new SNMP v3 account (Figure 6-70).

Figure 6-70. Updated SNMP v3 Display.

Editing an Existing SNMP v3 Account

Use the following procedure to edit an existing SNMP v3 account.

1. In the Content Area, select the **SNMP v3** tab.
2. Select the **Edit** icon corresponding to the SNMP v3 account you want to edit.
   The **Edit SNMP User** pop-up window is displayed (Figure 6-71).

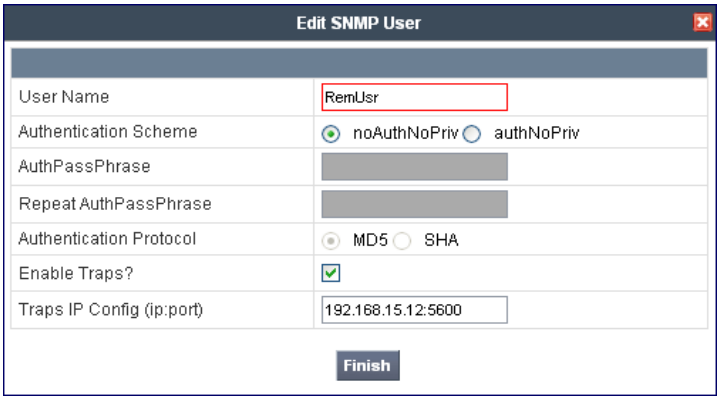


Figure 6-71. Edit SNMP User Pop-up Window.

3. Edit the desired fields according to the information contained in Table 6-5 and press **Finish** when done or **Cancel** to close the pop-up window without saving your changes.
   The **SNMP Sv3** display is updated to include your changes.

Deleting an Existing SNMP v3 Account

Use the following procedure to delete an existing SNMP v3 account.

1. In the Content Area, select the **SNMP v3** tab.
2. Select the **Delete** icon corresponding to the SNMP v3 account you want to delete.
   A confirmation pop-up window is displayed asking you to confirm your selection (Figure 6-72).

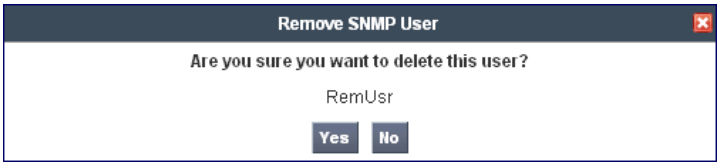


Figure 6-72. Delete Confirmation Pop-up Window.

3. Select **Yes**.
4. The selected SNMP v3 user is deleted and the **SNMP v3** tab display is updated.

Routing Profiles

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

Creating a New Routing Profile

Use the following procedure to create a new **Routing** profile.

Caution! A default Routing profile named **default** is provided by Sipera. Editing this profile is not recommended as improper configuration may cause subsequent calls to fail.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Routing** function from the **Global Profiles** feature from the Task Pane.

Existing routing profiles are displayed in the Application Pane. The routing rules comprising a selected routing profile are displayed in the Content Area of the E-SBC Control Center as shown in Figure 6-73.

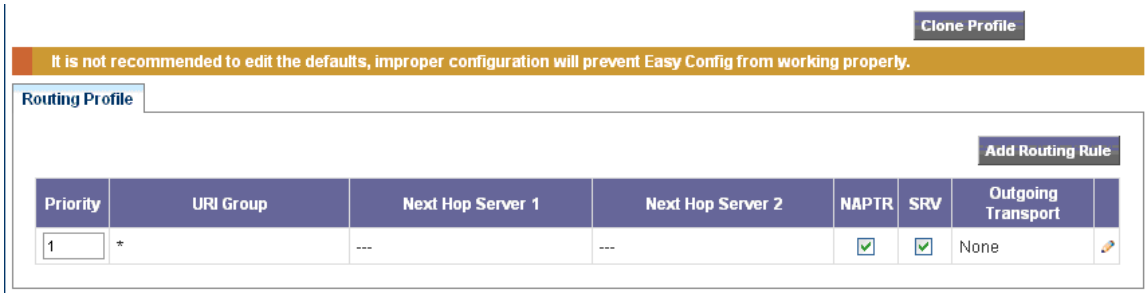


Figure 6-73. Routing Profile Screen.

3. Select **Add Profile** from the Applications Pane.
   The **Add Routing Profile** pop-up window is displayed (Figure 6-74).

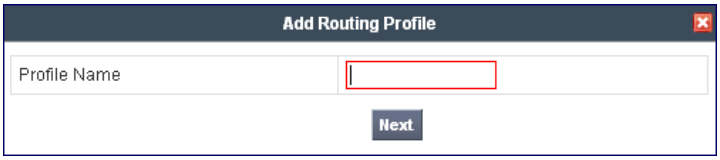


Figure 6-74. Add Routing Profile Pop-up Window.

4. Enter a distinctive name for the new **Routing Profile** and press **Next.**
   The **Add Routing Profile: Next Hop Routing** pop-up window is displayed (Figure 6-75).

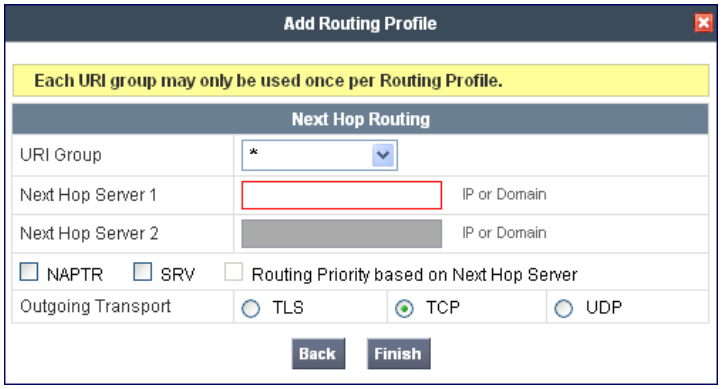


Figure 6-75. Add Routing Profile: Next Hop Routing Pop-up Window.

5. Enter the requested information into the appropriate fields.
   Table 6-6 describes each user-definable field displayed in the **Add Routing Profile: Next Hop Routing** pop-up window.

Table 6-6. Add Routing Profile: Next Hop Routing Pop-up Window Field Descriptions.

Field	Description
	Next Hop Routing
URI Group	A drop-down menu from which you select the URI Group to which this Next Hop Routing profile will be applied.
Next Hop Server 1	The IP address or domain of the primary Next Hop server.
Next Hop Server 2	The IP address or domain of the secondary Next Hop server.
NAPTR	A checkbox that activates (☑) or deactivates (☐) the **Naming Authority Pointer**.
SRV	A checkbox that activates (☑) or deactivates (☐) the **Service Record**.
Routing Priority based on Next Hop Server	A checkbox which indicates that routing priority will be determined by the next hop server (☑). or deactivates (☐) the **Service Record**.
Outgoing Transport	The protocol(s) used for transporting outgoing signaling packets. Available selections are: **TLS**, **TCP**, and **UDP**.

Note: The above options are given for finding the destination address.

The user can choose any one of three methods for finding the destination address: (1) SRV; (2) NAPTR; and (3) Routing priority based on next hop server.

6. Select **Finish.**
   The new **Routing** profile appears in the Application Pane (Figure 6-76).

Figure 6-76. Updated Routing Profile Screen.

Cloning an Existing Routing Profile

Use the following procedure to make an exact copy (clone) of an existing **Routing** profile.

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Routing** function from the **Global Profiles** feature from the Task Pane.
   Existing routing profiles are displayed in the Application Pane.
3. From the Applications Pane (Figure 6-77) select the routing profile you want to clone.
4. Select **Clone Profile.**
   The **Clone Profile** pop-up window is displayed (Figure 6-78).

Figure 6-77. Selecting an Existing Routing Profile.

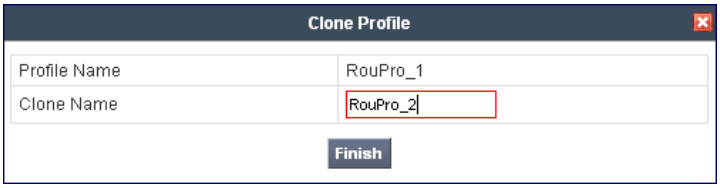


Figure 6-78. Clone Profile Pop-up Window.

5. Provide a name for the cloned **Routing** profile and press **Finish.** The **Routing** profile is cloned and renamed (Figure 6-79).

Figure 6-79. Updated Routing Profile Screen.

Editing an Existing Routing Profile

Editing a routing profile consists of managing the routing rules it contains. Routing rules within a profile can be added, edited, reordered, and deleted. These procedures are contained in the following sections.

Adding a Routing Rule

Use the following procedure to add a new routing rule to an existing routing profile.

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Routing** function from the **Global Profiles** feature from the Task Pane, as shown in the example below.
   Existing routing profiles are displayed in the Application Pane. The routing rules comprising a selected Routing profile are displayed in the Content Area of the E-SBC Control Center.

Figure 6-80. Selecting the Routing Function

3. From the Applications Pane select the routing profile to which you want to add a new routing rule
4. Select **Add Routing Rule**
   The **Add Routing Rule** pop-up window is displayed, which is similar to the Edit Routing Rule pop-up window shown in Figure 6-82.
5. In the **Add Routing Rule** pop-up window, enter the desired fields and press **Finish** when done or **Cancel** to close the pop-up window without saving your changes.
   The new routing rule is saved and the **Routing Profile** display is updated (Figure 6-81).

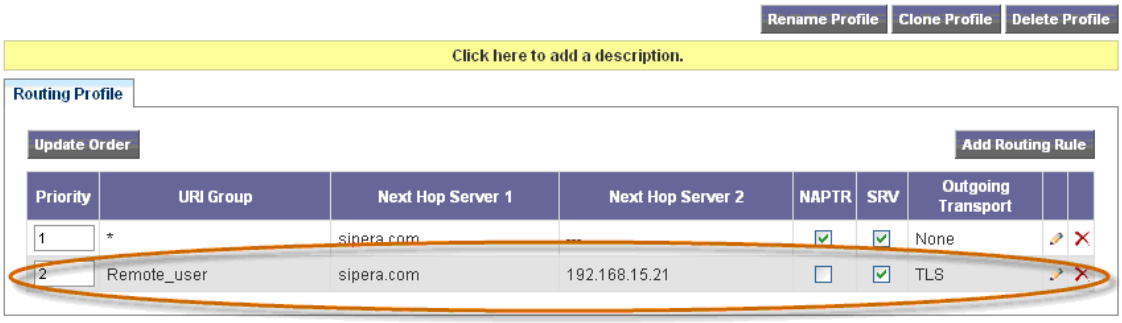


Figure 6-81. Updated Routing Profile Display.

Editing a Routing Rule

Use the following procedure to edit an existing routing rule.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Routing** function from the **Global Profiles** feature from the Task Pane.
   Existing routing profiles are displayed in the Application Pane. The routing rules comprising a selected Routing profile are displayed in the Content Area of the E-SBC Control Center.
3. From the Applications Pane select the routing profile to which you want to add a new routing rule.
4. Click the **Edit** icon corresponding to the routing rule you want to edit.
   The **Edit Routing Rule** pop-up window is displayed (Figure 6-82).

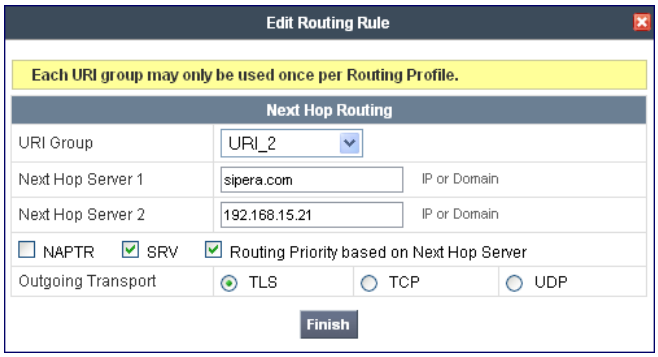


Figure 6-82. Edit Routing Rule Pop-up Window.

5. Edit the desired fields and press **Finish** when done or **Cancel** to close the pop-up window without saving your changes.
   Your changes are saved and the **Routing Profile** display is updated (Figure 6-81).

Deleting a Routing Rule

Use the following procedure to delete an existing routing rule.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Routing** function from the **Global Profiles** feature from the Task Pane.

Existing routing profiles are displayed in the Application Pane. The routing rules comprising a selected Routing profile are displayed in the Content Area of the E-SBC Control Center.

3. From the Applications Pane select the routing profile from which you want to delete a routing rule.
4. Click the **Delete** icon corresponding to the routing rule you want to delete. The **Delete Confirmation** pop-up window is displayed (Figure 6-83).
5. Click **OK**. The routing rule is deleted and the **Routing Profile** display is updated.

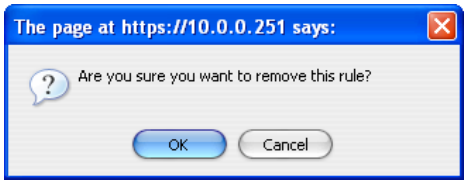


Figure 6-83. Delete Confirmation Pop-up Window.

Reordering Routing Rule Precedence

Use the following procedure to reorder the precedence of the routing rules within a routing profile.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Routing** function from the **Global Profiles** feature from the Task Pane. Existing routing profiles are displayed in the Application Pane.
3. From the Applications Pane select the routing profile whose routing rules you want to reorder (Figure 6-84).
4. Change the number in the **Order** column to reflect the order or precedence which you want the routing rules to be executed (Figure 6-84).

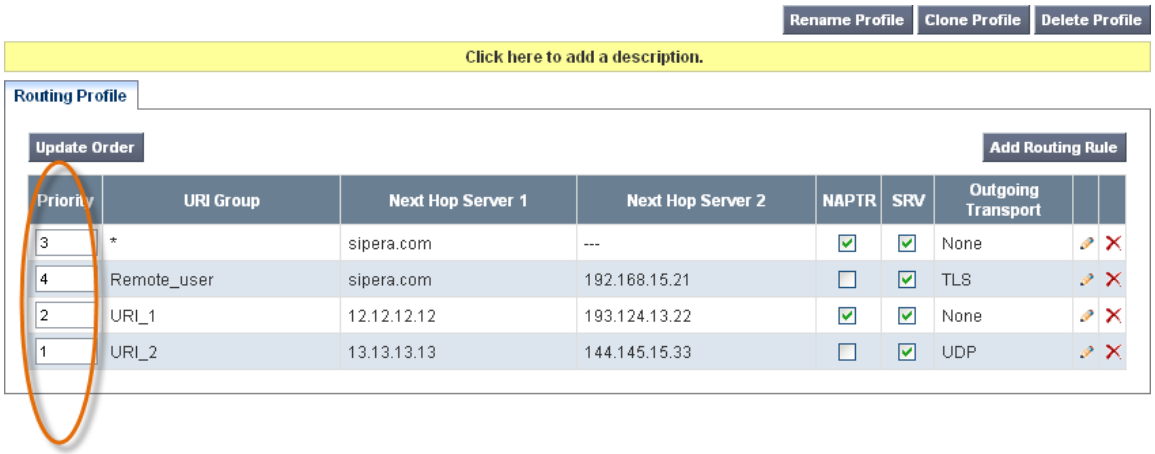


Figure 6-84. Selecting a New Order of Precedence for Existing Routing Rules.

5. Click the **Update Order**.
   The routing rules are redisplayed in the Content Area to reflect the new order of precedence (Figure 6-85).

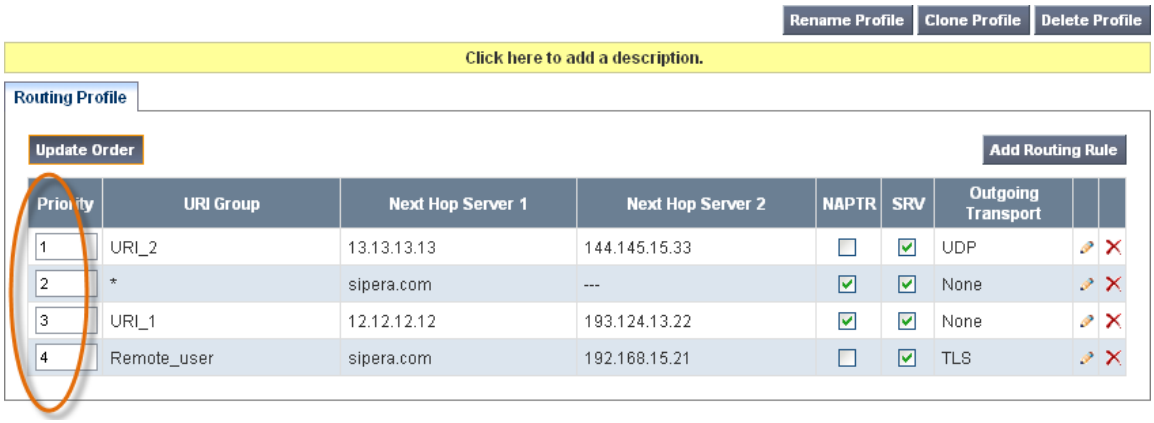


Figure 6-85. Reordered Routing Rules.

Renaming an Existing Routing Profile

Use the following procedure to rename an existing **Routing** profile.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Routing** function from the **Global Parameters** feature from the Task Pane
   Existing routing profiles are displayed in the Application Pane.
3. From the Applications Pane select the **Routing** profile you want to rename (Figure 6-86).

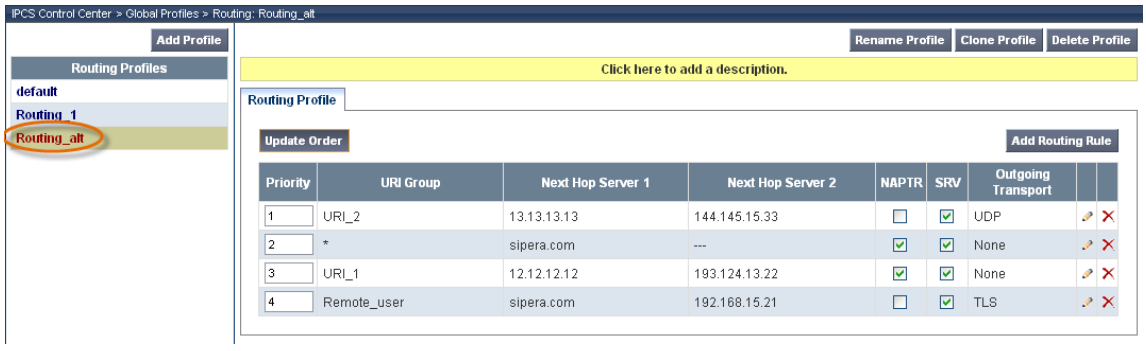


Figure 6-86. Selecting a Routing Profile.

4. Select **Rename Profile**.
   The **Rename Profile** pop-up window is displayed (Figure 6-87).

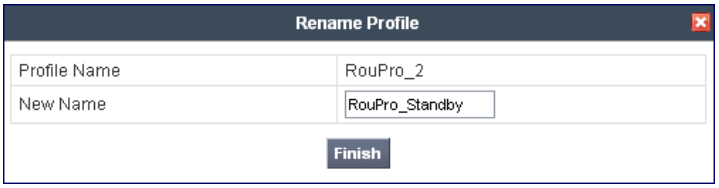


Figure 6-87. Rename Profile Pop-up Window.

5. Enter a new name for the routing profile and press **Finish**.
   The selected routing profile is renamed and the **Routing Profile** screen is updated and redisplayed.

Deleting an Existing Routing Profile

Use the following procedure to delete an existing **Routing** profile.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Routing** function from the **Global Profiles** feature from the Task Pane (Figure 6-88).
   Existing routing profiles are displayed in the Application Pane.

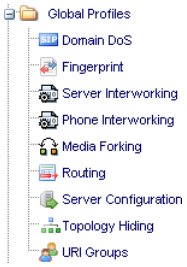


Figure 6-88. Selecting the Routing Function

3. From the Applications Pane select the **Routing** profile you want to delete (Figure 6-86).
4. Select **Delete Profile**.
   The **Delete Confirmation** pop-up window is displayed (Figure 6-89).

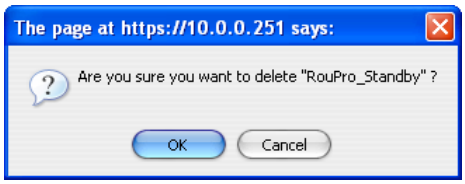


Figure 6-89. Delete Confirmation Pop-up Window.

5. Select **OK**.
   The routing profile is deleted and the **Routing Profile** screen updated and redisplayed.

Managing Syslog Parameters

This section provides a procedure for managing **syslog** parameters.
Syslog is a standard for forwarding log messages in an IP network. The term "syslog" is often used for both the actual syslog protocol, as well as the application or library sending syslog messages.

Syslog is a client/server protocol: the syslog sender sends a small (less than 1KB) textual message to the syslog receiver. The receiver is commonly called "syslogd", "syslog daemon" or "syslog server". Syslog messages can be sent via UDP and/or TCP. The data is sent in cleartext; although not part of the syslog protocol itself, an SSL wrapper can be used to provide for a layer of encryption through SSL/TLS.

Syslog is typically used for computer system management and security auditing. While it has a number of shortcomings, syslog is supported by a wide variety of devices and receivers across multiple platforms. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository.

Selecting Log Levels

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Syslog Management** function of the **Troubleshooting** feature from the Task Pane (Figure 6-90).
   The **Syslog Management** screen is displayed, defaulting to the **Log Level** tab view (Figure 6-91).

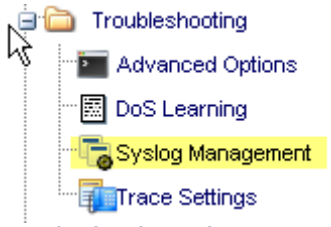


Figure 6-90. Selecting the Syslog Management Function

3. From the Application Pane, select the E-SBC security device for which you want to configure log level information.
4. Select the desired log collection facility from the pull-down menu for each class of logs (**Platform**, **Trace**, **Security**, and **Protocol**) and the types of information to be collected (Figure 6-92).
5. Select **Save**.
   The **Log Level** information is saved.

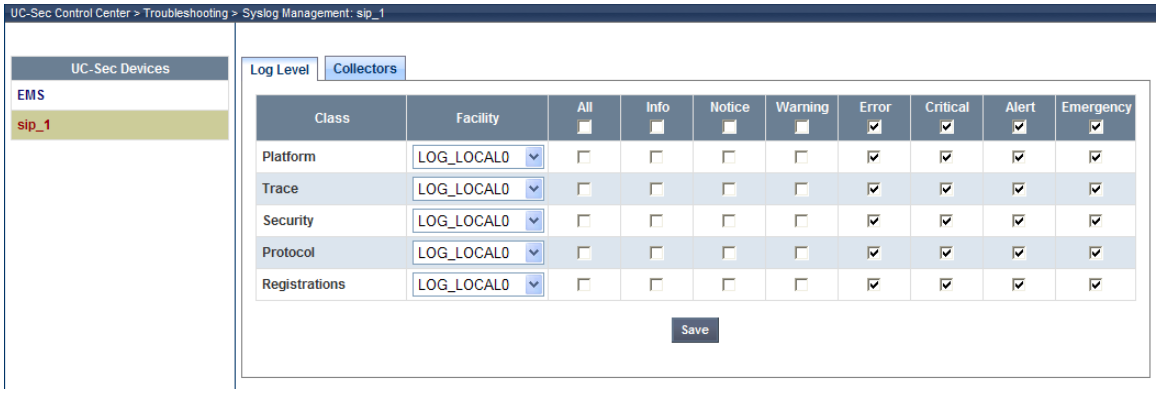


Figure 6-91. Syslog Management Display.

Figure 6-92. Selecting Log Collection Parameters.

Managing Device-Specific Settings

To complete the system configuration, two device-specific features must be defined: the **Signaling Interface** and the **Media Interface**. The procedures for managing these two features are provided in the following sections.

Managing Signaling Interface Parameters

Use the following procedures to view, add, edit, and delete signaling interface parameters.

Viewing an Existing Signaling Interface

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Signaling Interface** function of the **Device Specific Settings** feature from the Task Pane (Figure 6-93).
   The **Signaling Interface** screen is displayed (
   Figure 6-94).

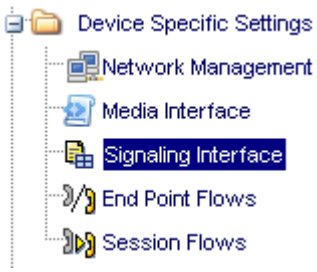


Figure 6-93. Selecting the Signaling Interface Function

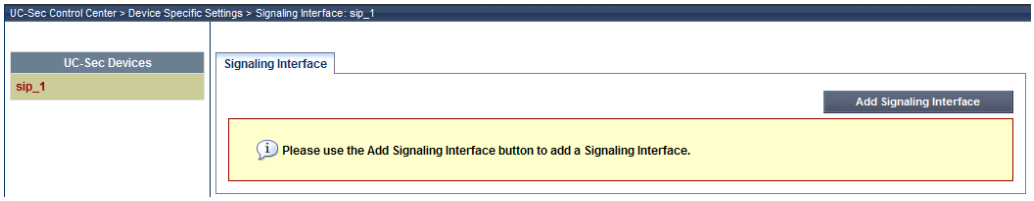


Figure 6-94. Signaling Interface Display.

3. From the Application Pane (Figure 6-95), select the E-SBC device (**sip_1** in the example) to display the **Signaling Interface** parameters (Figure 6-96) for that device.

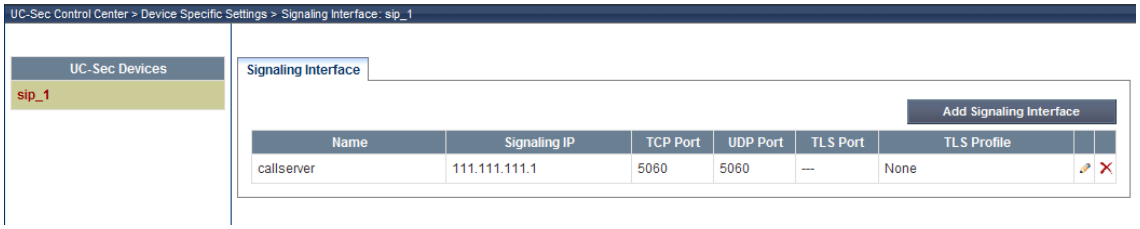


Figure 6-95. Selecting an E-SBC Device.

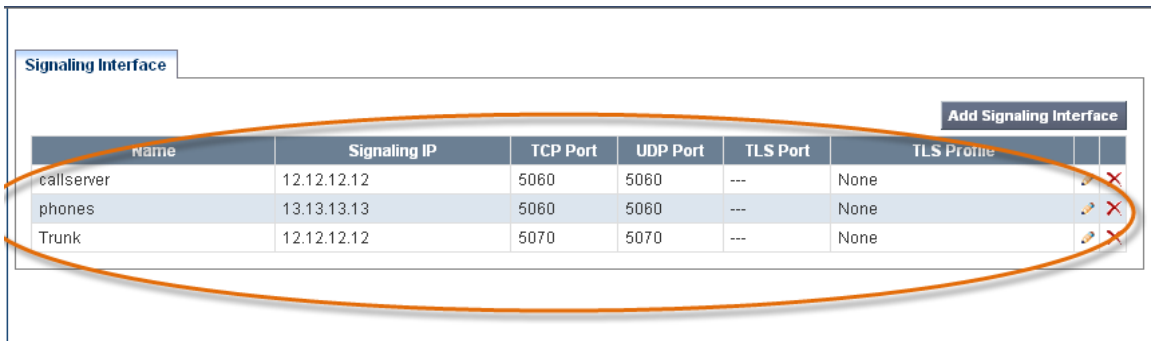


Figure 6-96. Signaling Interface Display.

Adding a New Signaling Interface

1. Select **Add Signaling Interface**.
   The **Add Signaling Interface** pop-up window is displayed (Figure 6-97).

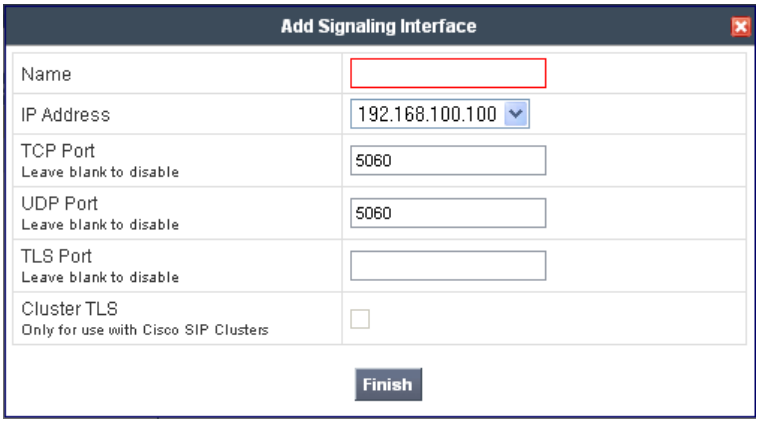


Figure 6-97. Add Signaling Interface Pop-up Window.

2. Enter the requested information into the appropriate fields.
   The table below describes each user-definable field displayed in the **Add Signaling Interface** pop-up window.

Table 6-7. Add Signaling Interface Pop-up Window Field Descriptions.

Field	Description
Name	The name used to refer to this profile.
IP Address	The IP address of the E-SBC security device used by SIP signaling messages traversing the network.
TCP Port	The port the E-SBC security device will 'listen' to for TCP packets.
UDP Port	The port the E-SBC security device will 'listen' to for UDP packets.
TLS Port	The port the E-SBC security device will 'listen' to for TLS packets.

Note: Ports configuration is the user's choice. However, it is important that if the user has a data firewall that the ports configured in the E-SBC be synchronized with the ports in the data firewall. If the user has no data firewall, no action is required.

3. Select **Finish.**
   The new configuration is displayed in the **Signaling Interface** display (Figure 6-98).

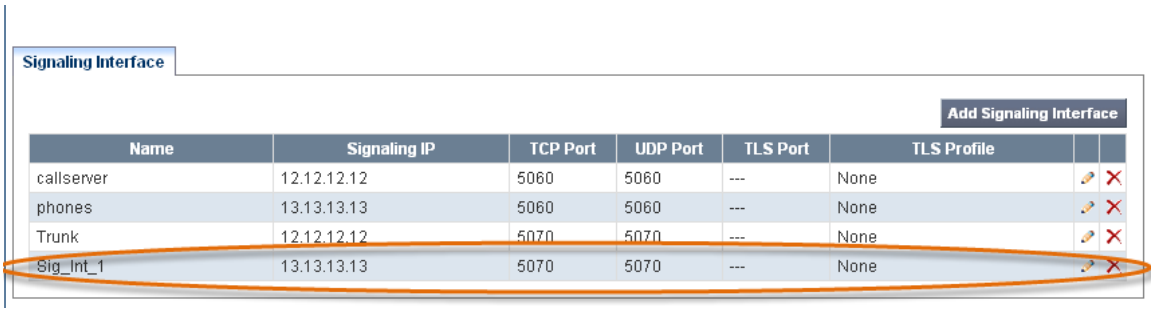


Figure 6-98. Updated Signaling Interface Display.

Editing an Existing Signaling Interface

1. From the **Signaling Interface** display, select the **Edit** icon corresponding to the **Signaling Interface** configuration you want to edit.
   The **Edit Signaling Interface** pop-up window is displayed (Figure 6-99).

Figure 6-99. Edit Signaling Interface Pop-up Window.

2. Edit the configuration as necessary and select **Finish**.
   The changes are saved and the Signaling Interface display is updated.

Deleting an Existing Signaling Interface

1. From the **Signaling Interface** display, select the **Delete** icon corresponding to the **Signaling Interface** configuration you want to delete.
   A **Delete Confirmation** pop-up window similar to that shown in Figure 6-100 is displayed.

Figure 6-100. Delete Confirmation Pop-up Window.

2. Click **OK**.
   The **Signaling Interface** configuration is deleted.

Managing Media Interface Parameters

Use the following procedures to view, add, edit, and delete media interface parameters.

Viewing an Existing Media Interface

1. Login to the E-SBC Control Center as the **Admin.**
2. Select the **Media Interface** function of the **Device Specific Settings** feature from the Task Pane (Figure 6-101).
   The **Media Interface** screen is displayed (Figure 6-102).

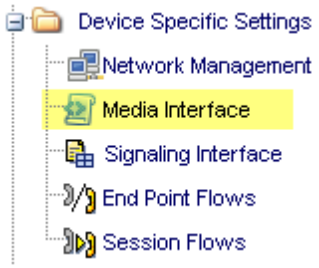


Figure 6-101. Selecting the Media Interface Function

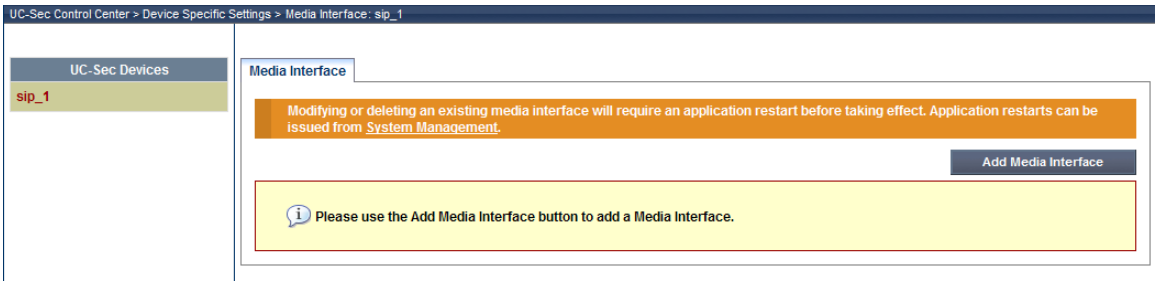


Figure 6-102. Media Interface Display.

3. From the Application Pane, select the E-SBC device for which you want to view the **Media Interface** parameters (Figure 6-103)
   The **Media Interface** parameters for that device are displayed (Figure 6-104).

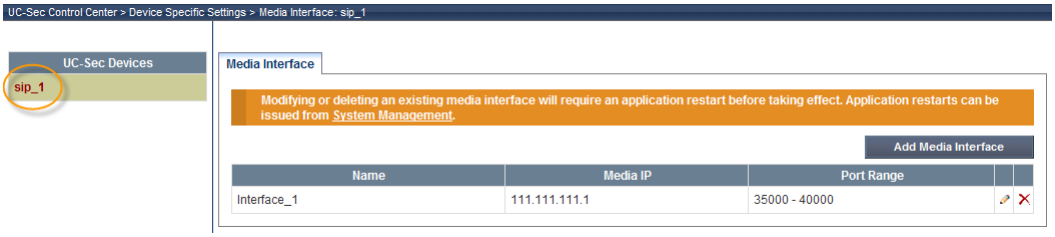


Figure 6-103. Selecting an E-SBC Device.

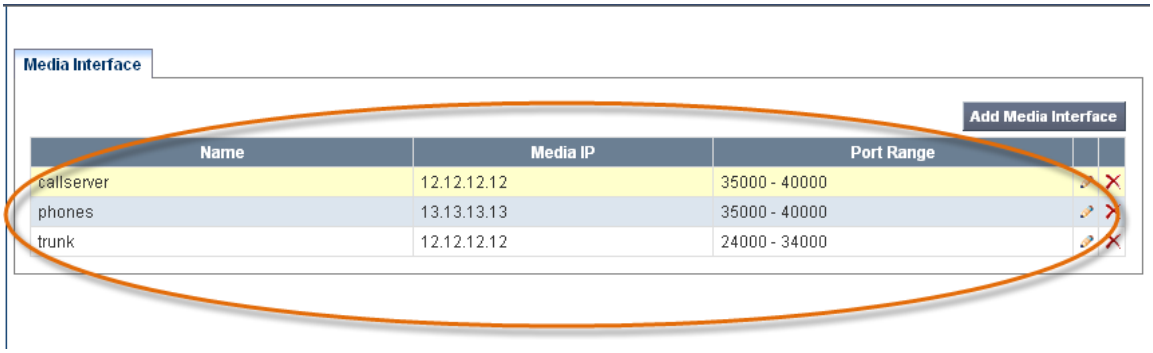


Figure 6-104. Media Interface Display.

Adding a New Media Interface

1. Select **Add Media Interface**.
   The **Add Media Interface** pop-up window is displayed (Figure 6-105).

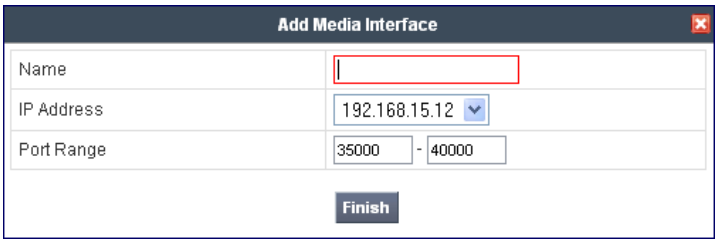


Figure 6-105. Add Media Interface Pop-up Window.

2. Enter the requested information into the appropriate fields.

   Table 6-8 describes each user-definable field displayed in the **Add Media Interface** pop-up window.

Table 6-8. Add Media Interface Pop-up Window Field Descriptions.

Field	Description
Name	The name used to refer to this profile.
IP Address	The IP address of the E-SBC security device to which media packets are sent.
Port Range	The range of ports on the E-SBC security device allocated for media traffic.

Note:	Ports configuration is the user's choice. However, it is important that if the user has a data firewall that the ports configured in the E-SBC be synchronized with the ports in the data firewall. If the user has no data firewall, no action is required.

3. Select **Finish.**
   The new configuration is displayed in the **Media Interface** display (Figure 6-106).

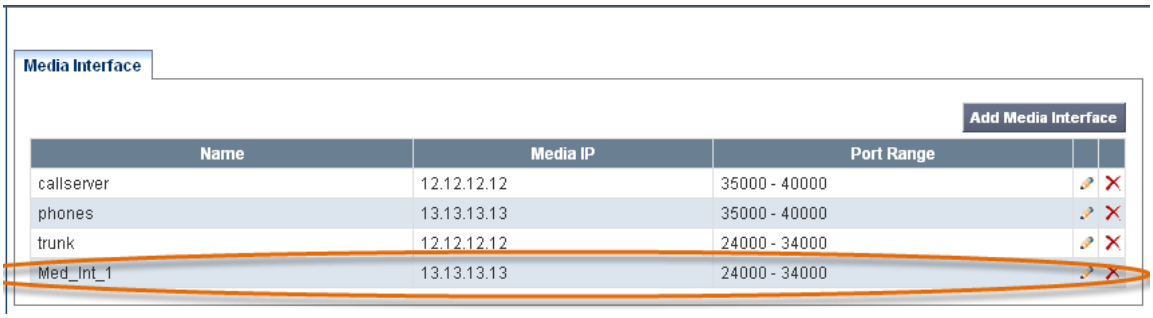


Figure 6-106. Updated Media Interface Display.

Editing an Existing Media Interface

1. From the **Media Interface** display, select the **Edit** icon corresponding to the **Media Interface** configuration you want to edit.
   The **Edit Media Interface** pop-up window is displayed (Figure 6-107).

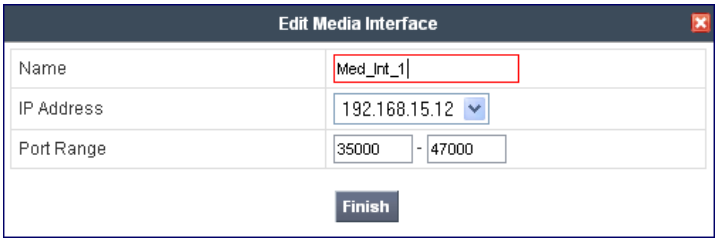


Figure 6-107. Edit Media Interface Pop-up Window.

2. Edit the configuration as necessary and select **Finish**.
   The changes are saved and the **Media Interface** display is updated.

Deleting an Existing Media Interface

1. From the **Media Interface** display, select the **Delete** icon corresponding to the **Media Interface** configuration you want to delete.
2. A **Delete Confirmation** pop-up window similar to that shown in Figure 6-108 is displayed.

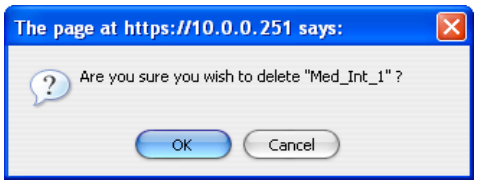


Figure 6-108. Delete Confirmation Pop-up Window.

3. Click **OK**.
   The **Media Interface** configuration is deleted.

Security Configuration 7

Overview

The E-SBC Control Center allows you to view various security-related features of E-SBC security products, such as:

- Configuring Denial-of-Service (DoS) Policies
  - DoS settings for SIP end-points
  - DoS settings for aggregate domains
  - DoS activity profiling per user-definable time-period

More on DoS Configuration can be found below.

- Protocol Scrubber Rules
- Topology Hiding

DoS Configurations

System Wide Single Endpoint DoS Configurations

- Found by clicking on DoS/DDoS under Global Parameters in the Task Pane
- Used to configure DoS settings for system wide SIP end-points

Domain DoS Configurations

- Found by clicking on Domain DoS under Global Profiles in the task pane
- Used to create a DoS profile for particular aggregate domains
- Once profile is created it is applied to aggregate domains using DoS Security Rules found under Domain Policies in the Task Pane

SIP Server DoS Configuration

- Found by clicking on Server Configuration under Global Profiles in the Task Pane
- Used to configure DoS security settings for particular SIP servers
- Guidance for DoS thresholds for SIP servers can be found by DoS learning
  - Found by clicking on DoS Learning under Troubleshooting in the Task Pane
  - Enables DoS activity profiling per user-definable time-period
  - Applied to DoS configuration for SIP Servers (see above).

For more on DoS Configurations, please see the sections in this chapter titled “DoS Security Features.”

DoS Security Features

The DoS Security feature of the E-SBC Control Center allows you to view and edit a wide variety of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attack response and control parameters that can then be applied either to individual SIP end-points or their parent domain. Additionally, the current release of the E-SBC supports DoS activity reporting for certain time periods. The procedures to perform these functions are contained in the following sections.

Note: The global Dos/DDos security parameter settings described next, are accessible by selecting: Global Parameters → DoS/DDoS

The threshold settings for each of DoS/DDoS attack protection security features defined here apply globally to all E-SBC Devices in the network. These settings only define the thresholds and not the activation of these security features.

The enabling/disabling of one or more of these DoS/DDoS attack protection security features is done uniquely for each individual E-SBC device within the network by selecting: Troubleshooting → Advanced Options
Then, one at a time, select each individual E-SBC device from the Application Pane and then select its Feature Control tab.

See the Chapter 6 section , "Enabling / Disabling E-SBC Security Features ," for more details.

DoS/DDoS

Viewing DoS/DDoS Settings

Use the following procedure to view DoS/DDoS settings that were previously configured using the Security Rules function of the Domain Policies feature.

Login to the E-SBC Control Center as the Admin.
Select the DoS/DDoS function of the Global Parameters feature from the Task Panel (Figure 7 - 1).

The DoS Settings screen will be displayed, containing four tabs (Single Source DoS, Phone DoS/DDoS, Stealth DoS/DDoS, and Call Waking) in the Content Area.

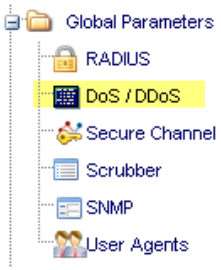


Figure 7 - 1. Selecting the DoS/DDoS Function

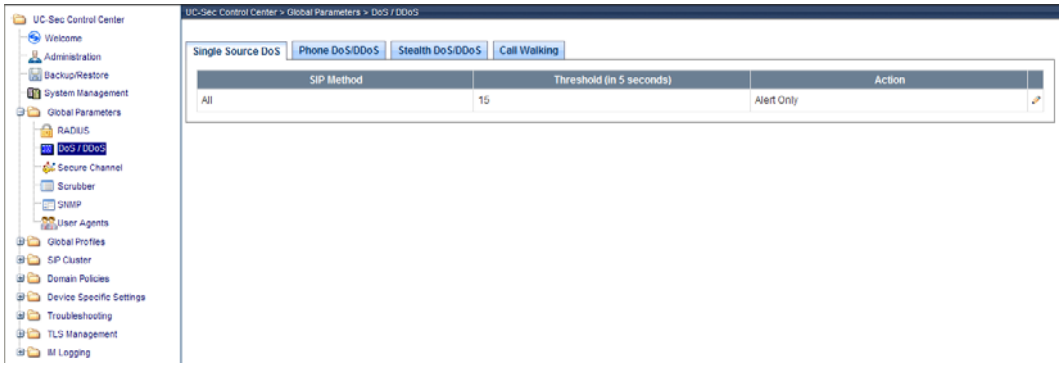


Figure 7 - 2. DoS **Settings Display.**

Table 7-1 contains a description of the DoS/DDoS attack types referenced by the tabs in the Content Area.

Table 7-1. DoS/DDoS Attack Type Descriptions.

DoS Attack Type	Attack Type Description
Single Source DoS	Any type of DoS attack that is directed against one or more enterprise end-points that originate from a single source (normally spoofed).
Phone DoS/DDoS	A type of DoS attack that is directed against a single enterprise end-point.
Stealth DoS/DDoS	A type of low-volume DoS attack that is directed against an end-point where the source of the call is constantly changed.
Call Walking	A type of DoS attack whereby serial calls originating from a single source (normally spoofed) are directed against a sequential group of end-points.

Select the tab containing the particular DoS/DDoS settings you want to view.

The selected settings will be displayed in the Content Area.

Editing DoS/DDoS Settings

Use the following procedure to edit DoS/DDoS settings.

Login to the E-SBC Control Center as the Admin.
Select the DoS/DDoS function of the Global Parameters feature from the Task Pane (Figure 7 - 1).

The DoS Settings screen will be displayed, containing four tabs (Single Source DoS, Phone DoS/DDoS, Stealth DoS/DDoS, and Call Waking) in the Content Area.
Select the tab containing the DoS/DDoS settings you want to edit.

The selected DoS/DDoS settings will be displayed in the Content Area.
Click the Edit icon corresponding to the specific DoS/DDoS settings you want to edit.

An Edit Response pop-up window similar to the one shown in Figure 7-3 for Call Walking will be displayed.

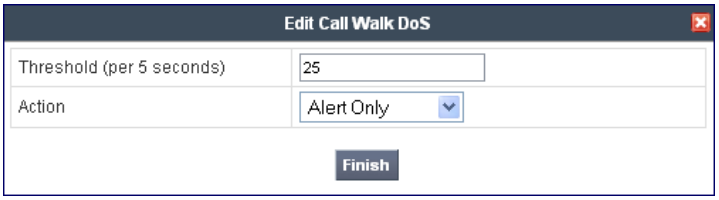


Figure 7-3. Edit Call Walk DoS Pop-up Window.

Edit the fields as desired and click Finish to save your changes or Cancel to return the fields to their previous values and close the window without saving.

Domain DoS Profiles

The Domain DoS profiles allow you to rate limit a number of SIP-specific services to ensure the availability of VoIP network resources. Domain DoS profiles can be viewed, added, cloned, edited, and deleted. The procedures to perform these functions are described below.

Viewing an Existing Domain DoS Profile

Use the following procedure to view an existing Domain DoS profile.

Login to the E-SBC Control Center as the Admin.
Select the Domain DoS/DDoS function of the Global Profiles feature from the Task Figure 7 - 1).

The Domain DoS screen is displayed, containing a list of available Domain DoS profiles in the Application Pane and their associated rate limited SIP services and corresponding thresholds in the Content Area (Figure 7-4).

From the Application Pane, select the Domain DoS profile you want to view (Figure 7-5).

The Rate Limit parameters corresponding to the selected Domain DoS profile will be displayed in the Content Area.

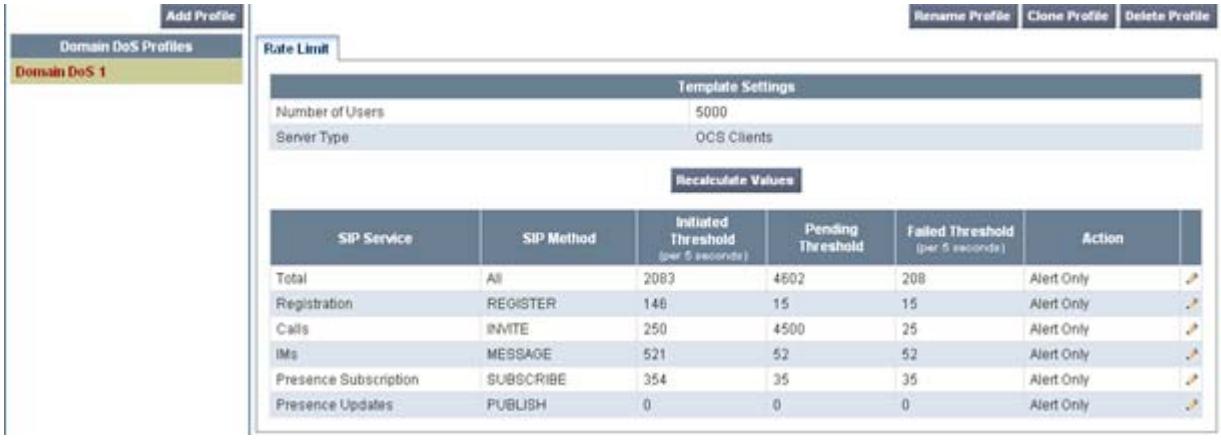


Figure 7-4. Domain DoS Display.

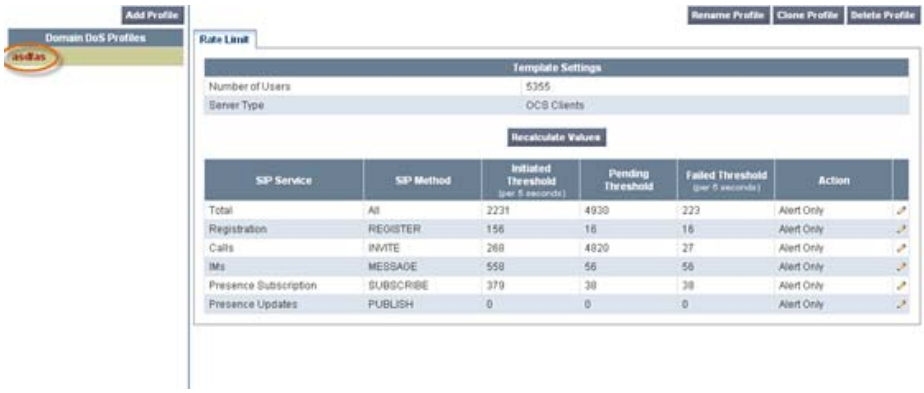


Figure 7-5. Selecting a Domain DoS Profile.

Adding a New Domain DoS Profile

Use the following procedure to view an existing Domain DoS profile.

Select Add Profile. The Add Domain DoS pop-up window is displayed (Figure 7-6).

Enter a name for the new profile and click Finish.

The new Domain DoS profile is saved and the Domain DoS screen redisplayed (Figure 7-8).

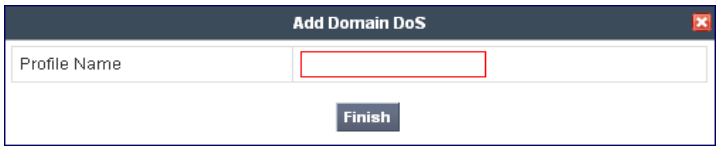


Figure 7-6. Add Domain DoS Pop-up Window.

Figure 7-7. Add Server Configuration Profile - Advanced Pop-up Window.

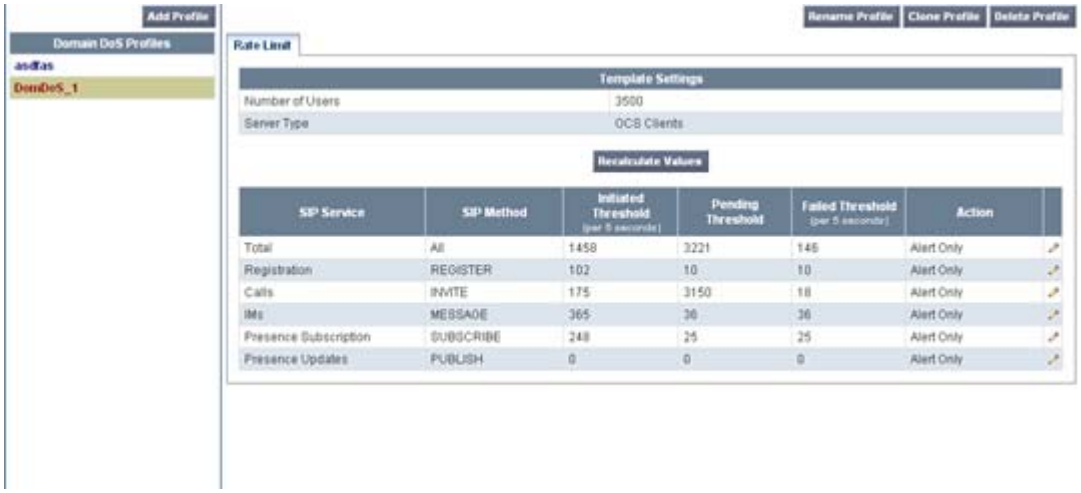


Figure 7-8. Updated Domain DoS Display.

Cloning an Existing Domain DoS Profile

Use the following procedure to make a copy (clone) of an existing Domain DoS profile.

From the Application Pane, select the Domain DoS profile you want to clone (Figure 7-5).
Select Clone Profile.

The Clone Domain DoS pop-up window is displayed (Figure 7-9).

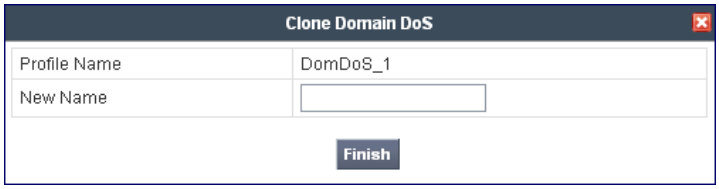


Figure 7-9. Clone Domain DoS Profile.

Enter a name for the cloned profile and click Finish.

The cloned Domain DoS profile is saved and the Domain DoS screen redisplayed (Figure 7-10).

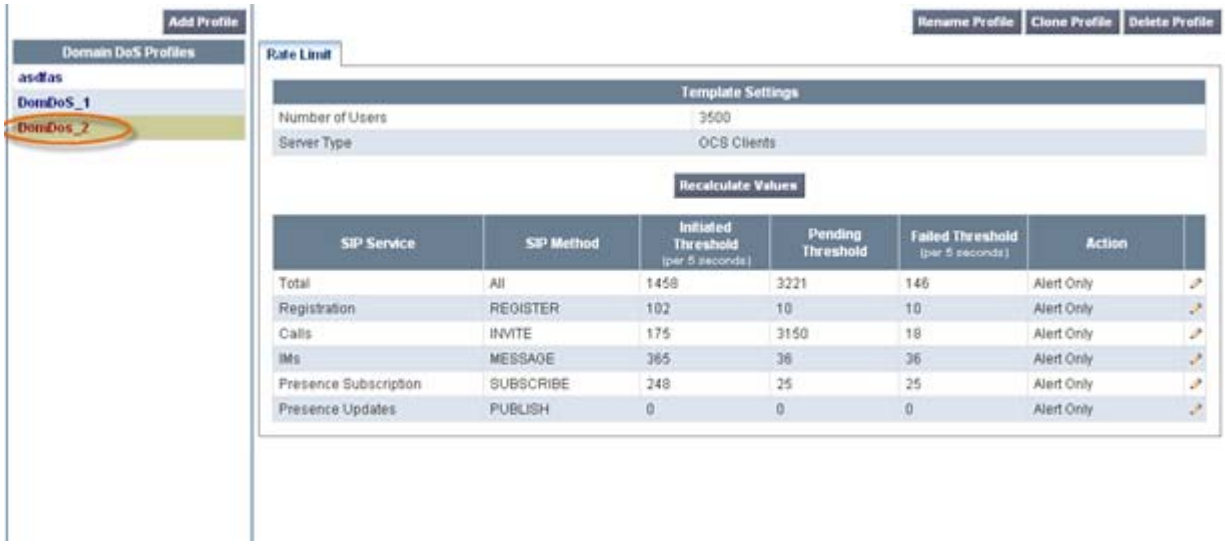


Figure 7-10. Updated Domain DoS Display.

Renaming an Existing Domain DoS Profile

Use the following procedure to rename an existing Domain DoS profile.

From the Application Pane, select the Domain DoS profile you want to rename (Figure 7-5).

Select Rename Profile.

The Rename Domain DoS pop-up window is displayed (Figure 7-11).

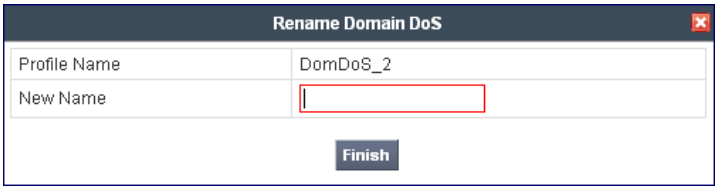


Figure 7-11. Rename Domain DoS Profile.

Enter a new name for the profile and click Finish.

The new name is saved and the Domain DoS screen redisplayed (Figure 7-12).

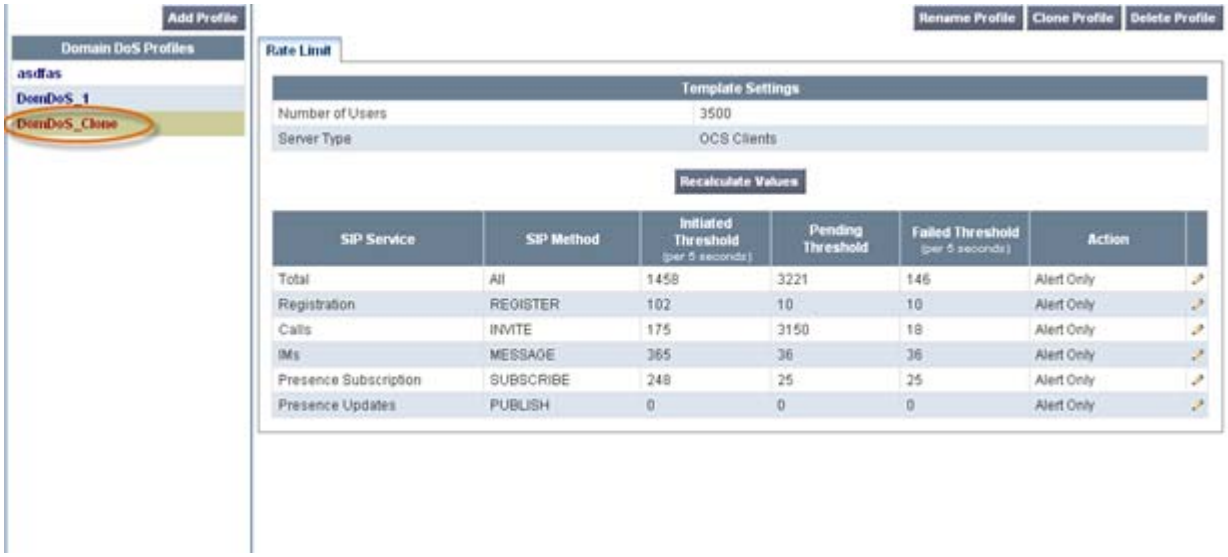


Figure 7-12. Updated Domain DoS Display.

Editing an Existing Domain DoS Profile

Use the following procedure to edit an existing Domain profile.

From the Application Pane, select the Domain DoS profile you want to edit (Figure 7-5).
Click the Edit icon corresponding to the SIP service or method you want to edit.

An Edit Domain DoS pop-up window similar to the one shown in Figure 7-13 will be displayed.

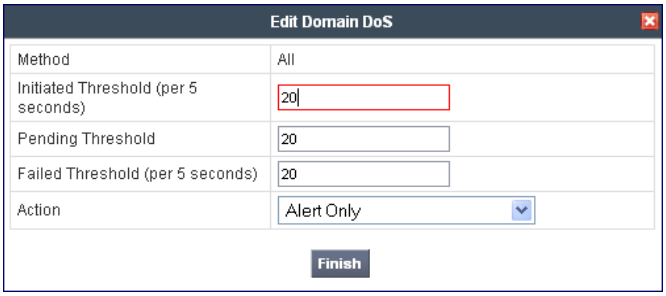


Figure 7-13. Edit Domain DoS Pop-up Window.

Edit the fields as desired.
Select Finish to save your changes or Cancel to return the fields to their previous values and close the window without saving.

Deleting an Existing Domain DoS Profile

Use the following procedure to delete an existing Domain DoS profile.

Note:	This procedure applies to DoS server profiles. Refer to the section titled "Editing the DoS Protection Tab," in Chapter 8 for information on creating and editing DoS server profiles.

From the Application Pane, select the Domain DoS profile you want to delete (Figure 7-5).
Select Delete Profile.

A confirmation pop-up window will be displayed similar to that shown in Figure 7-14 asking you to confirm your selection.

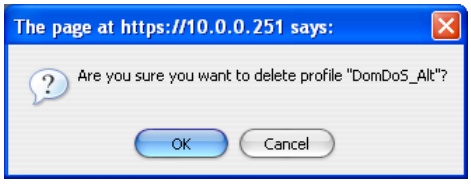


Figure 7-14. Delete Confirmation Pop-up Window.

Select OK.
The selected Domain DoS profile is deleted.

Setting DoS Learning Parameters

Use the following procedure define simple time-of-week and time-of-day parameters in which the EMS will 'learn' or gather, save, and report the historical traffic activity towards the server occurring at a particular E-SBC device deployed in the network.

Login to the E-SBC Control Center as the Admin.
Select the DoS Learning function of the Troubleshooting feature from the Task Pane

The Learned Info screen is displayed, containing a list of installed E-SBC devices in the Application Pane.
Select the E-SBC security device from the Application Pane whose DoS activity you want to learn (Figure 7-15).

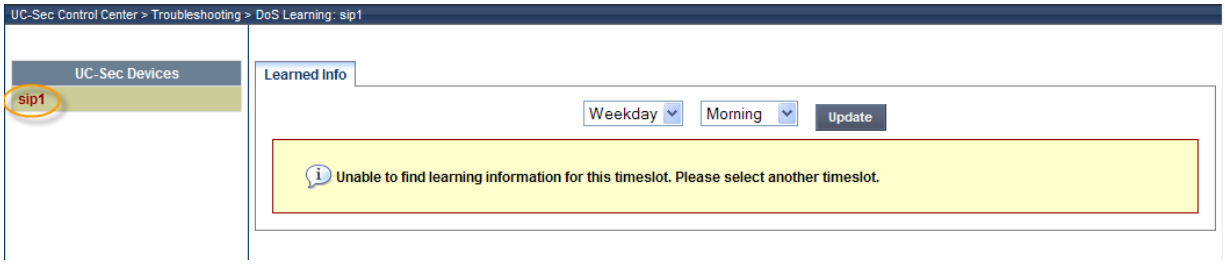


Figure 7-15. Selecting an E-SBC Device.

Using the pull-down menus on the Learned Info tab in the Content Area, select the time period for which you want to learn DoS activity (Figure 7-16).

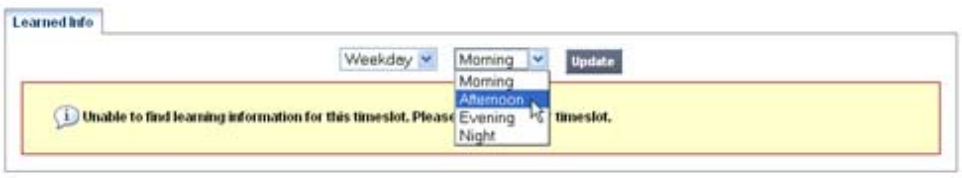


Figure 7-16. Selecting DoS Learning Time Parameters.

Select **Update**.

Any DoS activity detected for the specified time period will be displayed in the Content Area.

Protocol Scrubber

Protocol Scrubbing is an E-SBC feature that utilizes a highly sophisticated statistical mechanism to thoroughly check incoming SIP signaling messages for various types of protocol-specific events and anomalies. It verifies certain message characteristics such as proper message formatting, message sequence, field length, and content against updatable templates received from Sipera. Typically, messages which violate the security rules dictated by the scrubber templates will be dropped while those which violate syntax rules will be repaired (either re-written, truncate, rejected, or dropped, depending upon the processing rules imposed by the templates).

Note	Protocol Scrubbing rule templates are prepared by Sipera and can only be minimally edited by the user .

The Protocol Scrubbing feature for SIP allows you install a scrubber rules package, enable or disable the scrubber rules contained in the package, and delete the package from the system. In addition, you can view a list of all currently installed scrubber rules.

Note:	VIPER signatures are similar to Scrubber Packages, and are created by the VIPER team, and then packaged and released by the engineering team after testing. Refer to the section titled, “Security Rules” in Chapter 5 and the section titled, “Updating VIPER Signatures,” in Chapter 4.

Viewing Scrubber Rules

Login to the E-SBC Control Center as the Admin.
Select the Scrubber function of the Global Parameters feature from the Task Pane (**Figure 7-17**).

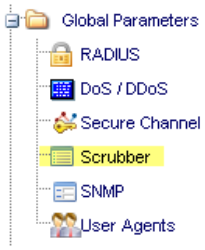


Figure 7-17. Selecting the Scrubber Function

The Scrubber screen is displayed, containing two user-selectable tabs in the Content Area: Packages and Rules (Figure 7-18).

Figure 7-18. Scrubber Display.

Select the Rules tab.

Any installed scrubber rules (templates) will be displayed in the Content Area.

Installing a Scrubber Rules Package

Click Install Package.

Select the Scrubber function of the Global Parameters feature from the Task Pane (Figure 7-17).

The Install Scrubber Package pop-up window is displayed (Figure 7-19).

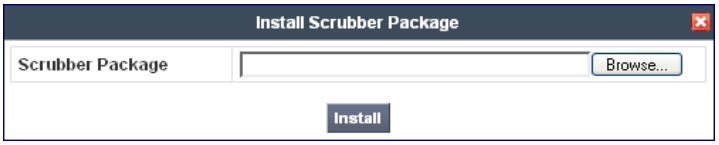


Figure 7-19. Install Scrubber Package Pop-up Window.

Enter a filename for the Scrubber Package to be installed or click Browse… to search your directory for a suitable Scrubber function of the Device Specific Settings feature from the Task Pane (Figure 7-17).

Click Install.

The selected Scrubber package is loaded, enabled, and listed in the Packages tab display.

Note:	The Scrubber must be enabled in the Security Rules of Domain Policies before it takes effect. Once the Scrubber is enabled there, a list of packages would be needed for the Security Rule. Refer to the section titled, “Security Rules” in Chapter 5.

Configuring Actions

After installing the Scrubber rules, actions can be configured by clicking on the Action button located on the right-hand side of the Rules tab screen

There are three actions allowed:

BLOCK — Drops the message

REJECT — Responds back to a request with a "400 Bad Request" response

DROP HEADER — Drops the header that the rule mismatched to

Enabling / Disabling an Installed Scrubber Rules Package

Note:	After installing a Scrubber Rules Package, the package must be enabled, as described in this section, before the rules package takes effect.

In the Content Area, click the Enable (or Disable) pushbutton corresponding to the scrubber package you want to enable/disable.

The selected scrubber package is enabled (or disabled).

Deleting an Existing Scrubber Rules Package

In the Content Area, click the Delete icon corresponding to the scrubber package you want to delete. A Delete Confirmation pop-up window similar to that sown in is displayed (Figure 7-20).

Click OK.

The selected Scrubber package is deleted.

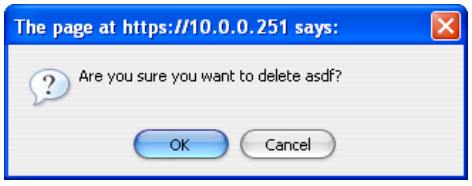


Figure 7-20. Delete Confirmation Pop-up Window.

Topology Hiding

Topology Hiding is an E-SBC security feature which allows you to change certain key SIP message parameters to 'hide' or 'mask' how your enterprise network may appear to an unauthorized or malicious user.

Creating a New Topology Hiding Profile

Use the following procedure to create a new Topology Hiding profile.

Login to the E-SBC Control Center as the Admin.
Select the Topology Hiding function from the Global Profiles feature from the Task Pane (Figure 7-21).

Existing Topology Hiding profiles are displayed in the Application Pane and their corresponding Topology Headers are displayed in the Content Area of the E-SBC Control Center as shown in Figure 7-22, which has the default profile selected.

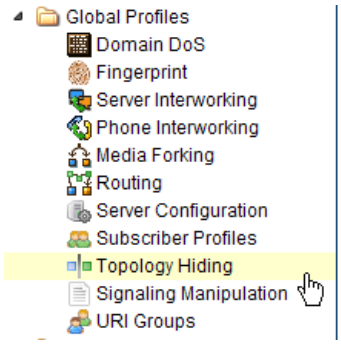


Figure 7-21. Selecting the Topology Hiding Function

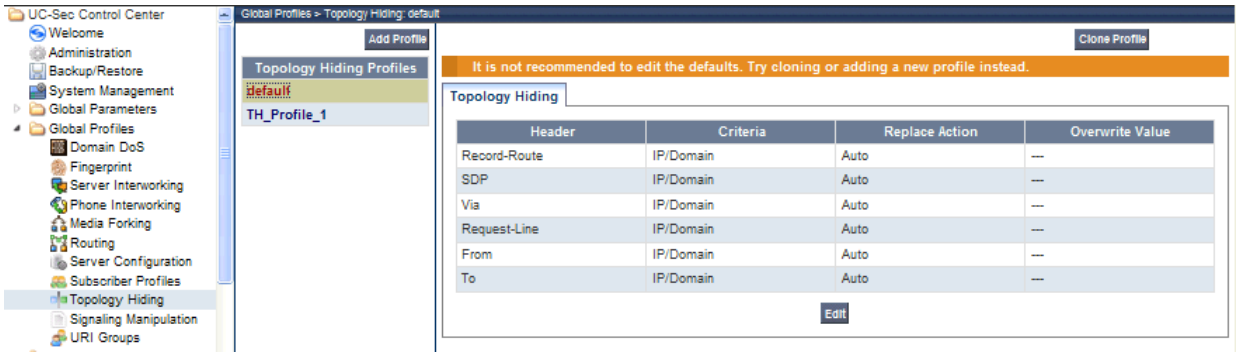


Figure 7-22. Topology Hiding Display.

From the Applications Pane, click Add Profile.
The first Topology Hiding Profile pop-up screen is displayed (Figure 7-23).

Enter a name for the new profile and click Next. The second Topology Hiding Profile screen is displayed (Figure 7-24).

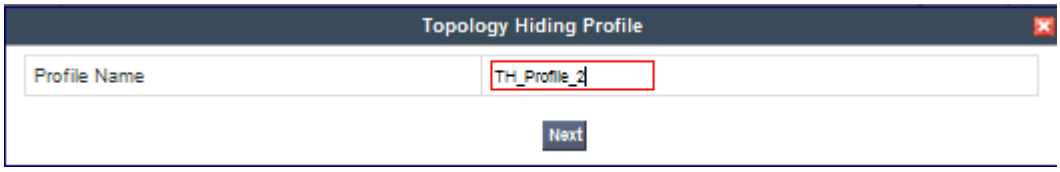


Figure 7-23. Topology Hiding Profile Screen 1

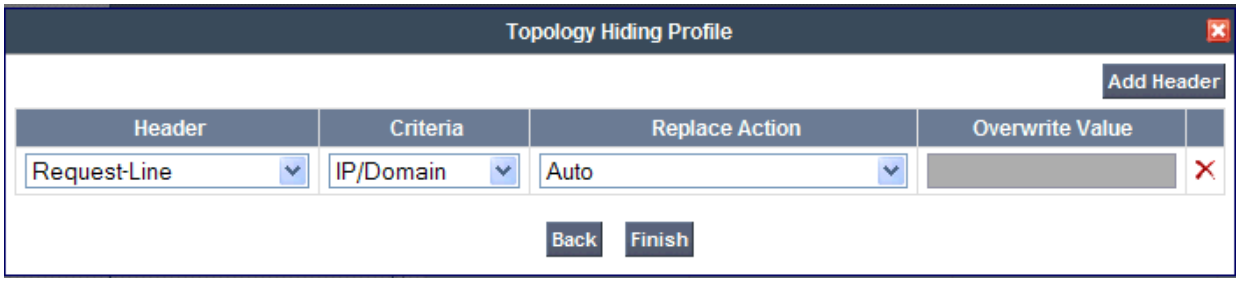


Figure 7-24. Topology Hiding Profile Screen 2

In the second Topology Hiding Profile screen (Figure 7-24), begin to select the chosen parameters by selecting the drop-down list of Header parameters to choose one of the parameters for the new profile as shown in Figure 7-25.

Figure 7-25. Topology Hiding Profile Header Parameters

In the second Topology Hiding Profile screen (Figure 7-24), next select the drop-down list of Criteria parameters to choose one of the parameters for the new profile as shown in Figure 7-26.

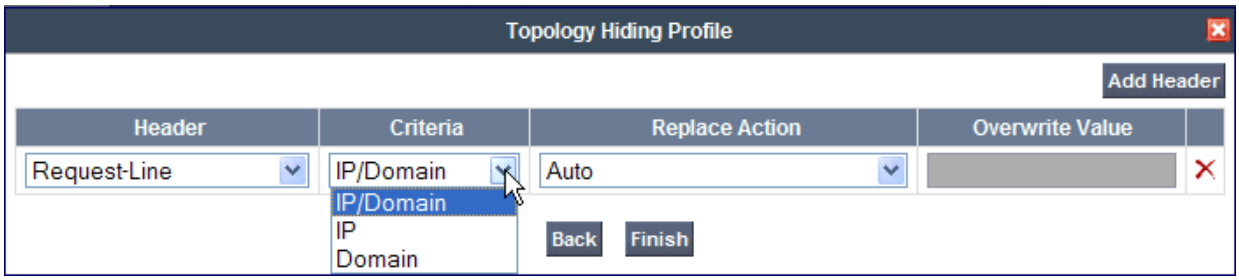


Figure 7-26. Topology Hiding Profile Screen 2 Criteria Parameters

In the second Topology Hiding Profile screen (Figure 7-24), next select the drop-down list of Replace Action parameters to choose one of the parameters for the new profile as shown in
Figure 7-27.

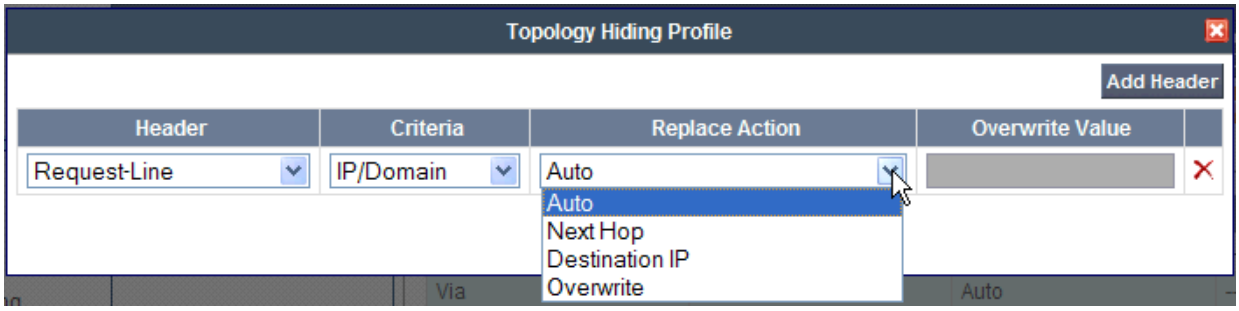


Figure 7-27. Topology Hiding Profile Screen 2 Replace Action

Note:	In the drop-down list in the Replace Action field, shown above, if you select the action, "Overwrite," the Overwrite Value field to the right will accept entry of a value (i.e., an IP address).

After selecting the appropriate values in the Topology Hiding Profile fields, select Finish to save, submit, exit, and redisplay the Topology Hiding Profile screen (Figure 7-28) showing the newly-created profile (TH_Profile_2 in the example).

This ends the procedure for creating a new Topology Hiding Profile.

Figure 7-28. Topology Hiding Profile Screen

Adding a New Topology Hiding Header

Note:	In previous versions of E-SBC prior to Release 4.0.4, this section was titled "Adding a New Topology Hiding Rule." With Release 4.0.4, Topology Hiding rules are now replaced with and based on headers instead of based on rules and URI groups as was done previously.

Use the following procedure to add a new Topology Hiding Header to an existing Topology Hiding profile.

In the Application Pane, select the Topology Hiding Profile (TH_Profile_2 in the example in Figure 7-28) to which you want to add a new Topology Hiding Header.
In the Content Area, click the Edit button to display the Edit Topology Hiding Profile screen (Figure 7-29).

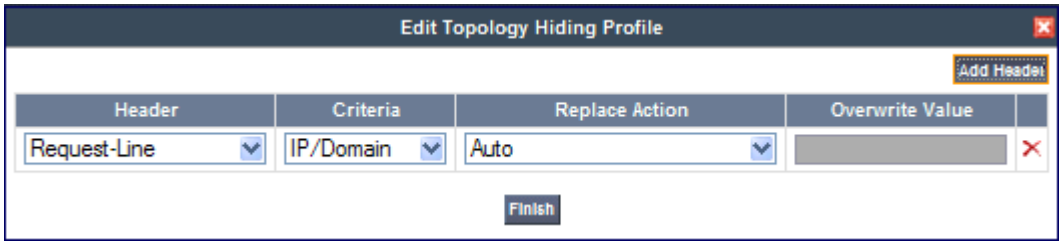


Figure 7-29. Edit Topology Hiding Profile Screen 1

In the Edit Topology Hiding Profile screen (Figure 7-29), select the Add Header button to add an additional Header description row, as shown in the second Edit Topology Hiding Profile screen (Figure 7-30).

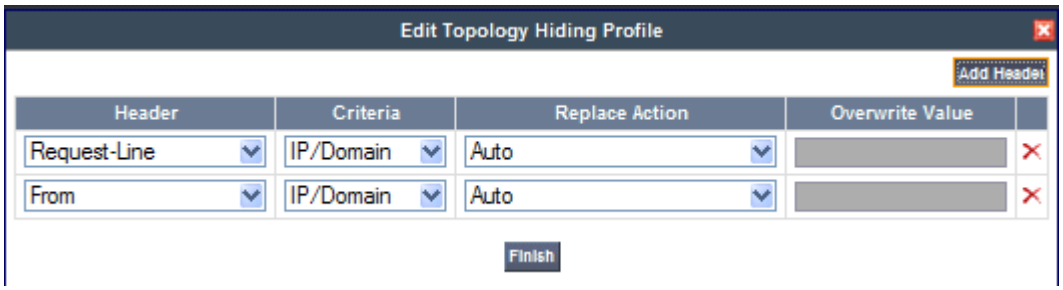


Figure 7-30. Edit Topology Hiding Profile Screen 2

Note:	The total number of new Headers that can be added is restricted to the number of parameter names in the Header field drop-down list. For example, the list contains six Header parameter names, therefore you are only able to create six Headers with the names, Request-Line, From, To, Record-Route, Via, and SDP. When you select the Add Header button, a new Header description row is added below with the Header field containing the value of the next available Header name (e.g., "From"), which you can change by selecting a different value from the list.

In the drop-down list in the new Header field (named “From” in the example in Figure 7-30), you can use the supplied name of “From” or select another unused Header parameter name for the new Topology Hiding Header. For this example, the Header name of Record-Route is selected, as shown in Figure 7-31.

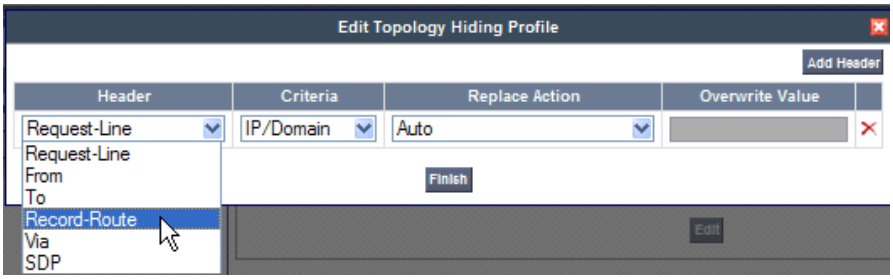


Figure 7-31. Edit Topology Hiding Profile Screen 3

After selecting an unused Header parameter name (e.g., Record_Route in the example) from the Header field drop-down list, select the remaining parameters from the Criteria field drop-down list, from the Replace Action field drop-down list, and if “Overwrite” was selected as the Replace-Action, enter an IP address in the Overwrite Value field.

Click Finish to submit, save, exit, and redisplay the Topology Hiding Profile display screen, which should now contain your newly-added Header, as shown in the updated Topology Hiding Profile display screen Figure 7-32.

Note in Figure 7-32 that the Topology Hiding Profile named TH_Profile_2 now has two Topology Hiding Headers defined, the original one named Request-Line and the one you just added named Record-Route.

Figure 7-32. Updated Topology Hiding Profile Display.

Editing a Topology Hiding Header

Use the following procedure to edit an existing a Topology Hiding rule for a specific Topology Hiding Profile.

In the Application Pane, select the Topology Hiding Profile (TH_Profile_2 in the example in Figure 7-32) containing the Topology Hiding Header you want to edit.

Click the Edit button (see Figure 7-32) at the bottom of the display an Edit Topology Hiding Profile screen (Figure 7-33), as shown in the example below.

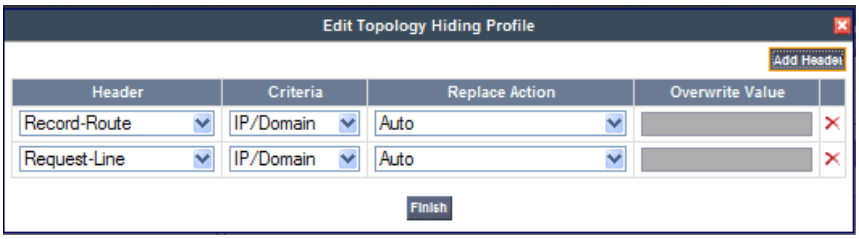


Figure 7-33. Edit Topology Hiding Profile Screen

In the Edit Topology Hiding Profile screen (Figure 7-33), you can edit any or all of the displayed Header rows just as described in the previous section, "Adding a New Topology Hiding Header." Just select new choices from the drop-down lists in the Header column, Criteria column, and Release Action column as described previously.

This ends the procedure for editing a Topology Hiding Header.

Deleting a Topology Hiding Profile or Header

Use the following procedures to delete an existing a Topology Hiding Profile or one of the Headers in a Topology Hiding Profile for a specific Topology Hiding Profile.

Delete a Topology Hiding Profile

In the Application Pane, select the Topology Hiding Profile (TH_Profile_2 in the example in Figure 7-32) that you want to delete.
Click the Delete Profile button (see Figure 7-32) at the top right-hand portion of the display to delete the selected Topology Hiding Profile.

This ends the procedure for deleting a Topology Profile.

Delete a Topology Hiding Header

In the Application Pane, select the Topology Hiding Profile (TH_Profile_2 in the example in Figure 7-32) containing the Topology Hiding Header you want to delete.
Click the Edit button (see Figure 7-32) at the bottom portion of the screen to display an Edit Topology Hiding Profile screen (Figure 7-33).
In the Edit Topology Hiding Profile screen (Figure 7-33), select the delete icon (✕) corresponding to the Topology Hiding Header you want to delete.

This ends the procedure for deleting a Topology Hiding Header.

Cloning an Existing Topology Hiding Profile

Use the following procedure to clone (copy) an existing Topology Hiding Profile.

Login to the E-SBC Control Center as the Admin.
Select the Topology Hiding function from the Global Profiles feature from the Task Pane.

Existing Topology Hiding Profiles are displayed in the Application Pane and their corresponding Topology rules are displayed in the Content Area of the E-SBC Control Center.

In the Application Pane, select the Topology Hiding Profile (TH_Profile_2 in the example in Figure 7-32) that you want to clone.

In the Content Area, click Clone Profile.

The Clone Profile pop-up window will be displayed (Figure 7-34).

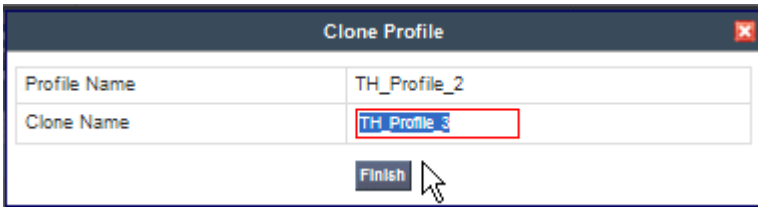


Figure 7-34. Clone Profile Pop-up Window.

Enter a name (e.g., TH_Profile_3) for the cloned profile and click Finish.

The Topology Hiding Profile is cloned and redisplayed (Figure 7-35) in the Application Pane.

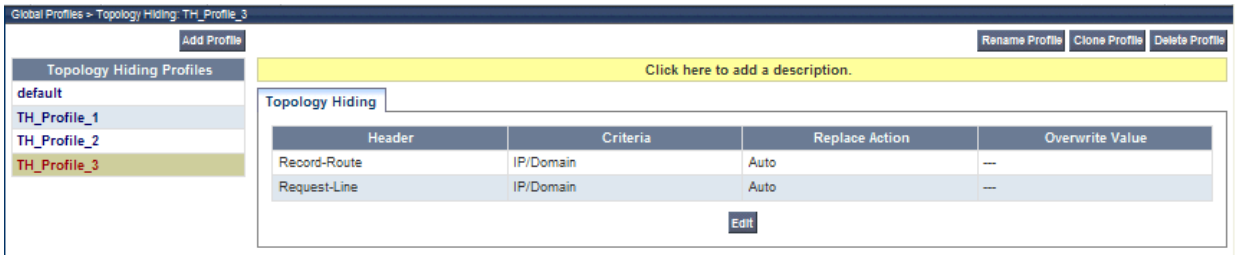


Figure 7-35. Updated Topology Hiding Display.

Renaming an Existing Topology Hiding Profile

Use the following procedure to rename an existing Topology Hiding Profile.

In the Application Pane, select the Topology Hiding Profile (TH_Profile_3 in the Figure 7-36 example that you want to rename.

In the Content Area, click Rename Profile.

The Rename Profile pop-up window (Figure 7-36) is displayed.

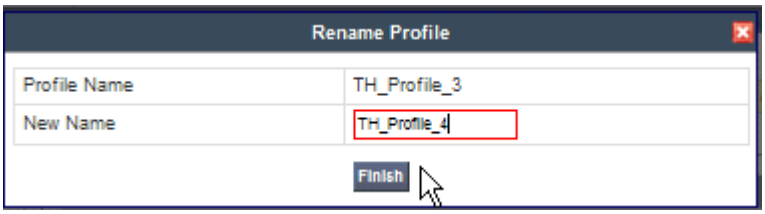


Figure 7-36. Rename Profile Pop-up Window.

Enter a new name (e.g.,TH_Profile_4) for the profile and click **Finish**.

The profile is renamed and redisplayed in the Application Pane (Figure 7-37).

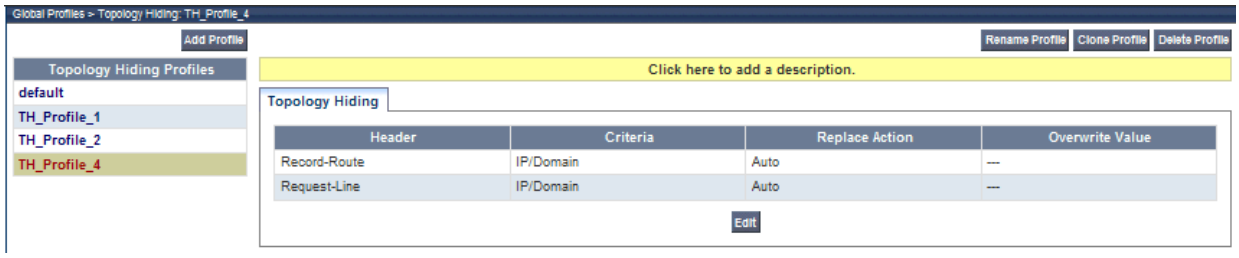


Figure 7-37. Updated Topology Hiding Display.

Headers Affected By Topology Hiding

When creating or editing Topology Hiding Profiles, there are six types of headers (i.e., **Request-Line**, **From**, **To**, **Record-Route**, **Via**, and **SDP**) available for selection in the **Header** drop-down list, as illustrated in below.

Note: In addition to the six headers listed in the drop-down list, there are additional headers (not listed) that are affected when either of two types of listed headers (i.e., **To Header** and **From Header**) are selected in the **Header** drop-down list.

Table 7-2 lists the six headers along with all of the other affected headers in three header categories (i.e., **Source Headers**, **Destination Headers**, and **SDP Headers**).

In the table, where applicable (i.e., **To Header** and **From Header**), additional affected headers are noted. In the next section titled, "*Topology Hiding Settings Examples*," descriptions are provided for all possible combinations of selections in the three parameter drop-down lists (i.e., **Header**, **Criteria**, and **Replace Action**), as shown in Figure 7-38 below.

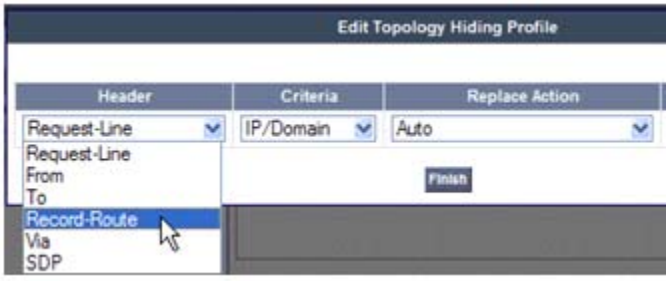


Figure 7-38. Topology Hiding Headers.

Table 7-2. Topology Hiding Headers.

Topology Hiding Headers		
Main Header Names	**Header(s) Affected by Main Header**	**Header Affecting This Header**
Source Headers		
Record-Route		
Route		
From	(1) Referred-By (2) PAsserted Identity	
Referred-By		From
PAsserted Identity		From
Destination Headers		
To	(1) ReferTo	
Request Start Line		
ReferTo		To
Diversion		
SDP Headers		
Origin Header		

Topology Hiding Settings Examples

This section provides examples for all of the possible combinations of topology hiding settings listed in the **Header** drop-down list (Figure 7-38), in the order listed (i.e., **Request-Line**, **From**, **To**, **Record-Route**, **Via**, and **SDP**). Each of the **Header** types is combined with each combination of the **Criteria** types (i.e., **IP/Domain**, **IP**, and **Domain**) and **Replace Action** types (i.e., **Auto**, **Next Hop**, **Destination IP**, and **Overwrite**) along with a description of the resulting action or effect.

Topology Hiding Examples for Request-Line Header

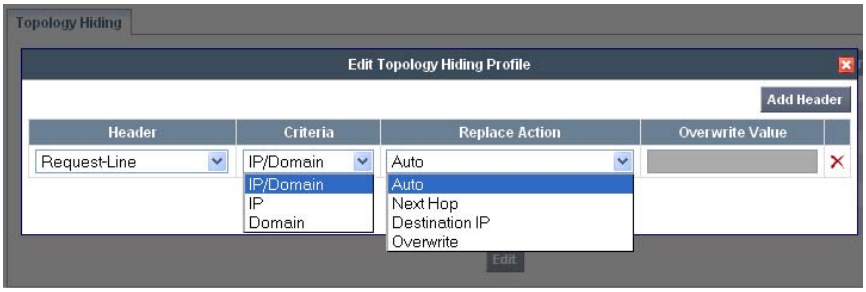


Figure 7-39. Topology Hiding Examples for Request-Line Header

1. Header - Request-Line
   Criteria - IP/Domain or IP or Domain
   Replace Action - Auto

   Topology Hiding will replace the **Request-Line** header by the next hop address/domain from the routing profile.

2. Header - Request-Line
   Criteria - IP/Domain
   Replace Action – Next Hop

   Topology Hiding will replace the **Request-Line** header by the next hop address/domain from the routing profile.

3. Header - Request-Line
   Criteria - IP/Domain
   Replace Action – Destination IP

   Topology Hiding will replace the **Request-Line** header with the Destination IP/Domain from the SIP message.

4. Header - Request-Line
   Criteria - IP/Domain
   Replace Action – Overwrite

   Topology Hiding will replace the **Request-Line** header by the Overwrite Value.

Topology Hiding Examples for From Header

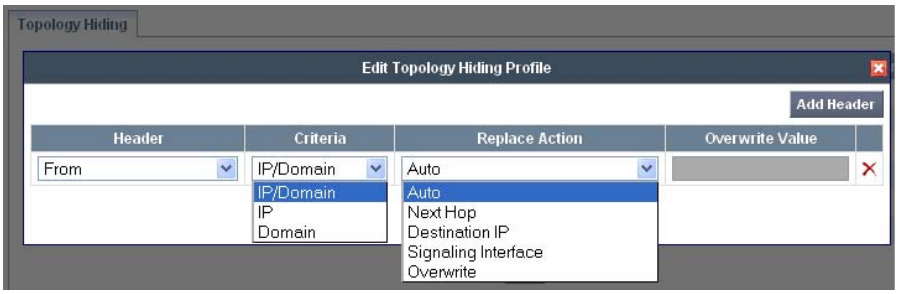


Figure 7-40. Topology Hiding Examples for From Header

Note:	The **From** header (and **To** header) settings also affect two other header types, the **Referred-By** header and the **P-Asserted-Identity** header. When the **From** header settings **Replace Actions** listed below are executed, automatic updates to the **Referred-By** header and **P-Asserted-Identity** header are performed as well.

1. Header - From
   Criteria - IP/Domain or IP or Domain
   Replace Action - Auto

   If the SIP message is from the Subscriber side then Topology Hiding will replace the **From Header** with the next hop address/domain from the routing profile
   If the SIP message is from the Call Server side or Trunk Server side then Topology Hiding will replace the **From Header** with the Signaling Interface

2. Header - From
   Criteria - IP/Domain or IP or Domain
   Replace Action – Next Hop

   Topology Hiding will replace the **From** header with the next hop address/Domain from the Routing profile.

3. Header - From
   Criteria - IP/Domain or IP or Domain
   Replace Action – Destination IP

   Topology Hiding will replace the **From** header with the Destination IP from the SIP Message.

4. Header - From
   Criteria - IP/Domain or IP or Domain
   Replace Action – Signaling Interface

   Topology Hiding will replace the **From** header with the Signaling Interface IP/Domain .

5. Header - From
   Criteria - IP/Domain or IP or Domain
   Replace Action – Overwrite

   Topology Hiding will replace the **From** header with the Overwrite Value.

Topology Hiding Examples for To Header

Figure 7-41. Topology Hiding Examples for To Header

Note:	The **To** header (and **From** header) settings also affect two other header types, the **Referred-By** header and the **P-Asserted-Identity** header. When the **To** header settings **Replace Actions** listed below are executed, automatic updates to the **Referred-By** header and **P-Asserted-Identity** header are performed as well.

1. Header - To
   Criteria - IP/Domain or IP or Domain
   Replace Action - Auto

   If the SIP message endpoint type is Subscriber then Topology Hiding will replace the **To** header with the Next Hop Address used by the Signaling Interface.
   If the SIP message endpoint type is Call Server or Trunk Server then Topology Hiding will replace the **To** header with the Next Hop Address.

2. Header - To
   Criteria - IP/Domain or IP or Domain
   Replace Action – Next Hop

   Topology Hiding will replace the **To** header with the Next Hop Address/Domain from the Routing profile.

3. Header - To
   Criteria - IP/Domain or IP or Domain
   Replace Action – Destination IP

   Topology Hiding will replace the **To** header with the Destination IP from the SIP Message.

4. Header - To
   Criteria - IP/Domain or IP or Domain
   Replace Action – Signaling Interface

   Topology Hiding will replace the **To** header with the Signaling Interface IP/Domain

5. Header - To
   Criteria - IP/Domain or IP or Domain
   Replace Action – Overwrite

   Topology Hiding will replace the **To** header with the Overwrite Value

Topology Hiding Examples for Record-Route Header

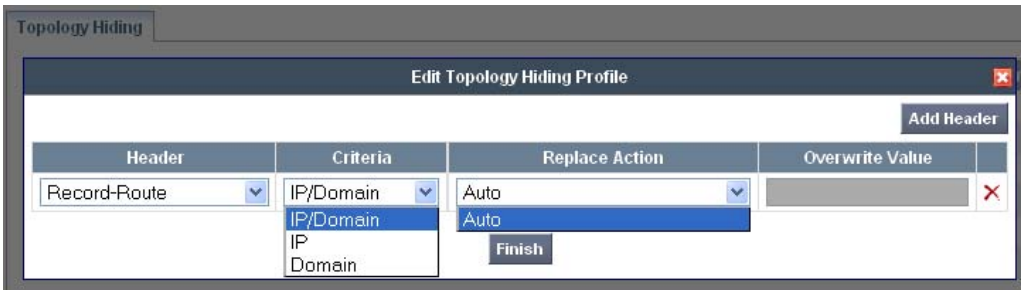


Figure 7-42. Topology Hiding Examples for Record-Route Header

1. Header – Record-Route
   Criteria - IP/Domain or IP or Domain
   Replace Action - Auto

   Topology Hiding will take and store the IP/Domain from the outbound message **Record-Route** header and then remove the Record-Route header from the outbound message. When the inbound message is received, Topology Hiding will put the stored IP/Domain in a **Record-Route** header and add the header to the inbound message.

Topology Hiding Examples for Via Header

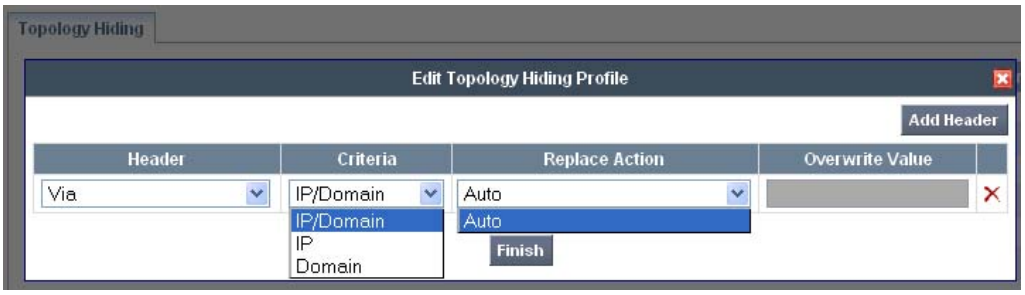


Figure 7-43. Topology Hiding Examples for Via Header

1. Header – Via
   Criteria - IP/Domain or IP or Domain
   Replace Action - Auto

   Topology Hiding will take and store the IP/Domain from the outbound message **Via** header and then remove the **Via** header. When the inbound message is received, Topology Hiding will put the stored IP/Domain in a **Via** header and add the header to the inbound message.

Topology Hiding Examples for SDP Header

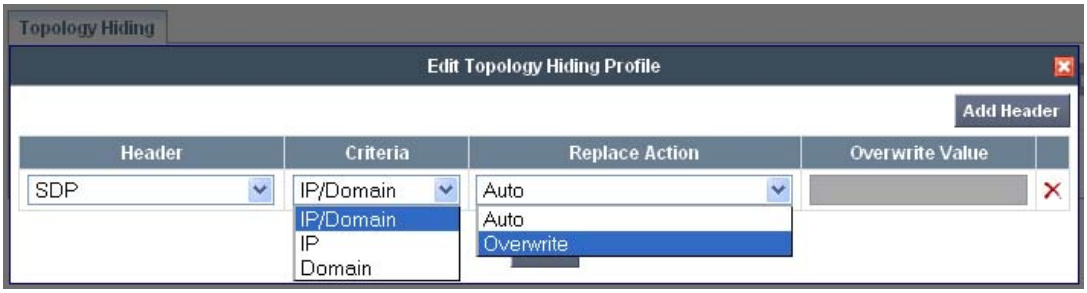


Figure 7-44. Topology Hiding Examples for SDP Header

1. Header – SDP
   Criteria - IP/Domain or IP or Domain
   Replace Action - Auto

   Topology Hiding will replace the **SDP** message IP/Domain with the Media Interface IP/Domain.

2. Header – SDP
   Criteria - IP/Domain or IP or Domain
   Replace Action - Overwrite

   Topology Hiding will replace the **SDP** message IP/Domain with the Overwrite Value.

Network Configuration 8

Overview

The E-SBC Control Center allows you to perform a number of network-specific configuration and management functions. These include the ability to:

- Manage SIP server configurations
- Manage interworking profiles
- Manage network configurations and custom routes
- Manage Transport Layer Security (TLS) parameters

The procedures required to perform these functions are contained in the following sections.

Managing SIP Server Configuration Profiles

Use the following procedures to manage SIP server configuration profiles.

Viewing SIP Server Profiles

Use the following procedure to view SIP server profiles.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Server Configuration** function of the **Global Profiles** feature from the Task Pane.
   The **Server Configuration** screen (Figure 8 - 1) will be displayed, containing a list of available Server Configuration profiles in the Application Panel.

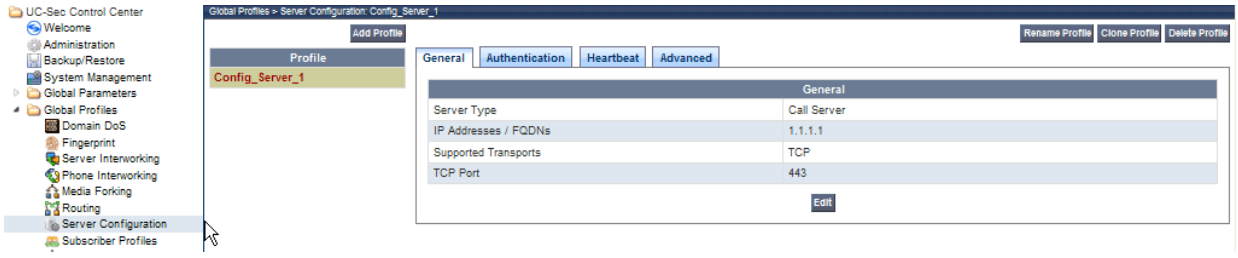


Figure 8 - 1. Server Configuration Display.

Adding a New SIP Server Profile

Use the following procedure to add a new SIP server profile.

1. Select **Add Profile**.
   The **Add Server Configuration Profile** pop-up window (Figure 8-2) is displayed.

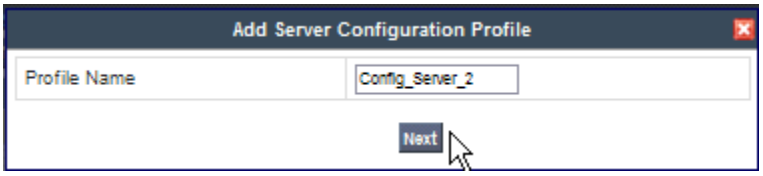


Figure 8-2. Add Server Configuration Pop-up Window.

2. Enter a name for the new profile and click **Next**.
   The **Add Server Configuration Profile – General** pop-up window (Figure 8-3) is displayed.

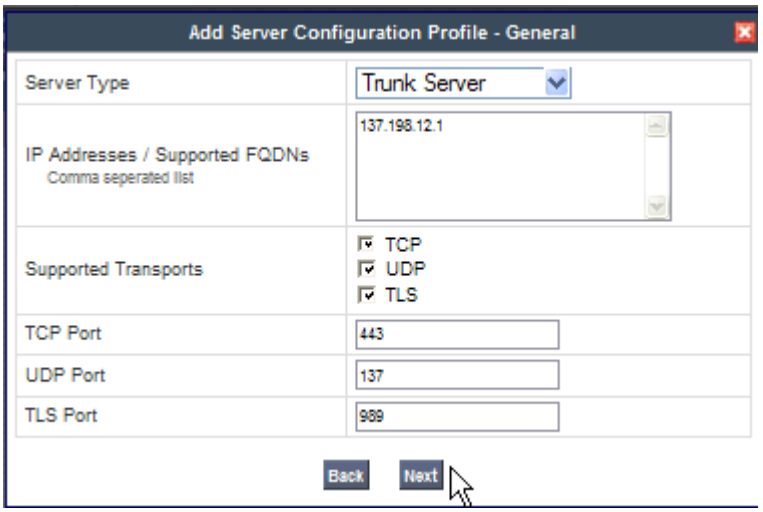


Figure 8-3. Add Server Configuration Profile - General Pop-up Window.

3. In the General pop-up window (Figure 8-3), enter the requested information into the appropriate fields.
   Selecting **Cancel** clears the fields and closes the pop-up window.

Table 8-1. Add Server Configuration Profile – General Pop-up Window Field Descriptions.

Field	Description
Server Type	Pull-down menu from which you select the type of SIP server for which this profile is being defined. Available selections are: **Trunk Server**, **Call Server**, **Proxy Server**, **Registrar Server**, **MWI Server**, **Presence Server**, and **Music Server**.

Field	Description
IP Addresses / Supported FQDNs	The IP address or Fully-Qualified Domain Name (FQDN) of the SIP server. You can add multiple IPs and FQDNs, separated by commas.
Supported Transports	Checkboxes indicating which type(s) of transport protocols are supported by the SIP server. Available selections are: **TCP**, **UDP**, and **TLS**. Clicking the checkbox indicates that protocol is supported by the server and the corresponding port field is then activated.
TCP Port	The port assignment for TCP traffic.
UDP Port	The port assignment for UDP traffic.
TLS Port	The port assignment for TLS traffic.

4. Select **Next**.
   The **Add Server Configuration Profile – Authentication** pop-window (Figure 8-4) is displayed.

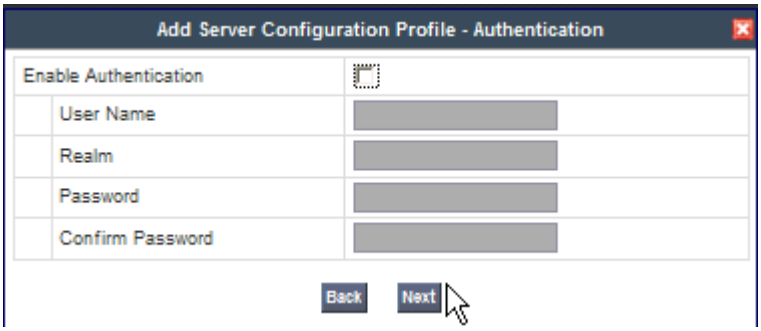


Figure 8-4. Add Server Configuration Profile - Authentication Pop-up Window.

5. Enter the requested information into the appropriate fields.

   (Selecting **Cancel** clears the fields and closes the pop-up window.)

Table 8-2. Add Server Configuration Profile – Authentication Pop-up Window Field Descriptions.

Field	Description
Enable Authentication	Checkbox indicating whether or not the SIP server requires authentication. Checking this box ( ) indicates authentication is required and the remaining fields are activated. An empty checkbox ( ) indicates no authentication is required and the remaining fields remain inactivated.
User Name	The user name required for authentication.
Realm	The realm from which the legitimate authentication request will be made.
Password	The password required for authentication.

6. Select **Next**.

The **Add Server Configuration Profile – Heartbeat** pop-window (Figure 8-5) is displayed.

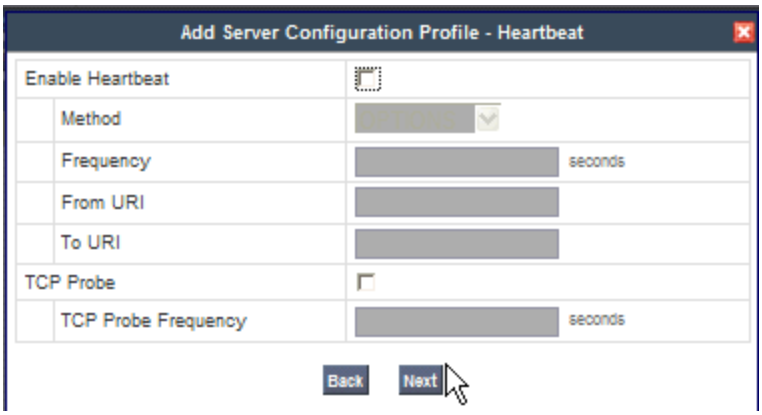


Figure 8-5. Add Server Configuration Profile - Heartbeat Pop-up Window.

7. Enter the requested information into the appropriate fields (Table 8-3). Selecting **Cancel** clears the fields and closes the pop-up window.

Table 8-3. Add Server Configuration Profile – Heartbeat Pop-up Window Field Descriptions.

Field	Description
Enable Heartbeat	Checkbox indicating whether or not a synchronization signal (heartbeat) will be established between the E-SBC security device and the SIP server. Checking this box (☑) indicates a heartbeat will be established and maintained and the remaining fields are activated. An empty checkbox (☐) indicates no heartbeat will be maintained and the remaining fields remain inactivated.
Method	Drop-down menu from which you determine the manner in which the heartbeat will be maintained. Available selections are: **Ping** and **Register**.
Frequency	The frequency with which the heartbeat signal will be sent.
From URI	The source of the heartbeat signal.
To URI	The destination of the heartbeat signal.

8. Select **Next**.
   The **Add Server Configuration profile – Advanced** pop-window (Figure 8-6) is displayed.

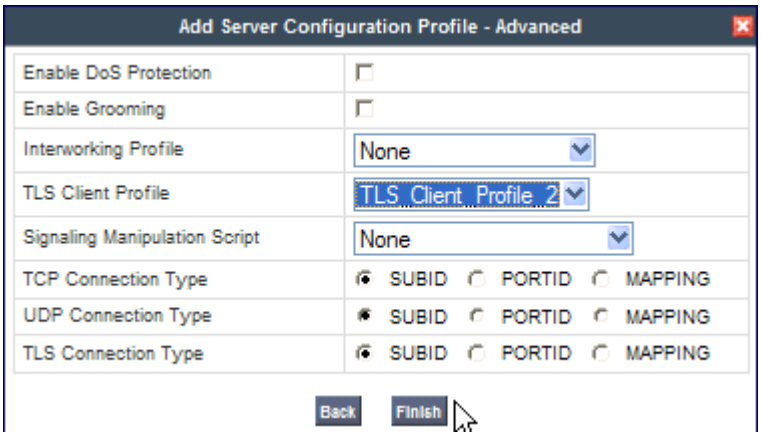


Figure 8-6. Add Server Configuration Profile - Advanced Pop-up Screen

9. Enter the requested information into the appropriate fields (Table 8-4). Selecting **Cancel** clears the fields and closes the pop-up window.

Note:	When the Enable DoS Protection checkbox is checked in the previous screen, a second Add Server Configuration Profile – Heartbeat pop-up screen is displayed, prompting for the number of users on this Call Server.

Table 8-4. Add Server Configuration Profile – Heartbeat Pop-up Window Field Descriptions.

Field	Description
Enable DoS Protection	Checkbox indicating whether or not DoS protection will be enabled for this SIP server. Checking this box (☑) indicates DoS protection will be enabled for this server. An empty checkbox (☐) indicates no DoS protection will be enabled for this SIP server.
Topology Hiding Profile	Drop-down menu from which you can select the Topology Hiding profile to be used for this SIP server.
Interworking Profile	Drop-down menu from which you can select the Interworking profile to be used for this SIP server.
TLS Client Profile	Drop-down menu from which you can select the TLS Client profile to be used for this SIP server.
Routing Profile	Drop-down menu from which you can select the Routing profile to be used for this SIP server.
TCP Connection Type	Manner in which TCP connections will be established. Available selections are: **SUBID**, **PORTID**, and **MAPPING**.
UDP Connection Type	Manner in which UDP connections will be established. Available selections are: **SUBID**, **PORTID**, and **MAPPING**.
TLS Connection Type	Manner in which TLS connections will be established. Available selections are: **SUBID**, **PORTID**, and **MAPPING**.
Enable Grooming	Checkbox indicating whether or not the same connection will be used for the same subscriber or port.

10. Select **Next**. An updated Server Configuration screen (Figure 8-7) is displayed.

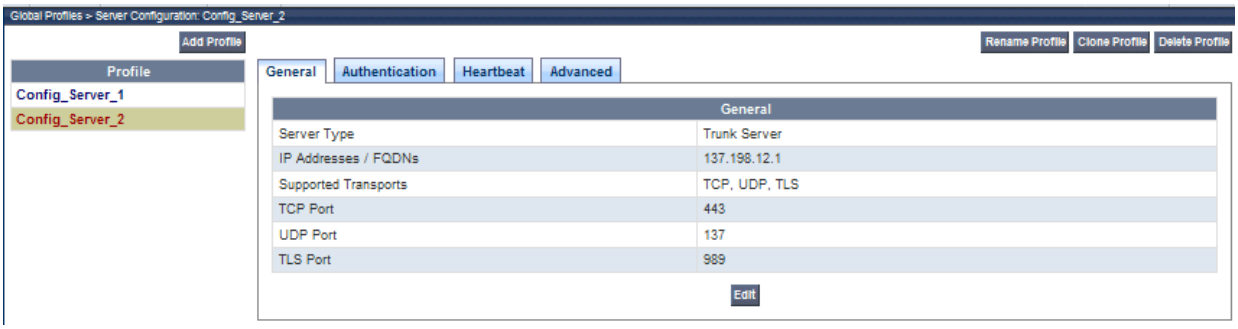


Figure 8-7. Updated Server Configuration Display.

Editing a SIP Server Profile

Use the following procedure to edit a SIP server profile.

Notes

SIP server profiles are edited by selecting the desired parameters tab (**General**, **Authentication**, **Heartbeat**, and **Advanced**, and then changing the information contained on the screen displayed.

If the **Enable DoS Protection** checkbox (see Figure 8-6) is checked in Step 9, there will be two additional parameters tabs, **DoS Whitelist** and **DoS Protection** (see Figure 8-12).

1. In the Application Pane (Figure 8-8), select the server profile you want to edit.
2. In the Content Area, select the tab whose parameters you want to edit (Figure 8-8).
3. Click the **Edit** button at the bottom of the selected tab screen.
   As an example, if the **Config_Server_2** profile is selected and its **Advanced** tab is selected prior to clicking on the **Edit** button, a **Server Configuration Profile – Advanced Edit** pop-up window similar to the example in Figure 8-9 is displayed.

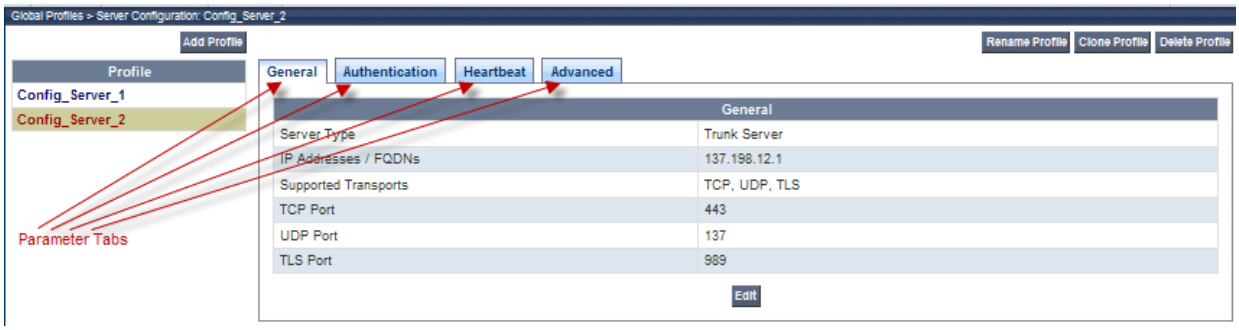


Figure 8-8. Server Configuration Parameter Tabs.

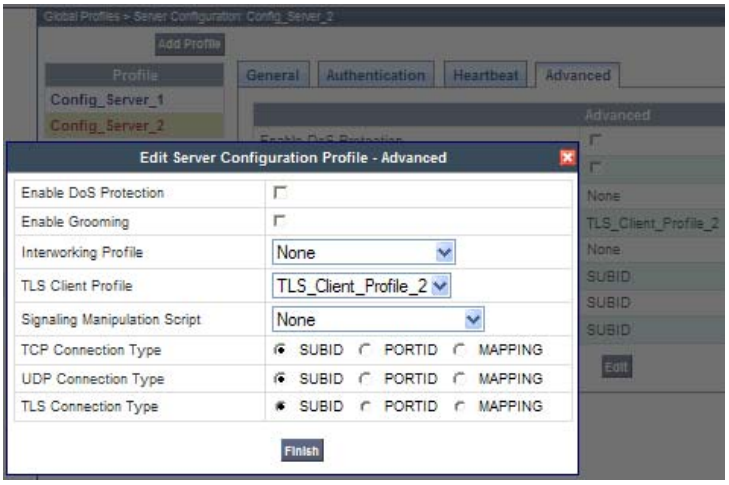


Figure 8-9. Server Configuration Profile – Advanced Edit Pop-up Window.

4. Edit the desired fields, and click **Finish**.
   Your changes are saved and the Server Configuration screen is redisplayed.

Editing the DoS Whitelist Parameter Tab

Editing the **DoS Whitelist** parameter tab entails either adding or deleting URI/Domain information to and from the DoS Whitelist. Each of these procedures is described below.

Note: In order for the **DoS Whitelist** parameter tab to be displayed, as described in the next section titled, "Editing the DoS Whitelist Parameter Tab," the **Enable DoS Protection** checkbox (see Figure 8-6) must be checked in Step 9 of the procedure described in the section, "Adding a New SIP Server Profile."

This can also be done later by editing the **Advanced** tab, as described in the previous section titled, "Editing a SIP Server Profile," and illustrated below.

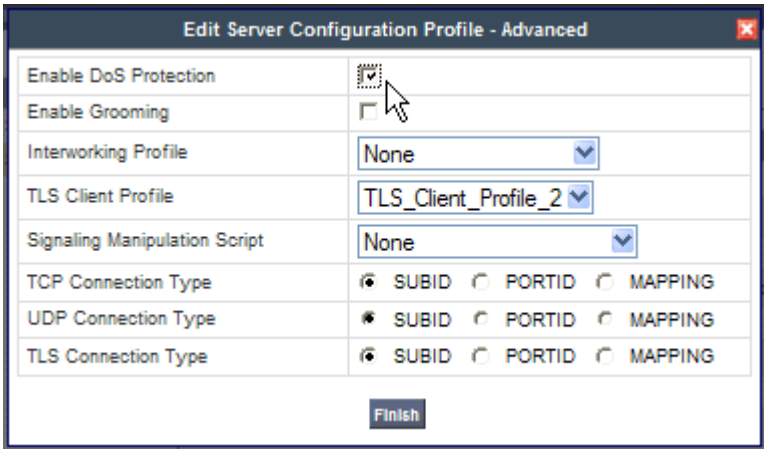


Figure 8-10. Enabling DoS Protection.

Adding a URI/Domain to the DoS Whitelist

1. In the Content Area, select the **DoS Whitelist** parameter tab.
2. Click **Add URI/Domain**. The **Add Whitelist** URI pop-up window is displayed (Figure 8-11).

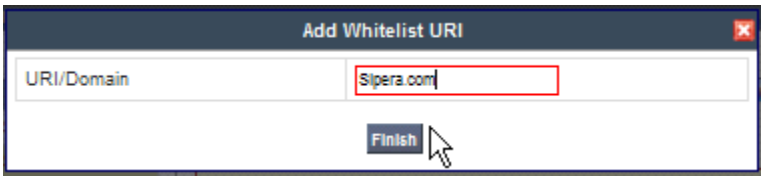


Figure 8-11. Add Whitelist URI Pop-up Window.

3. Enter the URI/Domain into the field provided as shown in the example and click **Finish**. The URI/Domain is added to the Whitelist (Figure 8-12).

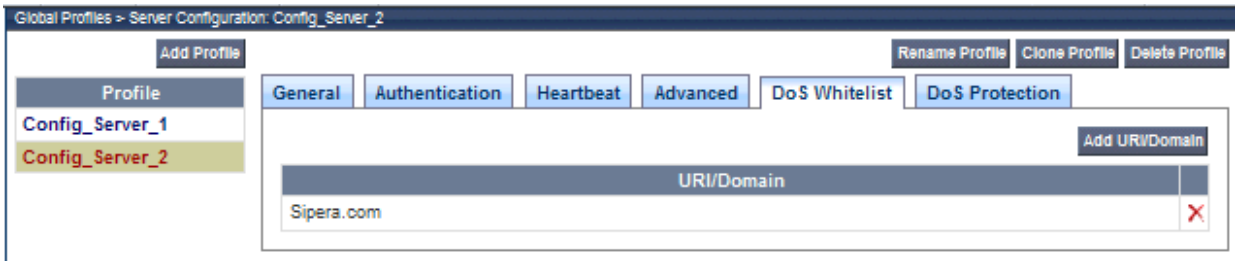


Figure 8-12. Updated DoS Whitelist Display.

Deleting a URI/Domain from the DoS Whitelist

1. In the Content Area, select the Delete icon (✕) corresponding to the URI/Domain you want to delete. As an example in above, click on the red delete icon (✕) to the right of the URI/Domain (**Sipera.com**) to delete it.
2. A Delete Confirmation pop-up window, similar to that shown in Figure 8-13 will be displayed.

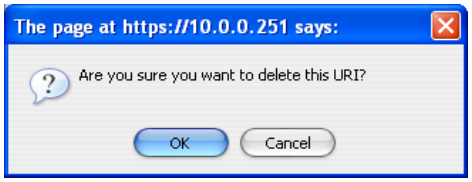


Figure 8-13. Delete Confirmation Pop-up Window.

3. Click **OK**.
   The URI/Domain is deleted and the DoS Whitelist redisplayed (Figure 8-14), showing that the URI/Domain (**Sipera.com**) has been removed.

Figure 8-14. Updated DoS Whitelist Display.

Editing the DoS Protection Parameter Tab

Editing the **DoS Protection** parameter tab only allows you to manage certain parameters for a specific set of SIP services and methods. The procedure to these parameters is contained below.

Note: In order for the **DoS Protection** parameter tab to be displayed, as described below, the **Enable DoS Protection** checkbox (see Figure 8-6) should have been checked in Step 9 of the procedure described in the section, "Adding a New SIP Server Profile."

This can be done later by editing the **Advanced** tab, as described in the section titled, "Editing a SIP Server Profile," and illustrated in Figure 8-10.

1. In the Content Area, select the **DoS Protection** parameter tab (Figure 8-15).
2. Click the Edit icon corresponding to the SIP service or method you want to edit. The corresponding Edit Server DoS pop-up window is displayed, similar to that shown in Figure 8-16 for the Presence Updates parameter.

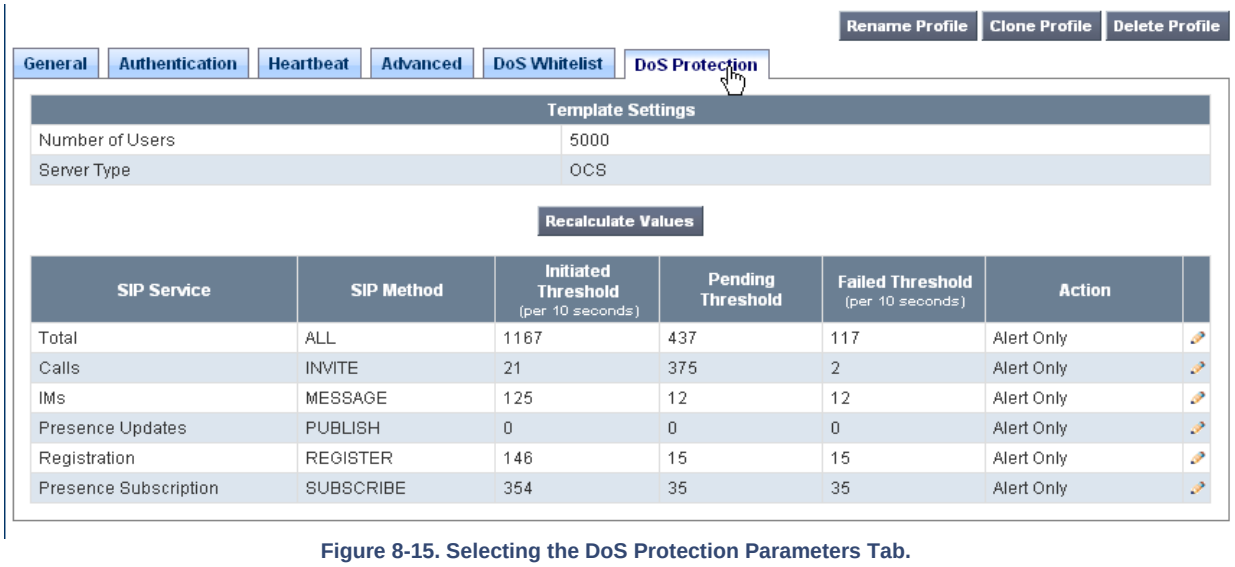


Figure 8-15. Selecting the DoS Protection Parameters Tab.

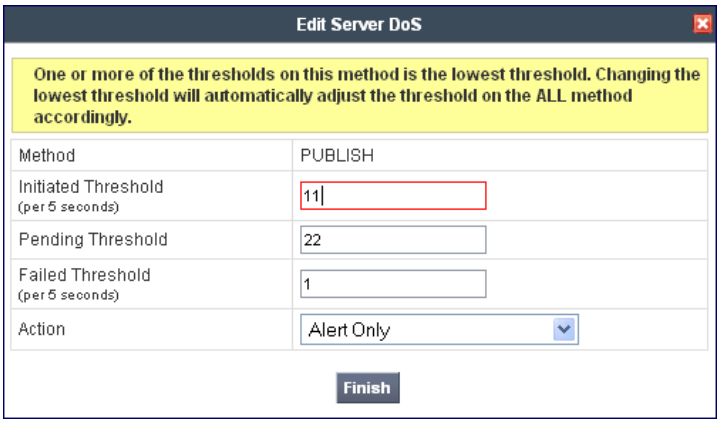


Figure 8-16. Edit Server DoS Pop-up Window.

3. Edit the desired fields and click **Finish**.
   Your changes are saved and the DoS Protection screen redisplayed.

Cloning an Existing SIP Server Profile

Use the following procedure to clone (make an exact copy of) an existing SIP server profile.

1. In the Application Pane, select the server profile you want to clone (Figure 8-17).
2. In the Content Area, click **Clone Profile**.
   The **Add Server Configuration Profile** pop-up window is displayed (Figure 8-18).

Figure 8-17. Selecting a SIP Configuration Profile.

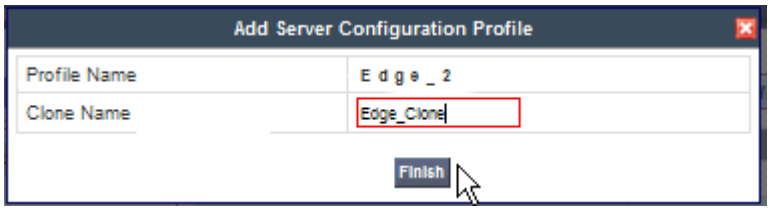


Figure 8-18. Add Server Configuration Profile Pop-up Window.

3. Enter a new name for the cloned profile and click **Finish**.
   The profile is copied, renamed, and saved and the **Server Configuration** screen redisplayed (Figure 8-19).

Figure 8-19. Updated Server Configuration Display.

Renaming an Existing SIP Server Profile

Use the following procedure to rename an existing SIP server profile.

1. In the Application Pane, select the server profile you want to rename.
2. In the Content Area, click Rename Profile.
   The Rename Server Configuration Profile pop-up window is displayed (Figure 8-20).

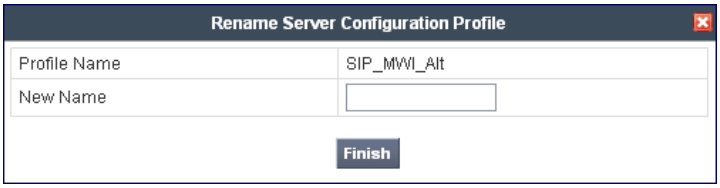


Figure 8-20. Rename Server Configuration Profile Pop-up Window.

3. Enter a new name for the profile and click **Finish**.
   The profile is renamed and the **Server Configuration** screen redisplayed (Figure 8-21).

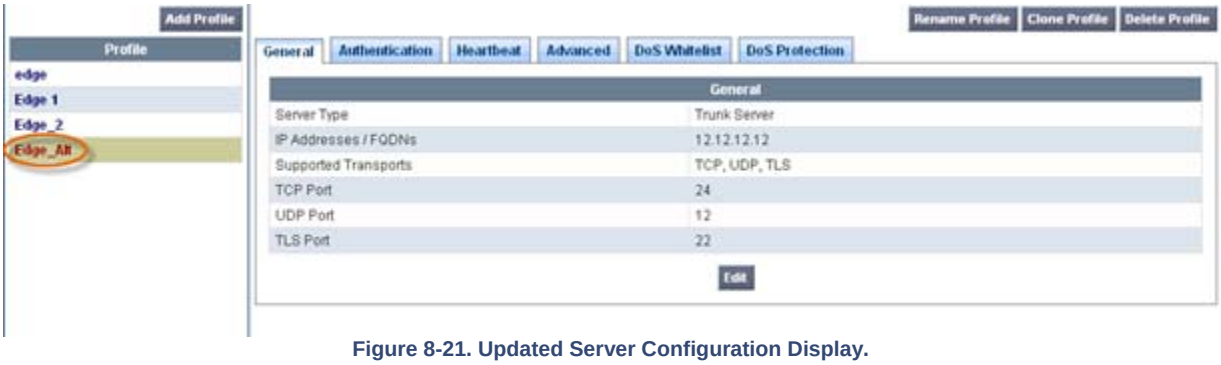


Figure 8-21. Updated Server Configuration Display.

Deleting an Existing SIP Server Profile

Use the following procedure to delete an existing SIP server profile.

1. In the Application Pane, select the server profile you want to delete (Figure 8-21).
2. In the Content Area, click **Delete Profile**.
   A **Delete Confirmation** pop-up window, similar to that shown in Figure 8-22 is displayed.

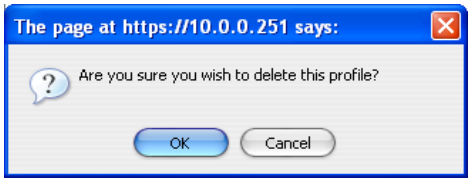


Figure 8-22. Delete Confirmation Pop-up Window.

3. Click OK.
   The SIP server profile is deleted and the Server Configuration screen redisplayed (Figure 8-23).

Figure 8-23. Updated Server Configuration Display.

Interworking

The **Interworking** function of the **Global Profiles** feature allows you to set certain parameters to make the E-SBC security device function in an enterprise VoIP network using different implementation of the SIP protocol.

Viewing Existing Interworking Profiles

Use the following procedure to view existing interworking profiles.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Interworking** function of the **Global Profiles** feature from the Task Pane.
   The **Interworking** screen will be displayed, containing a list of available **Interworking** profiles in the Application Pane (Figure 8-24).

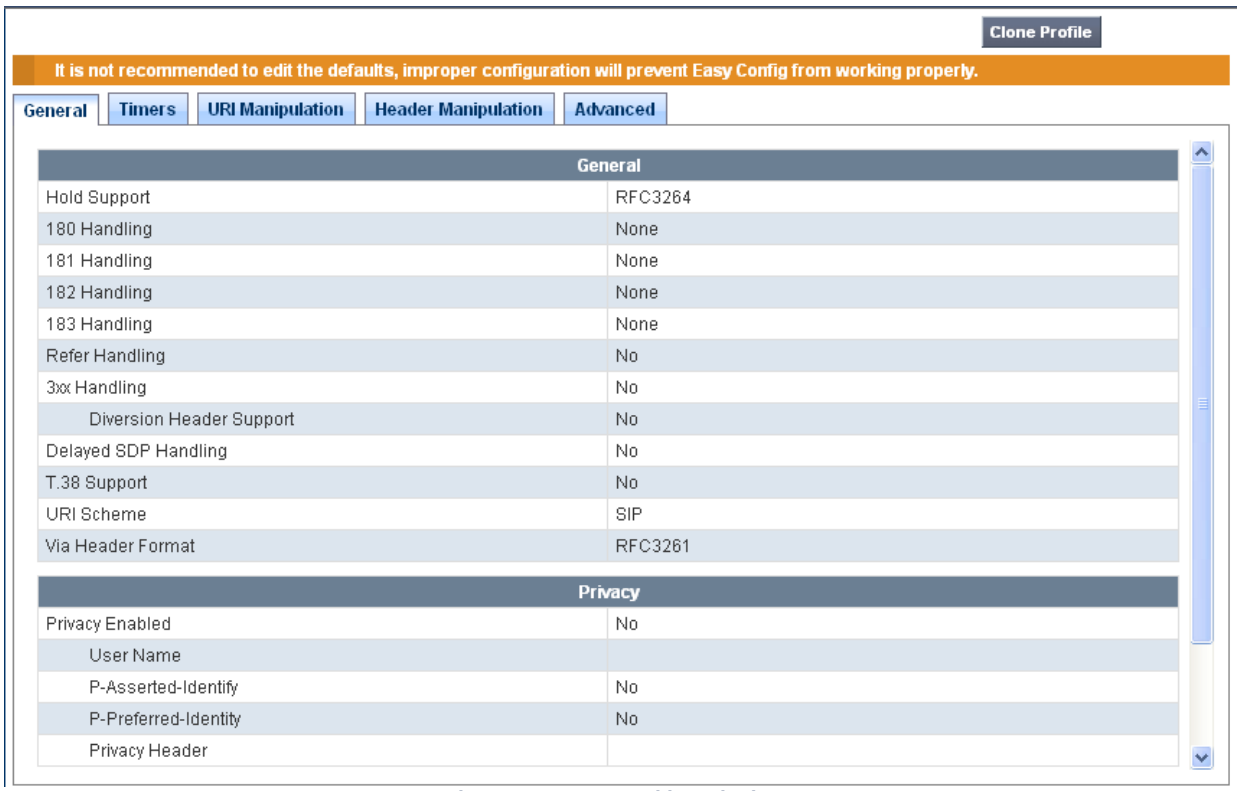


Figure 8-24. Interworking Display.

Adding a New Interworking Profile

Use the following procedure to add a new interworking profile.

1. From the Application Pane, click **Add Profile**.
   The **Add Interworking Profile** pop-up window is displayed (Figure 8-25).

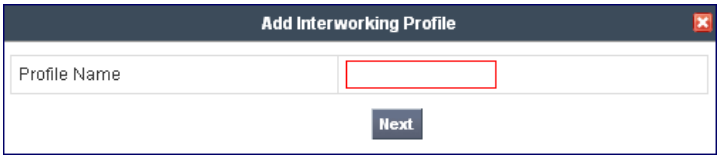


Figure 8-25. Add Interworking Profile Pop-up Window.

2. Enter a name for the new profile and click **Next**.
   The **Add Interworking Profile - General** pop-up window is displayed (Figure 8-26).

Enter the requested information into the appropriate fields (

3. Table 8-5).

4. Selecting **Cancel** clears the fields and closes the pop-up window.

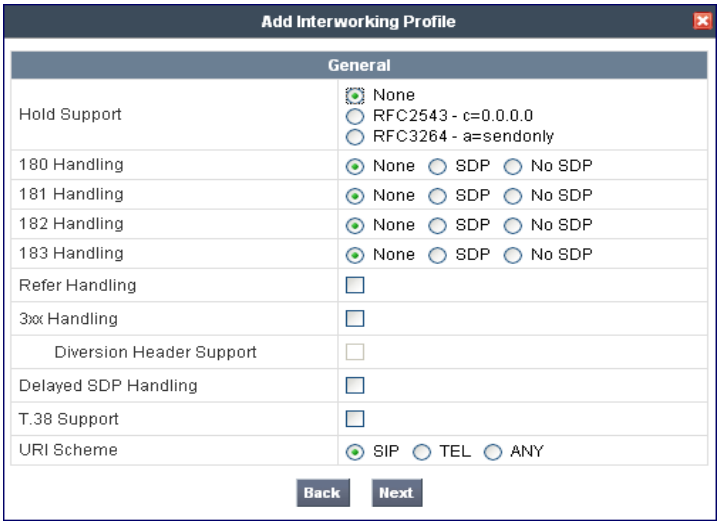


Figure 8-26. Add Interworking Profile - General Pop-up Window.

Table 8-5. Add Interworking Profile – General Pop-up Window Field Descriptions.

Field	Description
	General
Hold Support	The standard to be used to provide **HOLD** support. Available selections are: **None**, **RFC 2543**, and **RFC 3264**.
180 Handling	Radio buttons allowing you to determine how **180 Ringing** messages will be handled. Available selections are: **None**, **SDP**, and **No SDP**.
181 Handling	Radio buttons allowing you to determine how **181 Call is being Forwarded** messages will be handled. Available selections are: **None**, **SDP**, and **No SDP**.
182 Handling	Radio buttons allowing you to determine how **182 Queued** messages will be handled. Available selections are: **None**, **SDP**, and **No SDP**.
183 Handling	Radio buttons allowing you to determine how **183 Session Progress** messages will be handled. Available selections are: **None**, **SDP**, and **No SDP**.
Refer Handling	Checkbox indicating whether or not **REFER** requests will be handled by the E-SBC security device.
3xx Handling	Checkbox indicating whether or not the E-SBC security device will handle **3xx Redirection Response** messages.
Diversion Header Support	Checkbox indicating whether or not **Diversion Headers** will be supported by the E-SBC security device.
Delayed SDP Handling	Checkbox indicating whether or not delayed SDP packets will be processed by the E-SBC security device.
T.38 Support	Checkbox indicating whether or not the **T.38 FAX Relay** standard will be supported by the E-SBC security device.
URI Scheme	The URI scheme to be used by the E-SBC security device. Available selections are: **SIP**, **TEL**, and **ANY**.

5. Select **Next**.
   The **Add Server Configuration Profile – Privacy** pop-window is displayed (Figure 8-27).

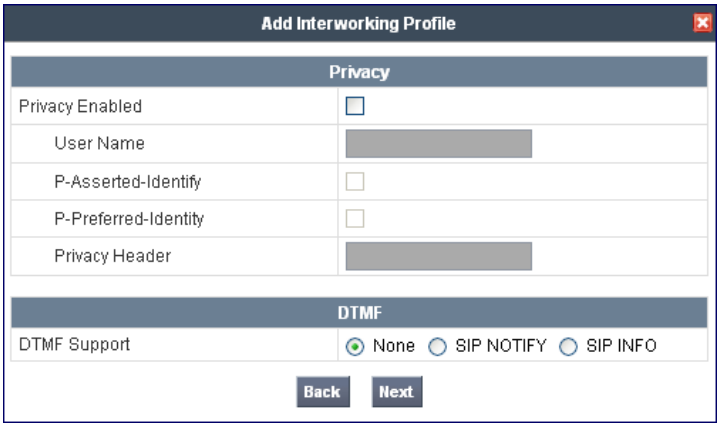


Figure 8-27. Add Interworking Profile - Privacy Pop-up Window.

6. Enter the requested information into the appropriate fields (Table 8-6). Selecting **Cancel** clears the fields and closes the pop-up window.

Table 8-6. Add Interworking Profile – Privacy Pop-up Window Field Descriptions.

Field	Description
	Privacy
Privacy Enabled	Checkbox indicating whether or not privacy will be used between the E-SBC security device and the SIP server.
User Name	**User Name** to be used for privacy authentication.
P-Asserted-Identity	Checkbox indicating that the E-SBC will rewrite the **FROM** header in a trusted SIP message with the P-Asserted-ID. This is used for maintaining privacy for the From header. Trunk servers usually Accept SIP INVITE with P-asserted ID. For some Trunk servers, E-SBC will insert this header from the From header, insert it in P-asserted ID and change From as Anonymous user, and send out the request.
P-Preferred-Identity	Checkbox indicating that the E-SBC will use the P-Preferred-ID during the private sessions.
Privacy Header	The Privacy Header to be used during privacy sessions.
	DTMF
DTMF Support	Radio buttons indicating the type of DTMF support. Available selections are: **None**, **SIP NOTIFY**, and **SIP INFO**.

7. Select **Next**.
   The **Add Server Configuration Profile – SIP Timers** pop-window is displayed (Figure 8-28).

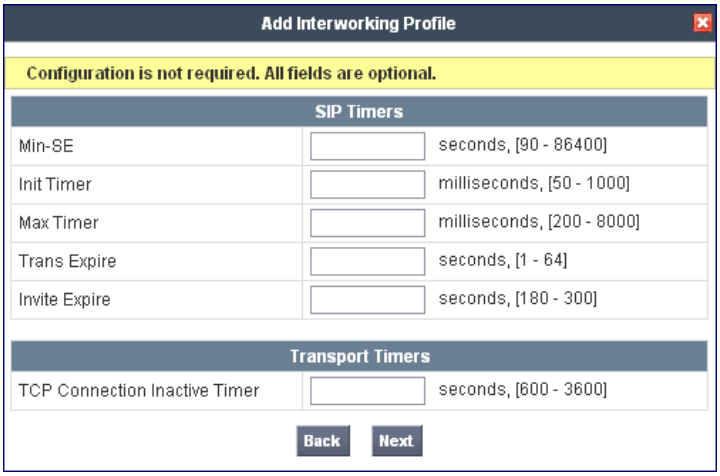


Figure 8-28. Add Interworking Profile – SIP Timers Pop-up Window.

8. Enter the requested information into the appropriate fields.
   (Selecting **Cancel** clears the fields and closes the pop-up window.)

Table 8-7. Add Interworking Profile – SIP Timers Pop-up Window Field Descriptions.

Field	Description
	SIP Timers
Min-SE	The minimum value (in seconds) for the SIP **min-SE** timer. The Min-SE timer is used for SIP refresh (Re-Invite/Update) session as the minimum session expire time value.
Init Timer	Initial request retransmission interval (in milliseconds). This is the initial SIP request retransmission interval. It corresponds to Timer T1 in RFC 3261.This timer is used when sending request over UDP.
Max Timer	The maximum retransmission interval for non-INVITE requests (in milliseconds). This is the maximum retransmission interval for non-INVITE requests. It corresponds to Timer T2 in RFC 3261.
Trans Expire	Value of the **Transaction Expiration** timer (in seconds).
Invite Expire	The transaction expiration time for an INVITE transaction after a provisional response has been received (in seconds).
	Transport Timers
TCP Inactive Timer	The maximum amount of inactivity allowed to lapse (in seconds) before the TCP connection is terminated.

9. Select **Next**.
   The **Add Server Configuration Profile – Advanced Settings** pop-window is displayed (Figure 8-29).

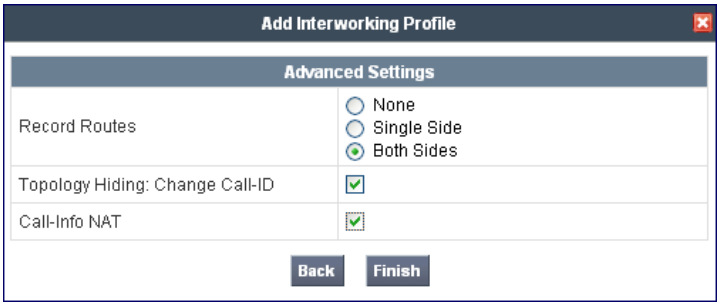


Figure 8-29. Add Interworking Profile – Advanced Settings Pop-up Window.

10. Enter the requested information into the appropriate fields (Table 8-8). Selecting **Cancel** clears the fields and closes the pop-up window.

Table 8-8. Add Interworking Profile – Advanced Settings Pop-up Window Field Descriptions.

Field	Description
	Advanced Settings
Record Routes	Radio buttons which direct the E-SBC security device to record route information. Available selections are: **None**, **Single Side**, and **Both Sides**.
Topology Hiding: Change Call-ID	Checkbox which directs the E-SBC security device to change the **Call-ID** field in the SIP message header.
Call-Info NAT	Checkbox indicating that the **Call-Info** field should be changed by the E-SBC security device to accommodate NAT functionality.

11. Click **Finish**.

The new **Server Configuration Profile** is added and the Server Configuration screen redisplayed (Figure 8-30).

Figure 8-30. Updated Server Configuration Display.

Editing Existing Interworking Profiles

Interworking profiles have their parameters grouped across five tab displays: **General**, **Timers**, **URI Manipulation**, **Header Manipulation**, and **Advanced**, all of which can be selected and easily edited. Editing the contents of the **General**, **Timers**, and **Advanced** tabs is different than how the contents of the **URI Manipulation** and **Header Manipulation** tabs are edited.

Refer to the procedure *Editing the General, Timers, and Advanced Parameter Tabs* for editing the **General**, **Timers**, and **Advanced** tabs.

Refer to the procedure *Editing the URI Manipulation and Header Manipulation Parameter Tabs* for editing the **URI Manipulation** and **Header Manipulation** tabs

Editing the General, Timers, and Advanced Parameter Tabs

Use the following procedure to edit the contents of the **General**, **Timers**, and **Advanced** parameter tabs.

Note

For the purposes of this procedure, the **General** parameters tab is as an example. The editing procedure is the same for the **Timers** and **Advanced** parameter tabs.

1. In the Application Pane, select the Interworking profile you want to edit (Figure 8-31).
2. In the Content Area, select the parameter tab you want to edit (**General**, **Timers**, or **Advanced**). The parameters for that tab are displayed in the Content Area.
3. In the Content Area, click **Edit**.

The corresponding **Editing Profile** pop-up window is displayed, similar to that shown in Figure 8-32.

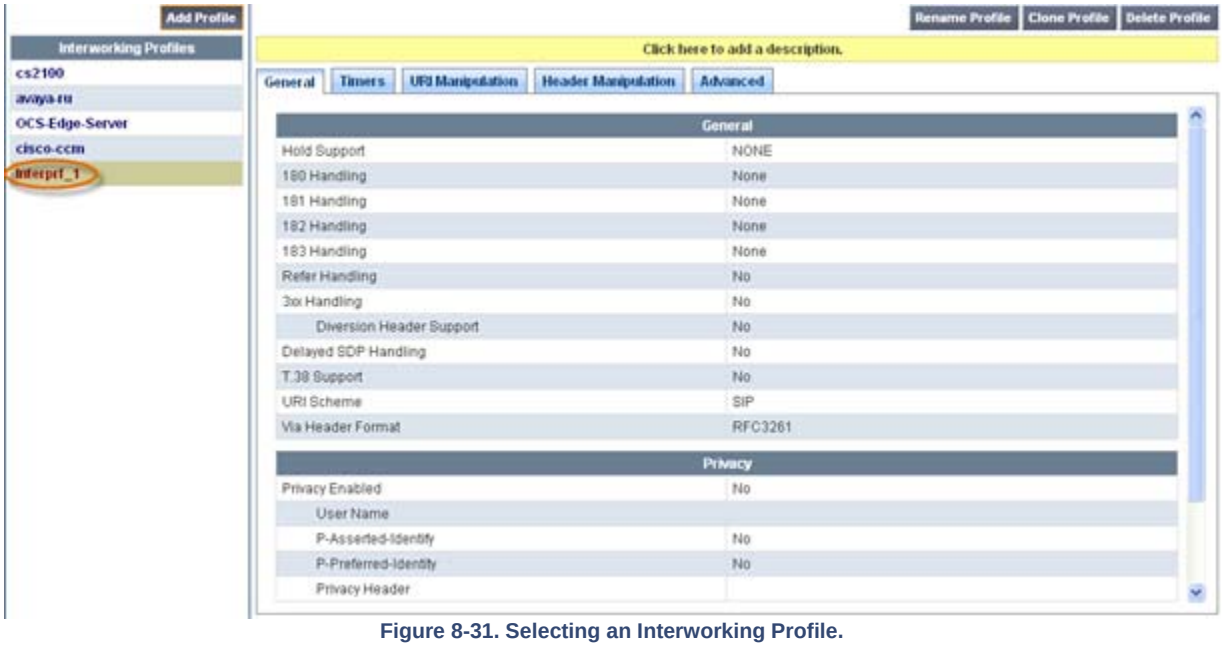


Figure 8-31. Selecting an Interworking Profile.

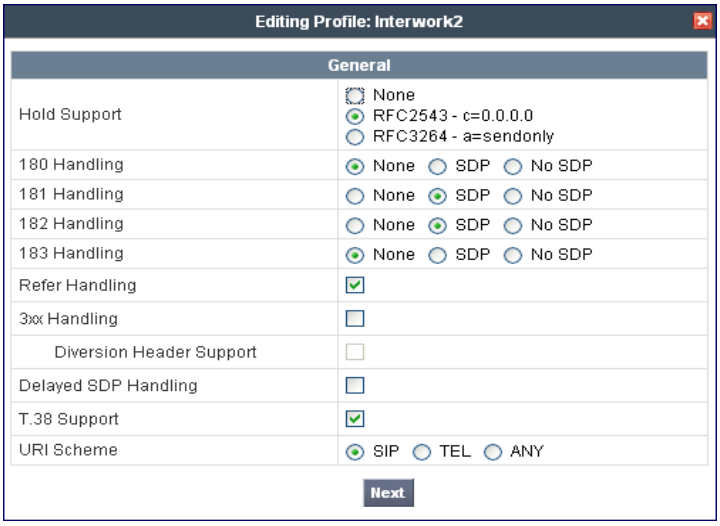


Figure 8-32. Edit Profile Pop-up Window.

4. Edit the desired fields and click **Next**.
   The next **Editing Profile** pop-up window is displayed, similar to that shown in Figure 8-33.

Note

Not all editing pop-up windows have additional follow-up editing windows. If the pop-up window currently displayed is the only window that can be edited, then the pushbutton on the bottom of the window will display **Finish**. Click **Finish** and proceed to step 5.

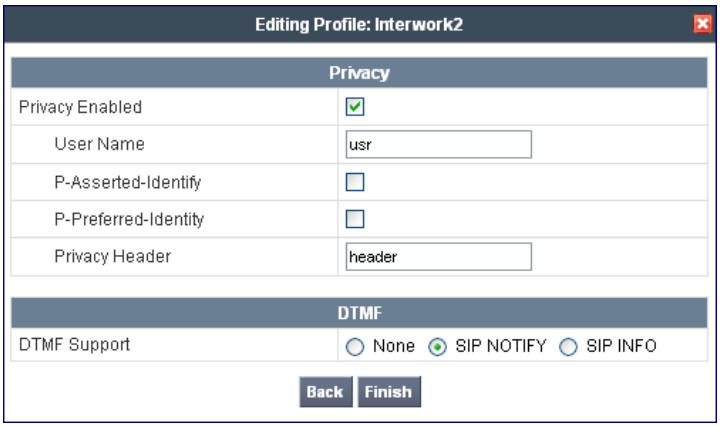


Figure 8-33. Editing Profile Pop-up Window.

5. Edit the desired fields and click **Finish**.
   Your changes are saved and the **Interworking** screen is redisplayed.

Editing the URI Manipulation and Header Manipulation Parameter Tabs

In addition to being added and edited, the contents of the **URI Manipulation** and **Header Manipulation** parameter tabs can also be deleted. Each of these procedures is provided in the following sections.

Adding a New Regex Expression

1. In the Content Area, click the **URI Manipulation** tab.
   The existing Regex entries are displayed.
2. Click **Add Regex**.
   The **Add Regex** pop-up window is displayed (Figure 8-34).

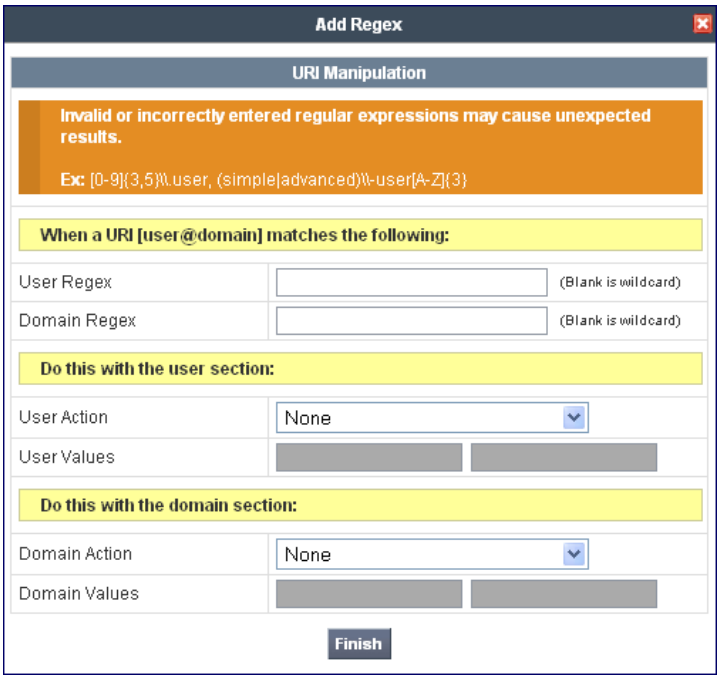


Figure 8-34. Add Regex Expression Pop-up Window.

3. Enter the requested information into the appropriate fields (Table 8-9). Selecting **Cancel** clears the fields and closes the pop-up window.

Table 8-9. Add Regex Expression Pop-up Window Field Descriptions.

Field	Description
	URI Manipulation
User Regex	The Regex rule to be used to match the User field in the SIP message.
Domain Regex	The Regex rule to be used to match the Domain field in the SIP message.
User Action	The action to be taken by the E-SBC security device if a **User Regex** match is found. Available selections are contained in a drop-down menu.
User Values	The values to be used in the manner directed by the **User Action** field.
Domain Action	The action to be taken by the E-SBC security device if a **Domain Regex** match is found. Available selections are contained in a drop-down menu.
Domain Values	The values to be used in the manner directed by the **Domain Action** field.

4. Click **Finish**.
   The new Regex expression is added to the Content Area and the **URI Manipulation** screen is redisplayed (Figure 8-35).

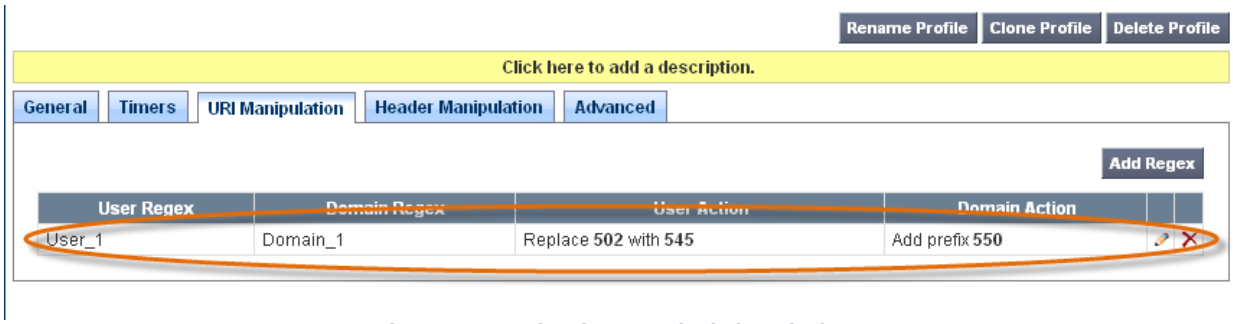


Figure 8-35. Updated URI Manipulation Display.

Editing an Existing Regex Expression

1. In the Content Area, click the **URI Manipulation** tab.
   The existing Regex entries are displayed.
2. Click the **Edit** icon corresponding to the Regex expression you want to edit.
   The **Edit Regex** pop-up window is displayed (Figure 8-36).

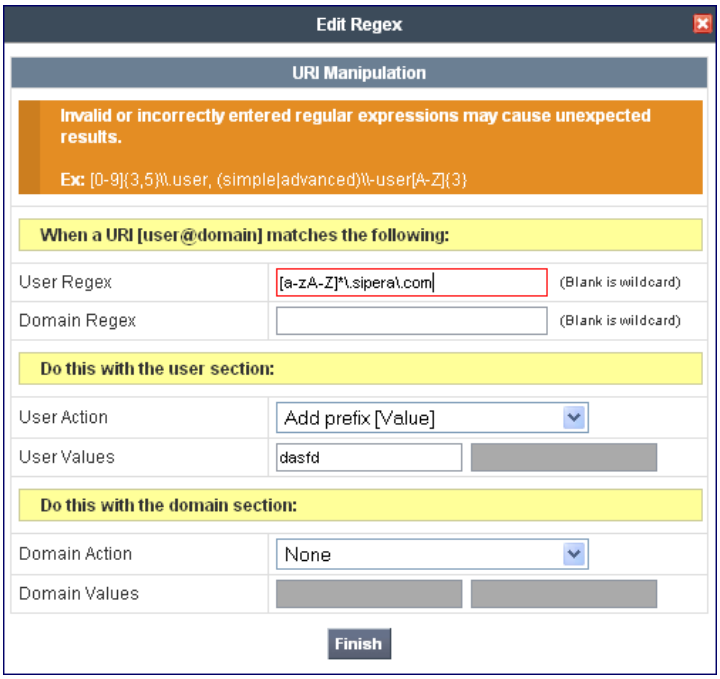


Figure 8-36. Edit Regex Pop-up Window.

3. Edit the desired fields and click **Finish**.
   The changes to the Regex expression are saved and the **URI Manipulation** screen is redisplayed.

Deleting an Existing Regex Expression

1. In the Content Area, click the **URI Manipulation** tab.
   The existing Regex entries are displayed.
2. Click the **Delete** icon corresponding to the Regex expression you want to delete.
   A **Delete Confirmation** pop-up window, similar to that shown in Figure 8-37 is displayed.

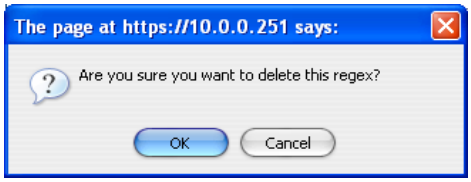


Figure 8-37. Delete Confirmation Pop-up Window.

3. Click **OK**.
   The Regex expression is deleted.

Adding New Header Manipulation Parameters

1. In the Content Area, click the **Header Manipulation** tab.
   The existing parameter entries are displayed.
2. Click **Add Parameter.**
   The **Add Parameter** pop-up window is displayed (Figure 8-38).
   Enter the requested information into the appropriate fields (Table 8-10).
   Selecting **Cancel** clears the fields and closes the pop-up window.

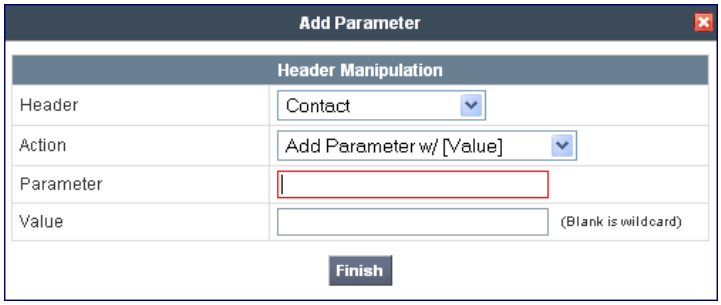


Figure 8-38. Add Parameter Pop-up Window.

Table 8-10. Add Parameter Pop-up Window Field Descriptions.

Field	Description
	Header Manipulation
Header	The SIP header field to be manipulated. Available selections are contained in a drop-down menu.
Action	The action to be performed. Available selections are contained in a drop-down menu.
Parameter	The parameter to be used in the action performed by the **Action** field.
Value	The value of the parameter defined in the **Parameter** field.

3. Click **Finish**.

The new header manipulation parameters are added to the Content Area and the **Header Manipulation** screen is redisplayed (Figure 8-39).

Figure 8-39. Updated Header Manipulation Display.

Editing Header Manipulation Parameters

1. In the Content Area, click the **Header Manipulation** tab.
   The existing parameter entries are displayed.
2. Click the **Edit** icon corresponding to the parameters you want to edit.
   The **Edit Parameter** pop-up window is displayed (Figure 8-40).

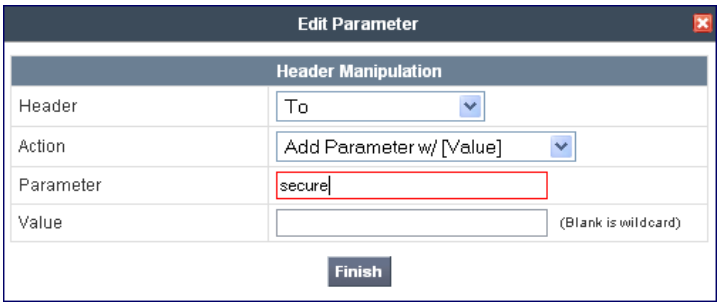


Figure 8-40. Edit Parameter Pop-up Window.

3. Edit the desired fields according to the information contained in
4. Table 8-10 and click **Finish**.
   The changes to the header manipulation parameters are saved and the **URI Manipulation** screen is redisplayed (Figure 8-41).

Figure 8-41. Updated Header Manipulation Parameters Display.

Deleting Header Manipulation Parameters

1. In the Content Area, click the **Header Manipulation** tab.
   The existing parameter entries are displayed.
2. Click the **Delete** icon corresponding to the parameters you want to delete.
   A **Delete Confirmation** pop-up window, similar to that shown in Figure 8-42 is displayed.

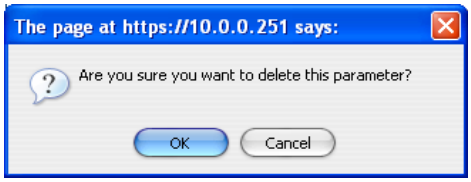


Figure 8-42. Delete Confirmation Pop-up Window.

3. Click **OK**.
   The header manipulation parameters are deleted.

Cloning an Existing Interworking Profile

Use the following procedure to clone (make an exact copy of) an existing Interworking profile.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Interworking** function of the **Global Profiles** feature from the Task Pane.
3. In the Application Pane, select the interworking profile you want to clone.
4. In the Content Area, click **Clone Profile**.
   The **Clone Profile** pop-up window is displayed (Figure 8-43).

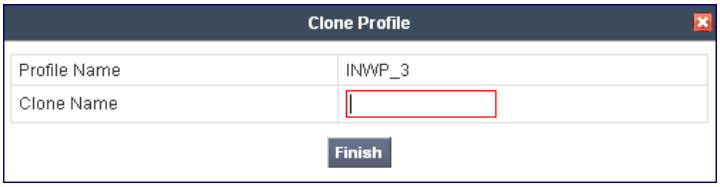


Figure 8-43. Clone Profile Pop-up Window.

5. Enter a name for the cloned **Finish**.
   The profile is copied, renamed, and saved and the **Interworking** screen is redisplayed (Figure 8-44).

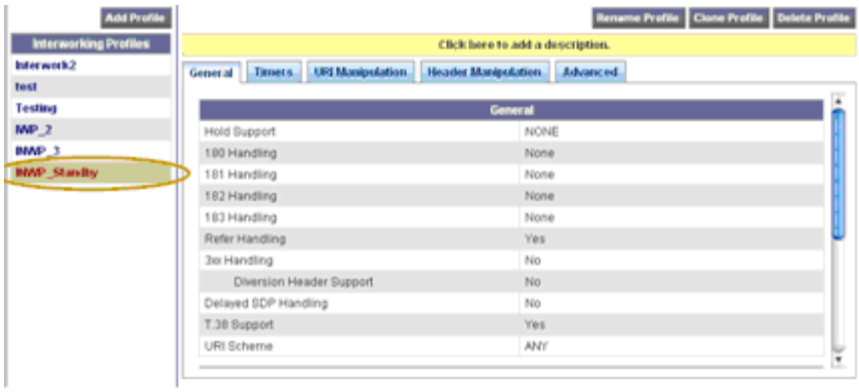


Figure 8-44. Updated interworking Display.

Renaming an Existing Interworking Profile

Use the following procedure to rename an existing Interworking profile.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Interworking** function of the **Global Profiles** feature from the Task Pane.
3. In the Application Pane, select the interworking profile you want to rename.
4. In the Content Area, click **Rename Profile**.
   The **Rename Profile** pop-up window is displayed (Figure 8-45).

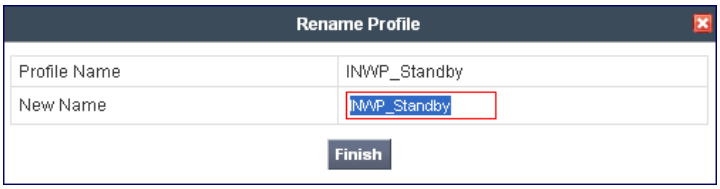


Figure 8-45. Rename Profile Pop-up Window.

5. Enter a new name for profile and click **Finish**.
   The profile is renamed and the **Interworking** screen redisplayed (Figure 8-46).

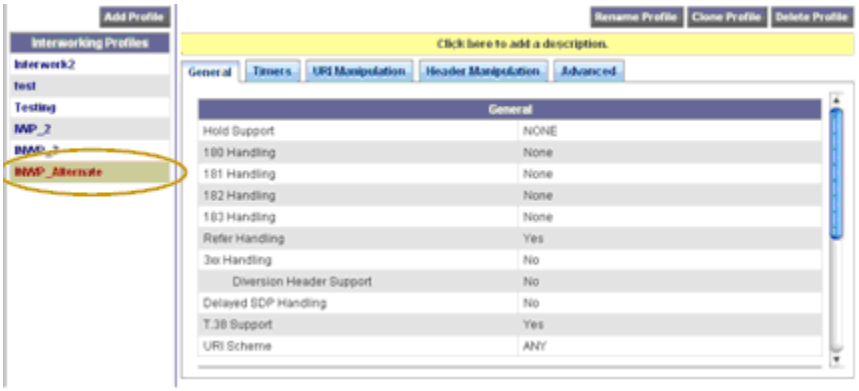


Figure 8-46. Updated Interworking Display.

Deleting an Existing Interworking Profile

Use the following procedure to delete an existing **Interworking** profile.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Interworking** function of the **Global Profiles** feature from the Task Pane.
3. In the Application Pane, select the interworking profile you want to delete.
4. In the Content Area, click **Delete Profile**.
   A **Delete Confirmation** pop-up window, similar to that shown in Figure 8-47 is displayed.

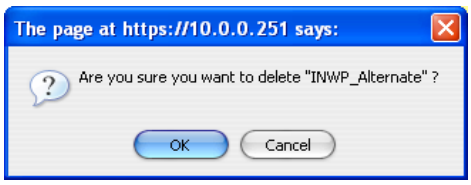


Figure 8-47. Delete Confirmation Pop-up Window.

Managing E-SBC Network Interfaces

The **Network Management** function of the **Device Specific Settings** feature allows you to configure the network interface settings affecting the E-SBC security devices deployed throughout the enterprise. Rather than following the network's interpretation of what the 'best path' to reach a destination is, source-based routing essentially follows the path specified in the IP header. One benefit of source-based routing is that it allows for multiple gateways but at the expense of not supporting custom routes.

Note Current E-SBC configuration capabilities allow for the configuration of only one input interface and one output interface.

Note Source-based routing essentially over-rides normal E-SBC routing protocols, thus requiring an intimate knowledge of the VoIP network topology to be effective.

When an E-SBC security device is installed using the **System Management** feature (see Chapter 4. *Device Configuration*), certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various **Network Management** tab displays, which can be edited as needed to optimize device performance and network efficiency.
Use the following procedure to manage E-SBC network interface parameters.

Viewing Network Interface Settings

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Network Management** function of the **Device Specific Settings** feature from the Task Pane (Figure 8-48).
   The **Network Management** screen is displayed.

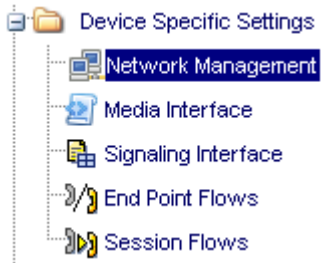


Figure 8-48. Device Specific Settings - Network Management Selection

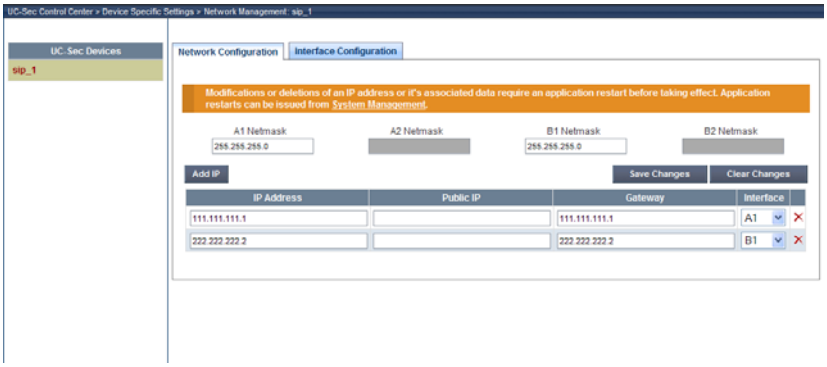


Figure 8-49. Network Management Display

Editing Network Management Parameters

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Network Management** function of the **Device Specific Settings** feature from the Task Pane (Figure 8-48).
3. In the Application Pane, select the E-SBC security device whose network parameters you want to edit (sample security device file **SipTest** provided in this example).
4. In the Content Area, select the parameter tab (**Network Configuration** or **Interface Configuration**) that you want to edit (Figure 8-49).
5. Edit the various fields using the procedures contained in the following sections.

Editing the Network Configuration Tab

Adding a New Network Interface

1. In the **Content Area** on the **Network Configuration** tab, click the **Add IP** button
   A blank IP Address / Public IP information line is added to the bottom of the IP Address display area (Figure 8-50).

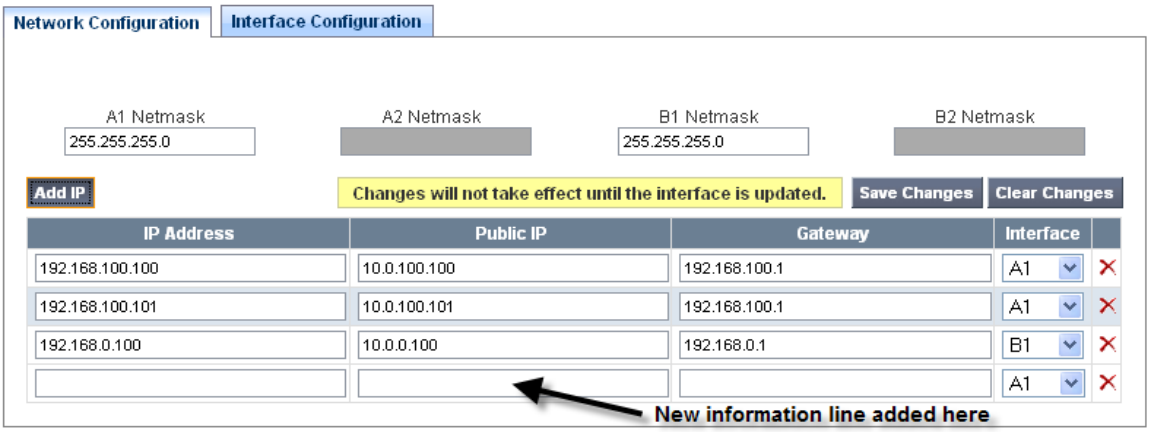


Figure 8-50. Add IP Information Line

Enter the requested information into the appropriate fields in the new information line according to the information in Table 8-11. Be sure to provide the necessary **Netmask** information, if the **Netmask** field is activated.

2. After entering the appropriate field information, select **Save Changes** in the information screen (Figure 8-51) to save and submit the updates.

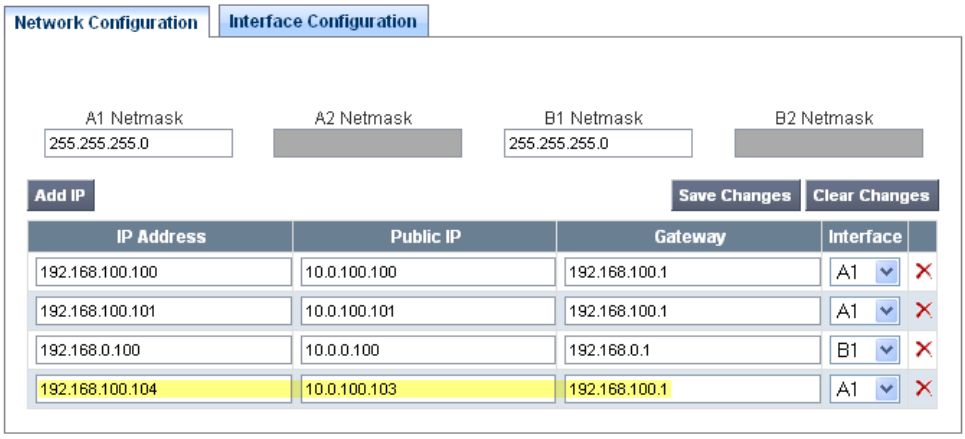


Figure 8-51. Information Fields Completed

A **Confirmation** pop-up window is displayed asking you to confirm your selection (Figure 8-52).

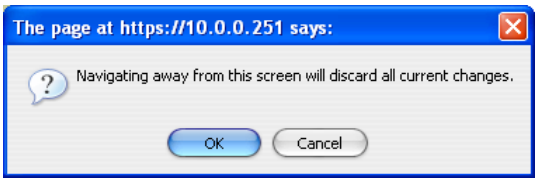


Figure 8-52. Confirmation Pop-up Window.

Table 8-11. E-SBC Interface Addressing Field Descriptions.

Field	Description
Netmask	The subnet mask to which the E-SBC security device is assigned.
IP Address	The IP address of the physical E-SBC interface.
Public IP	The publically-reachable IP address of the physical E-SBC interface.
Interface	A drop-down menu from which you select the specific physical interface of the E-SBC security device being defined.

Editing an Existing Network Interface

1. In the Content Area, make the desired changes to the existing information in the **Netmask, IP Address, Public IP** and **Interface** fields according to the information contained in

2. Table 8-11.
3. Select **Save Changes** in the information screen (Figure 8-51) to save and submit the updates.
   The IP and interface information is saved and the **Network Configuration** screen will be redisplayed with the updated information.

Deleting an Existing Network Interface

1. In the Content Area, click the **Delete** ✕ icon (located on the right-hand edge of each information row) corresponding to the E-SBC interface that you want to delete.
   A **Delete Confirmation** pop-up window is displayed, similar to that shown in Figure 8-53, asking you to confirm your selection.

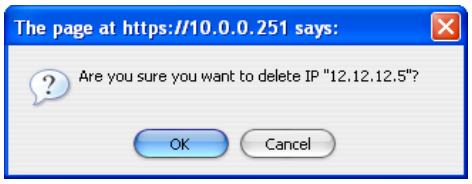


Figure 8-53. Delete Confirmation Pop-up Window.

2. Click **OK**.
   The interface is deleted and the **Network Management** screen will be redisplayed with the selected interface information removed.

Editing the Administrative State of the Interface Configuration

The administrative state of interface configurations can either be enabled or disabled. Use the following procedure to toggle the administrative state of an interface configuration.

1. In the Content Area, click the **Toggle State** button that corresponds to the physical interface on the E-SBC security device whose state you want to enable/disable (Figure 8-54), and the **Administrative Status** of the interface is changed to the opposite state.

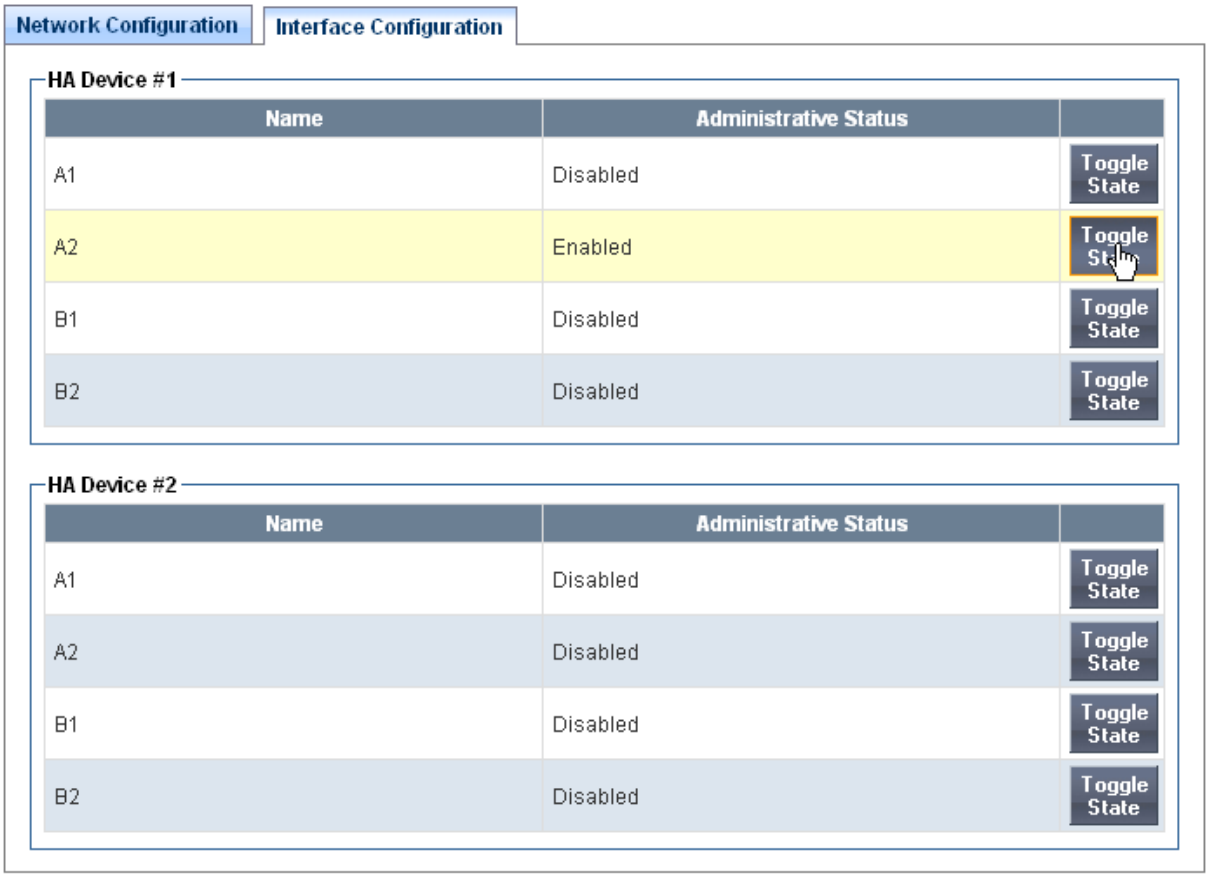


Figure 8-54. Toggling the Administrative State of an Interface Configuration.

Managing TLS Parameters

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. E-SBC security products utilize TLS primarily to facilitate secure communications with remote users.
Managing TLS parameters consists of generating and installing a Certificate Signing Request (CSR), installing a Certificate Authority (CA) certificate, and installing the Certificate Revocation List (CRL). Once these procedures are completed, you must create a client profile and a server profile.
The procedures required to perform these procedures are contained in the following sections.

Managing Certificate Signing Requests (CSRs)

This section provides procedures for creating Certificate Revocation Lists (CRLs) and for installing certificates, CA certificates, and CSRs.

Installing Certificates

Use the following procedures to install a certificate.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Certificates** function of the **TLS Management** feature from the Task Pane.
   The **TLS Management: Certificates** screen (Figure 8-55) is displayed,

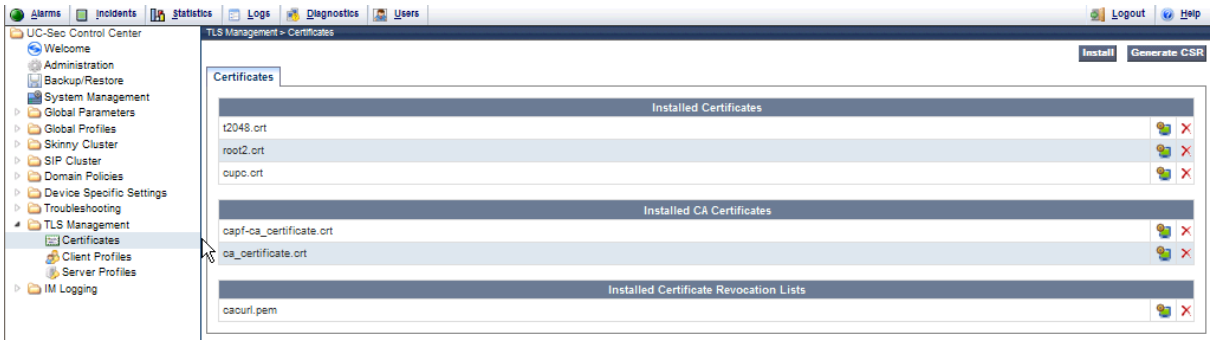


Figure 8-55. TLS Management Certificates Screen.

3. The TLS Management Certificates screen contains three sections: **Certificates**, **CA Certificates**, and **Certificate Revocation Lists (CRLs)**. These sections are described in Table 8-12 below.

Table 8-12. TLS Certificates Screen Field Descriptions.

Field	Description
Certificates	The available CSRs which can be sent by system subscribers to a Certificate Authority (CA) in order to apply for a digital identity certificate.
CA Certificates	The unsigned public key certificates from a Certificate Authority (CA) which vouches for the correctness of the data contained in a certificate.
Certificate Revocation Lists	The Certificate Revocation Lists (CRLs) which contain the serial numbers of CSRs which have been revoked, or are no longer valid, and should not be relied upon by any system subscriber.

Install Certificate Option

4. Select the **Install** button located in the upper-right-hand portion of the screen. The **Install Certificate** pop-up screen is displayed, similar to that shown in Figure 8-56.

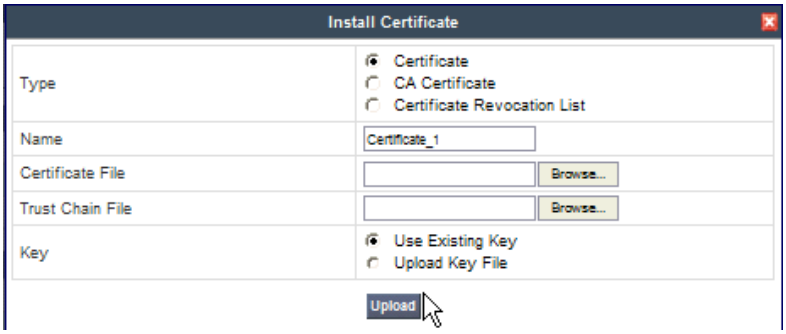


Figure 8-56. Install Certificate Pop-up screen.

5. In the Install Certificate screen (Figure 8-56), select or enter the appropriate information. Below provides descriptions of the parameter fields. There are three options for type of certificate. The screen display changes with each option selection. In the example in Figure 8-56, the top option, **Certificate**, is selected.

Table 8-13. Install Certificate Pop-up Screen Field Descriptions.

Field	Description
	Certificate Installation
Certificate Name	The name of the CSR certificate you want to install.
Certificate File	Location of the certificate on your system. Use the **Browse** feature to locate the file, if necessary.
Trust Chain File	The trust chain file used to verify the authenticity of the certificate. Use the **Browse** feature to locate the file, if necessary.
Key	The private key you want to use. You may opt to either use the existing key or select a file containing another key. Use the **Browse** feature to locate the file, if necessary.

6. Enter a certificate name in the **Name** field and then click the **Browse** buttons to navigate to the **Certificate File** and **Trust Chain File**.
7. Choose one of the two **Key** options: **Use Existing Key** or **Upload Key File**.
8. Click the **Upload** button.

Install CA Certificate Option

9. In the Install Certificate screen (Figure 8-56), there are three options for type of certificate. The screen display changes with each option selection. In the example below in Figure 8-57, the middle option, **CA Certificate**, is selected.

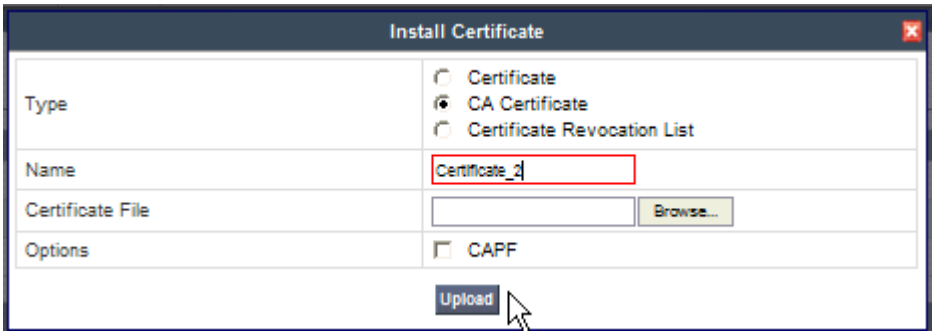


Figure 8-57. Install CA Certificate Pop-up screen.

10. Select or enter the appropriate information in the Install CA Certificate screen (Figure 8-57). The parameter field descriptions are provided in Table 8-14 below.

Table 8-14. CA Certificate Screen Field Descriptions.

Field	Description
	CA Certificate Installation
Name	Name of the CA file to be installed.
Certificate File	Location on your system of the CA file.
Options	Select the CAPF checkbox for support of the Certificate Authority Proxy Function (CAPF) services of Cisco Unified Communications Manager (CUCM).

Note: Beginning with E-SBC Release 4.0.4, Certificate Authority Proxy Function (**CAPF**) services of Cisco Unified Communications Manager (**CUCM**) is supported.

CAPF is used to manage the certificates on the phones including soft clients (**CUCIMOC** and IP Communicator).

11. Enter a certificate name in the **Name** field and then click the **Browse** buttons to navigate to the **Certificate File.**
12. Choose the **CAPF** option, if applicable.
13. Click the **Upload** button.

Install Certificate Revocation List (CRL) Option

14. In the Install Certificate screen (Figure 8-56), there are three options for type of certificate. The screen display changes with each option selection. In the example below in Figure 8-58, the lower option, **Certificate Revocation List**, is selected.

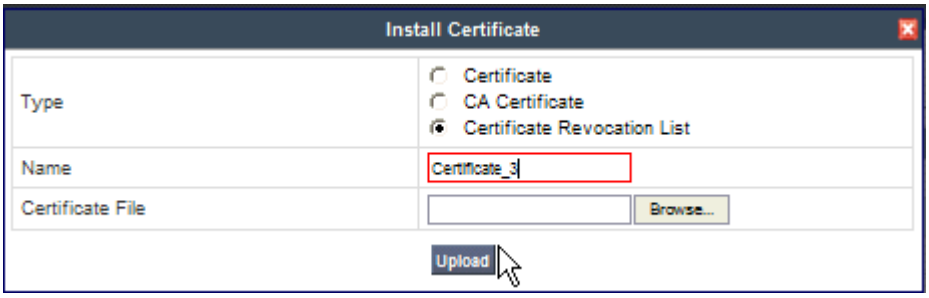


Figure 8-58. Install Certificate Revocation List Pop-up screen.

15. Select or enter the appropriate information in the Install Certificate Revocation List screen (Figure 8-58). The parameter field descriptions are provided in Table 8-15.

Table 8-15. Install CRL Screen Field Descriptions.

Field	Description
CRL Installation	
CRL Name	Name of the Certification Revocation List (CRL) file to be installed.
CRL File	Location on your system of the Certification Revocation List (CRL) file.

16. Enter a certificate name in the **Name** field and then click the **Browse** buttons to navigate to the **Certificate File.**
17. Click the **Upload** button.

Creating a Certificate Signing Request (CSR)

Use the following procedures to create a Certificate Signing Request (CSR).

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Certificates** function of the **TLS Management** feature from the Task Pane. The **TLS Management: Certificates** screen is displayed (Figure 8-59).

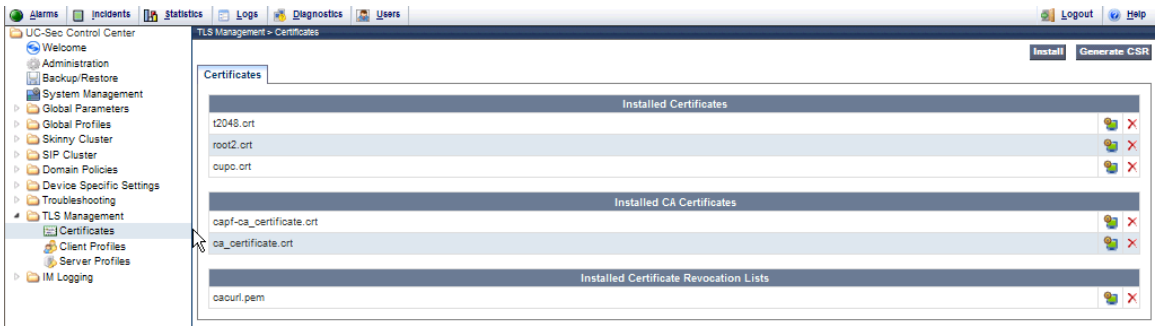


Figure 8-59. TLS Management Certificates Screen.

3. Select the **Generate CSR** button located in the upper-right-hand portion of the screen. The TLS Management Generate CSR pop-up screen (Figure 8-60) is displayed.

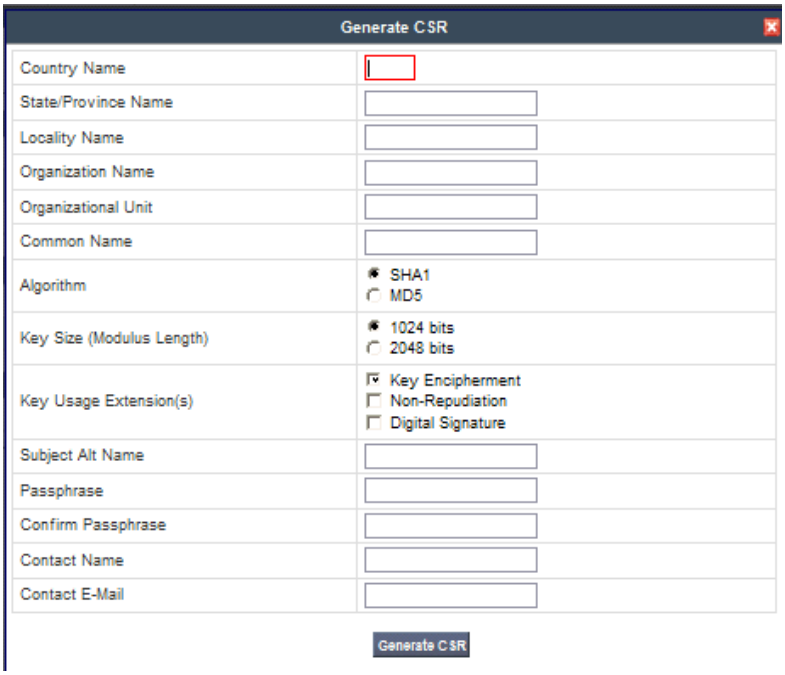


Figure 8-60. TLS Management Generate CSR Screen.

4. Enter the appropriate information in the TLS Management Generate CSR screen (Figure 8-60) and then click the **Generate CSR** button at the bottom of the screen to create the Certificate Revocation List. The parameter field descriptions are provided in Table 8-16 below.

   Figure 8-61 and Figure 8-62 provide examples of a completed TLS Management Generate CSR screen with parameters entered and the resulting display after clicking on the **Generate CSR** button.

Table 8-16. TLS Management Generate CSR Screen Field Descriptions.

Field	Description
	Certificate Signing Request
Country Name	Name of the country within which the certificate is being created.
State/Province Name	The state/province where the certificate is being created.
Locality Name	The locality (city) where the certificate is being created.
Organization Name	The name of the company or organization creating the certificate.
Organizational Unit	The group within the company or organization creating the certificate.

Field	Description
Common Name	The name used to refer to or identify the company or group creating the certificate.
Algorithm	The hash algorithms (**MD5** or **DSA**) to be used with the RSA signature algorithm.
Key Size (Modulus Length)	The certificate key length (**1024** or **2048**) in bits.
Key Usage Extension	The purpose for which the public key may be used: **Key Encipherment**, **Non-Repudiation**, **Digital Signature**.
Subject Alt Name	Optional text field which can be used to further identify this certificate.
Passphrase	Password used when encrypting the private key.
Repeat Passphrase	A verification field for the **Passphrase**.
Contact Name	Individual within the issuing organization acting as point-of-contact for issues relating to this certificate.
Contact E-mail	E-mail address of the **Contact**.

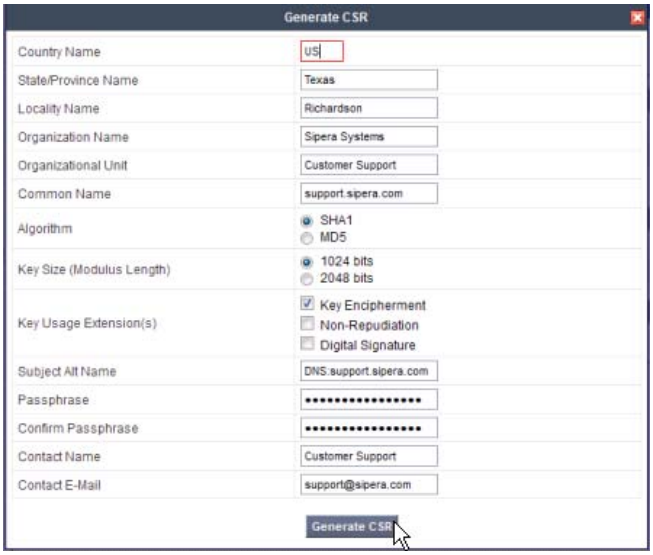


Figure 8-61. Sample Completed TLS Management Generate CSR Screen.

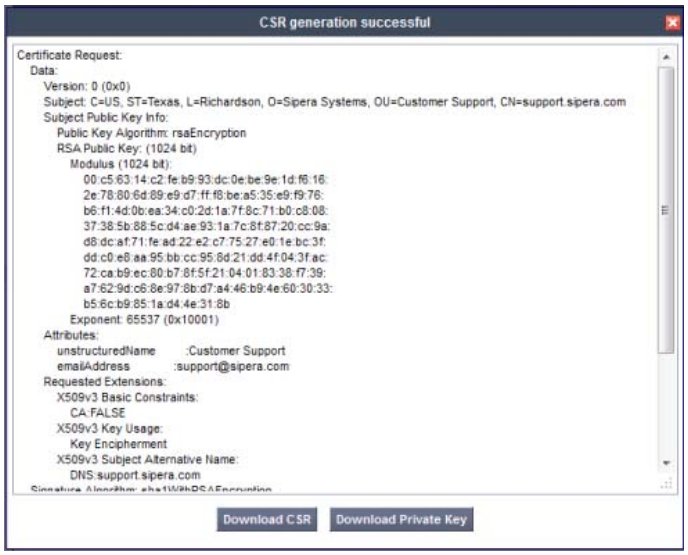


Figure 8-62. Sample CSR Display

Managing Client Profiles

Use the following procedures to create, edit, and delete TLS client profiles.

Creating a New Client Profile

Use the following procedure to create a new TLS client profile.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Client Profiles** function of the **TLS Management** feature from the Task Pane.
   The **Client Profiles** screen is displayed (Figure 8-63).
3. Select **New Profile**.
   The **New TLS Client Profile** pop-up window is displayed (Figure 8-64).

Figure 8-63. TLS Client Profiles Screen.

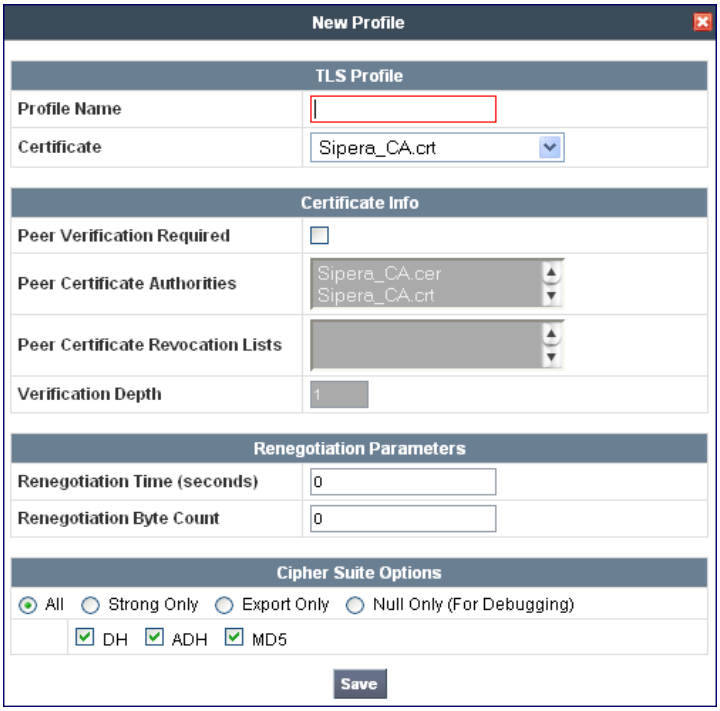


Figure 8-64. New TLS Client Profile Pop-up Screen.

4. Enter the requested information into the appropriate fields.

Table 8-17. TLS Client Profile Pop-up Screen Field Descriptions.

Field	Description
TLS Profile	
Profile Name	Descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
Certificate Info	

Peer Verification Required	Checkbox indicating whether or not peer verification is required. If this box is checked (☑), then peer verification is required and the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields become active. If this box remains unchecked (☐), then peer verification is *not* required and the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields become inactive (grayed-out).
Peer Certificate Authorities	Certificates to be used for peer verification. Using Ctrl+Shift, any combination of selections can be made from this list.
Peer Certificate Revocation Lists	Revocation lists that are to be used to verify whether or not a peer certificate is valid. Using Ctrl+Shift, any combination of selections can be made from this list.
Verification Depth	Maximum depth used for the certificate chain verification.
Renegotiation Parameters	
Renegotiation Time (optional)	The amount of time after which the certificate is renegotiated.
Renegotiation Byte Count (optional)	The number of bytes after which the certificate is renegotiated.
Cipher Suite Options	
Cipher Suites	The level of security to be used for encrypting data. Available selections are: *All* — Support all cipher suite options. *Strong Only* — Encryption support that is strong enough for most business or government needs. For use within the United States only. *Export Only* — The strongest level of encryption allowed by federal law for exportable products. *Null Only* — Weakest level of encryption. Only used for debugging. *DH* — Diffie-Hellman key exchange. *ADH* — Authenticated Diffie-Hellman. *MD5* — Message Digest algorithm 5.

5. Select **Save**.
   The TLS client profile is installed and displayed (Figure 8-65).

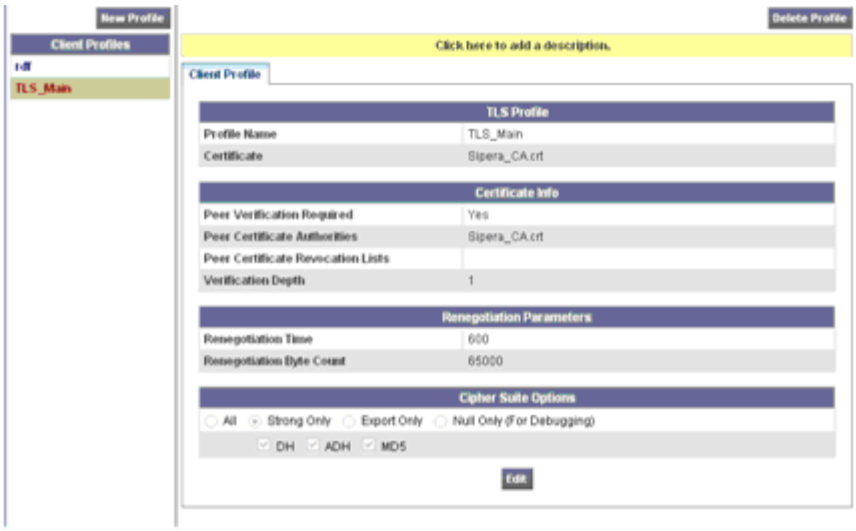


Figure 8-65. Updated Client Profiles Screen.

Editing a Client Profile

Use the following procedure to edit an existing TLS client profile.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Client Profiles** function of the **TLS Management** feature from the Task Pane.
   The **Client Profiles** screen is displayed (Figure 8-65).
3. From the Applications Pane, select client profile you want to edit.
   The configuration of the selected client profile is displayed in the Content Area.
4. From the Content Area, select **Edit**.
   The **Edit TLS Client Profile** pop-up window is displayed (Figure 8-66).

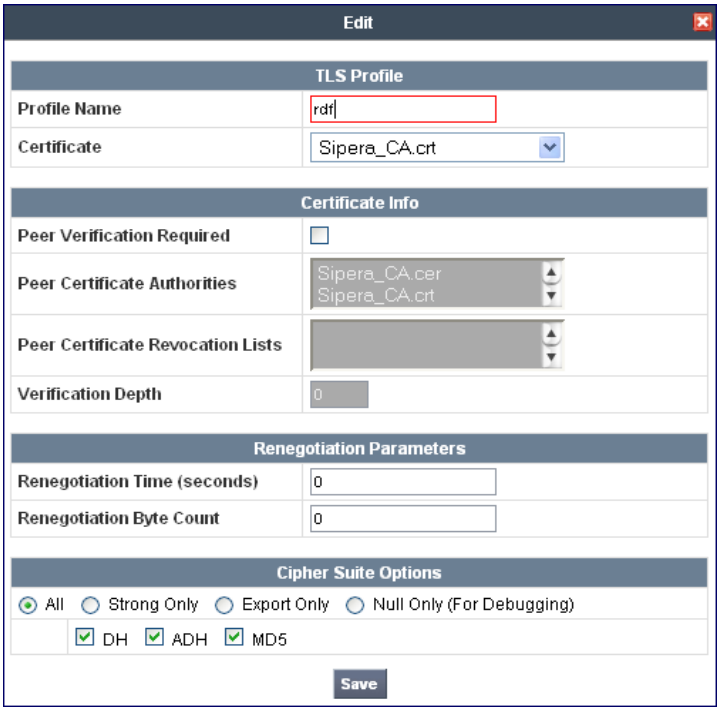


Figure 8-66. Edit TLS Client Profile Pop-up Window.

5. Edit the desired fields and select **Save** to save your changes or **Cancel** to revert to the previous field values and close the window. If necessary, refer back to Table 8-17 for a description of the fields contained on the **TLS Client Profile** pop-up window.

Deleting a Client Profile

Use the following procedure to delete an existing TSL client profile.

Caution! At least one TLS client profile must be configured for the TLS feature to function properly.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Client Profiles** function of the **TLS Management** feature from the Task Pane. The **Client Profiles** screen is displayed (Figure 8-65).
3. From the Applications Pane, select client profile you want to delete.
4. From the Content Area, select **Delete Profile**. A delete confirmation pop-up window similar to that shown in Figure 8-67 is displayed asking you to confirm your selection.

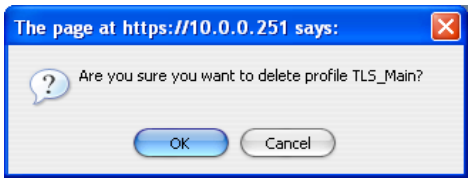


Figure 8-67. Delete Confirmation Pop-up Window.

5. Select **OK**.
   The TLS client profile is deleted.

Managing Server Profiles

Use the following procedures to create, edit, and delete TLS server profiles.

Creating a New Server Profile

Use the following procedure to create a new TLS server profile.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Server Profiles** function of the **TLS Management** feature from the Task Pane.
   The **Server Profiles** screen is displayed.
3. From the Applications Pane, select **New Profile**.
   The **TLS Server Profile** pop-up window is displayed (Figure 8-69).
4. Enter the requested information into the appropriate fields. Table 8-18 provides a description of each of the fields.

Figure 8-68. Server Profiles Screen.

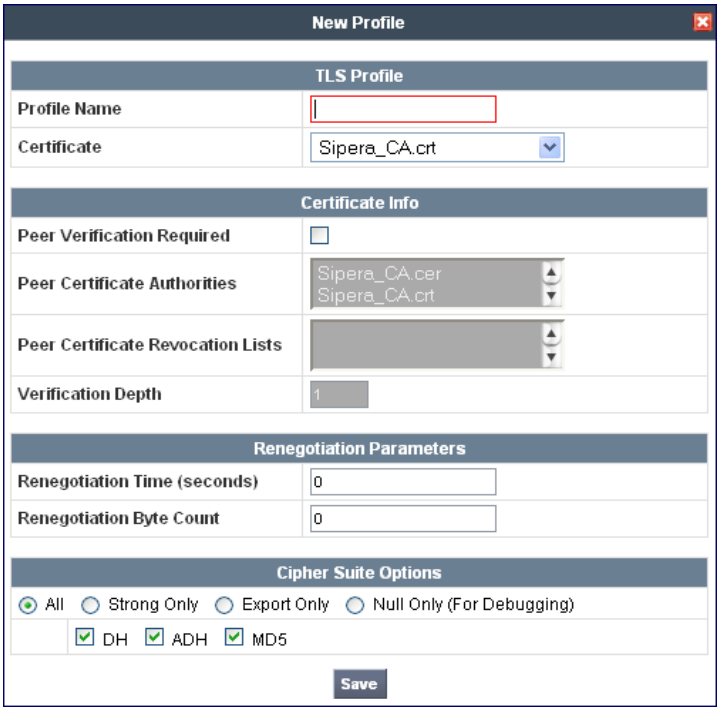


Figure 8-69. TLS Server Profile Pop-up Window.

Table 8-18. New TLS Server Profile Pop-up Window Field Descriptions.

Field	Description
	TLS Profile
Profile Name	Descriptive name used to identify this profile.
Certificate	The certificate presented when requested by a peer.
Certificate Info	
Peer Verification Required	Checkbox indicating whether or not peer verification is required. If this box is checked (☑), then peer verification is required and the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields become active. If this box remains unchecked (☐), then peer verification is *not* required and the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields become inactive (grayed-out).
Peer Certificate Authorities	Certificates to be used for peer verification. Using Ctrl+Shift, any combination of selections can be made from this list.
Peer Certificate Revocation Lists	Revocation lists that are to be used to verify whether or not a peer certificate is valid. Using Ctrl+Shift, any combination of selections can be made from this list.
Verification Depth	Maximum depth used for the certificate chain verification.
	Renegotiation Parameters

Renegotiation Time (optional)	The amount of time after which the certificate is renegotiated.
Renegotiation Byte Count (optional)	The number of bytes after which the certificate is renegotiated.
Cipher Suite Options	
Cipher Suites	The level of security to be used for encrypting data. Available selections are: *All* – Support all cipher suite options. *Strong Only* – Encryption support that is strong enough for most business or government needs. For use within the United States only. *Export Only* – The strongest level of encryption allowed by federal law for exportable products. *Null Only* – Weakest level of encryption. Only used for debugging. *DH* – Diffie-Hellman key exchange. *ADH* – Authenticated Diffie-Hellman. *MD5* – Message Digest algorithm 5.

5. Select **Save**.
   The TLS Server profile is created, installed, and listed in the Applications Pane with its configuration displayed in the Content Area.

Editing a Server Profile

Use the following procedure to edit the TLS server profile.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Server Profiles** function of the **TLS Management** feature from the Task Pane.
   The **Server Profiles** screen is displayed (
   Figure 8-68).
   The configuration of the server profile is displayed in the Content Area.
3. From the Content Area, select **Edit**.
   The **Edit TLS Server Profile** pop-up window is displayed (Figure 8-70).

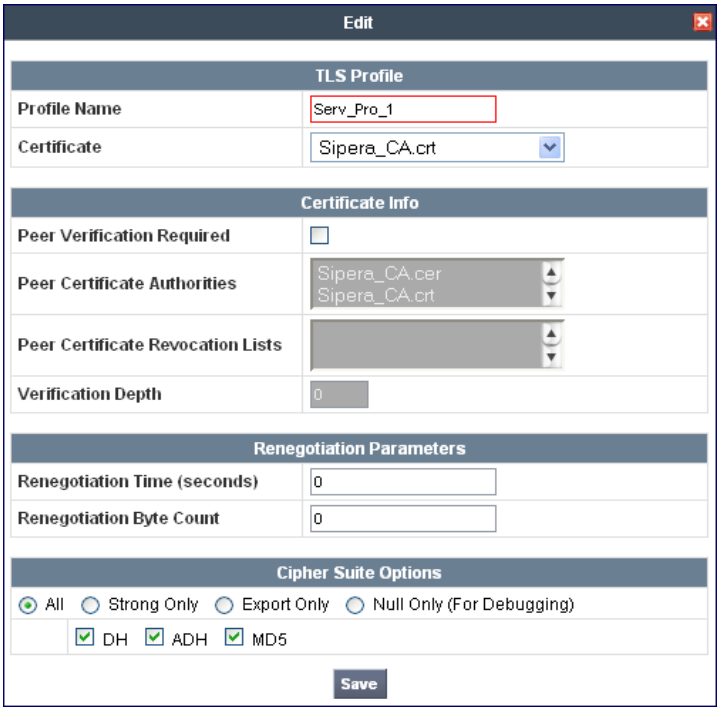


Figure 8-70. Edit TLS Server Profile Pop-up Window.

4. Edit the desired fields and select **Save** to save your changes or **Cancel** to revert to the previous field values and close the window.
   If necessary, refer back to Table 8-18 for a description of the fields contained on the **TLS Server Profile** pop-up window.

Deleting a Server Profile

Use the following procedure to delete an existing TSL server profile.

Caution! One TLS server profile must be configured for the TLS feature to function properly.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Server Profiles** function of the **TLS Management** feature from the Task Pane.
   The **Server Profiles** screen is displayed (Figure 8-68).
3. From the Content Area, select **Delete Profile**.
   A **Delete Confirmation** pop-up window similar to that shown in Figure 8-71 is displayed asking you to confirm your selection.

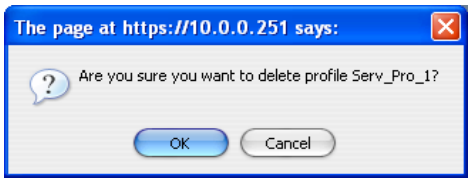


Figure 8-71. Delete Confirmation Pop-up Window.

4. Select **OK**.
   The TLS server profile is deleted.

This page intentionally left blank.

System Monitoring 9

This chapter describes how to use various aspects of the E-SBC Control Center (EMS) to monitor the current security activity of the VoIP network using the **Welcome, Alarms, Incidents, Statistics, Logs, Diagnostics,** and **Users** screens.
For information on logging into the E-SBC Control Center and for detailed descriptions of the different windows and screens, refer to the section *E-SBC Control Center Screen Descriptions* in Chapter 2, *Getting Started*.

Welcome Screen

The **Welcome** screen (Figure 9 - 1) is the top-level display screen which provides direct access to all the features, functions, and information available on the current release of the E-SBC security system. From this screen you can display additional, separate, summary windows (**Alarms, Incidents, Statistics, Logs, Diagnostics,** and **Users**) which contain active, up-to-the-minute alarms, incident, statistical, log, diagnostic, and user information as well as review and exchange textual messages with other administrative user accounts.
The Content Area of the **Welcome** screen contains various summary areas which display top-level, system-wide information such as which alarms and incidents are currently active, links to available **Quick Links**, a list of installed E-SBC security devices, E-SBC device deployment information, and an area for viewing and exchanging text messages with other administrators.

Figure 9 - 1. E-SBC Control Center - Welcome Screen.

Table 9-1 provides a brief description of each portion of the Content Area of the E-SBC **Welcome** screen.

Table 9-1. Dashboard Alarm and Event Reporting Component Descriptions.

Component	Description
Welcome Information	Provides a snapshot view of the E-SBC Control Center and system status information.
Available Links to External Sites	A list of active links to external Sipera-sponsored support sites.
Installed E-SBC Security Device List	A list of all E-SBC security devices currently deployed throughout the network.
Text Message Exchange Area	User-editable text message exchange area.
Current Incident List	A list of current incidents reported by the E-SBC security devices to the E-SBC Control Center (EMS).
Current System Alarm List	A list of current alarms reported by the E-SBC security devices to the E-SBC Control Center (EMS).

Managing System Alarms

Current system alarms are reported to the E-SBC Control Center and immediately displayed in two places: as a blinking red indicator on left side of the **Tool Bar** and as a corresponding text message in the **Latest Alarms** section (

Figure 9-2). These notifications provide the information necessary to clear the condition causing the alarm notification, after which time the alarm can be cleared from the display.

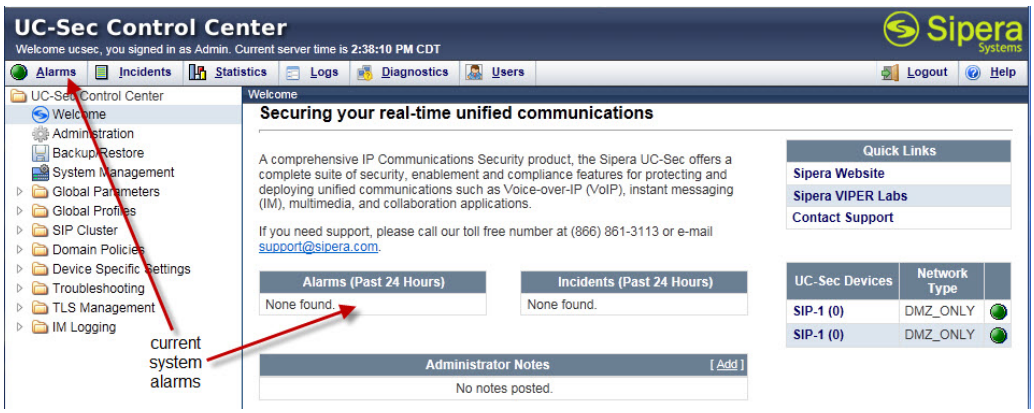
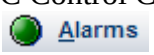


Figure 9-2. Current System Alarms Notifications.

Viewing Current System Alarms

The **Alarms** screen provides a summary display of all currently active system alarms. If no alarms are active, this display screen is blank. The **Alarms** screen is normally only accessed if the **Alarm Status Indicator** on the Toolbar indicates an alarm status (flashed red).
Use the following procedure to view current system alarms.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Alarms** 

icon from the **Toolbar** or click on the specific alarm you want to view from the **Latest Alarms** section of the **Welcome** screen.

The **Alarms** screen is displayed, similar to that shown in Figure 9-3.

Figure 9-3. Alarms Screen.

3. Select the E-SBC Device for which you want alarms displayed (Figure 9-4). All currently active alarms for selected E-SBC security device are displayed in the Content Area.

Figure 9-4. E-SBC Device-specific Alarms Screen.

Table 9-2 provides a brief description of each of the security reporting components of the **Alarms** Screen.

Table 9-2. Current Alarms Screen Field Descriptions.

Field	Description
Alarm Details	The specific / descriptive name of the active alarm.
State	Current state of the alarm: **ON** (The State field for any displayed alarm is always: **ON)**
Time	Date and time the alarm was generated.
Device	The E-SBC device which generated the alarm.
Alarm ID	Sequential, numerical identifier of the alarm being reported.

4. Clear the alarm using the appropriate clearing event from the corresponding appendix located at the back of this manual:

   Appendix C, *System Alarm List*
   Appendix D, *GUI and Console Alarm List*
   Appendix E, *Function Alarm List*
   Appendix F, *E-SBC Event List*

5. If the alarms list is long, you can use the navigation buttons at the bottom of the screen to quickly navigate to the specific alarm you are interested in viewing (Figure 9-5).
6. Delete the cleared alarm using the procedure *Deleting Current System Alarms*.

Figure 9-5. Alarms Screen Navigation Buttons.

Deleting Current System Alarms

Use the following procedure to delete current system alarms.

> **Note:** Alarms should only be deleted from the **Alarms** display after the condition which originally caused the alarm has been properly cleared by qualified personnel.
>
> Alarms can be cleared through two processes:
>
> 1. Once the failure condition is solved, an operator clears the alarm display manually depending on the alarm.
> 2. Once the failure condition is solved, no operator intervention is expected, and the alarm display clears automatically depending on the alarm.

1. From the **Alarms** screen select the **Delete** icon ✕ corresponding to the alarm notification you want to delete.
   A confirmation pop-up window similar to that shown in Figure 9-6 is displayed asking you to confirm your selection.
2. Select **OK**.
   The alarm display is cleared.

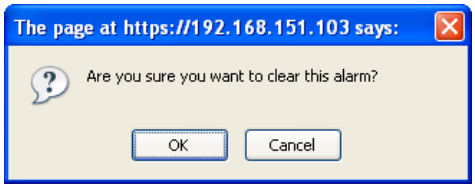


Figure 9-6. Delete Confirmation Pop-up Window.

Viewing Current System Incidents

In addition to viewing system alarms, you can view a complete descriptive list of all system incidents which have occurred since the last viewing period using the **Incident** screen. It shows the last five incidents at any point of time. This feature allows you to view system-wide incidents according to category (**DoS**, **Policy**, **Scrubbing**, etc.). When the **Incident** screen is open, all of

the latest incident information will be available, and the operator can scroll through the incidents list while displaying up to 15 incidents at one time.
Use the following procedure to view current system incidents.

> **Note** Incidents can only be viewed; they cannot be edited or deleted.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Incidents** Incidents icon from the **Toolbar** or click on the specific incident you want to view from the **Latest Incidents** section of the **Welcome** screen.
   The **Incidents** screen is displayed, similar to that shown in Figure 9-7.

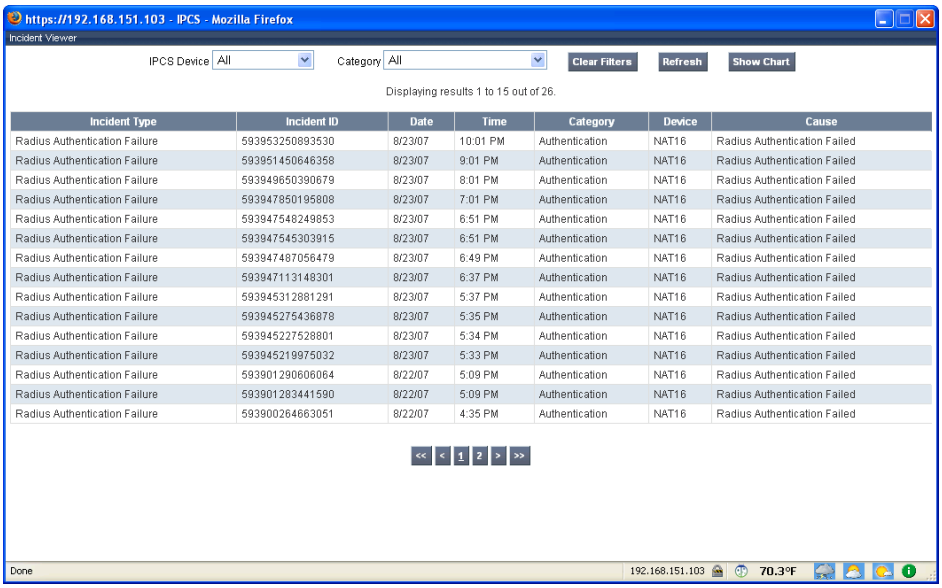


Figure 9-7. Incidents Screen.

3. Using the **E-SBC Device** and **Category** fields located at the top of the **Incidents** screen, define a search filter to find and display the particular incidents you want to view.
   The **Incident** display will change to reflect the search criteria as soon as a selection has been made. Periodically select **Refresh** to refresh the display as ensure all the desired incidents are displayed. Select **Clear Filters** to set the **E-SBC Device** and **Category** fields to **All**. This will cause all current **Incidents** to be displayed.

Incidents category selections include:

- All
- Authentication
- Black White List
- DoS

- High Availability
- Media Anomaly Detection
- Policy
- Protocol Discrepancy
- Scrubbing
- Spam
- TLS Certificate

Viewing System Statistics

The **Statistics** screen provides a snap-shot display of certain cumulative, system-wide generic and SIP-specific operational information.
The various **Statistics** tabs (**Calls**, **Policy**, and **Protocol**) can be displayed whenever up-to-date statistical information is required.

Note

Statistics information can only be viewed; it cannot be edited or deleted.

Use the following procedure to view system-wide SIP statistical information.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Statistics**

icon from the **Tool Bar**.
The **Statistics** screen is displayed, which defaults to the **Summary** tab (Figure 9-8).

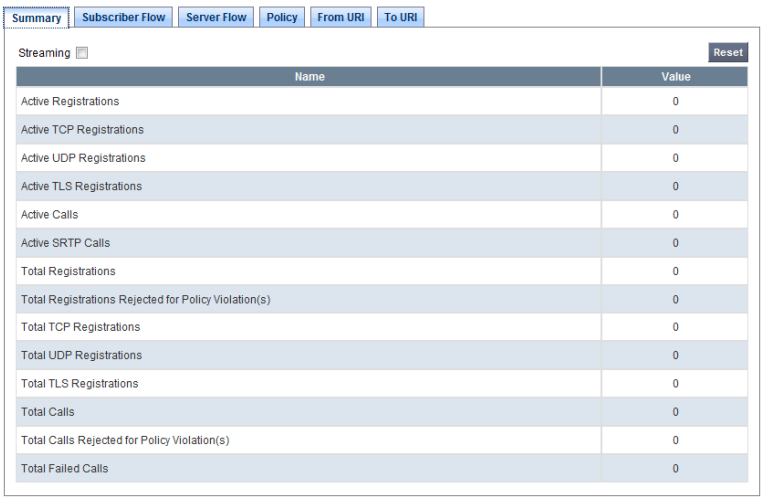


Figure 9-8. Statistics Screen: Summary Tab Display.

3. Select the specific **Statistics** tab you want to view.
The contents of each of the selected tabs will be displayed.

Viewing System Logs

The **SysLog Viewer** displays the syslog file, according to certain user-definable filtering criteria such as log type, time period, and severity. Use the following procedure to define and view syslog reports.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Logs** Logs icon from the **Tool Bar** to display the **Syslog Viewer** (Figure 9-9).

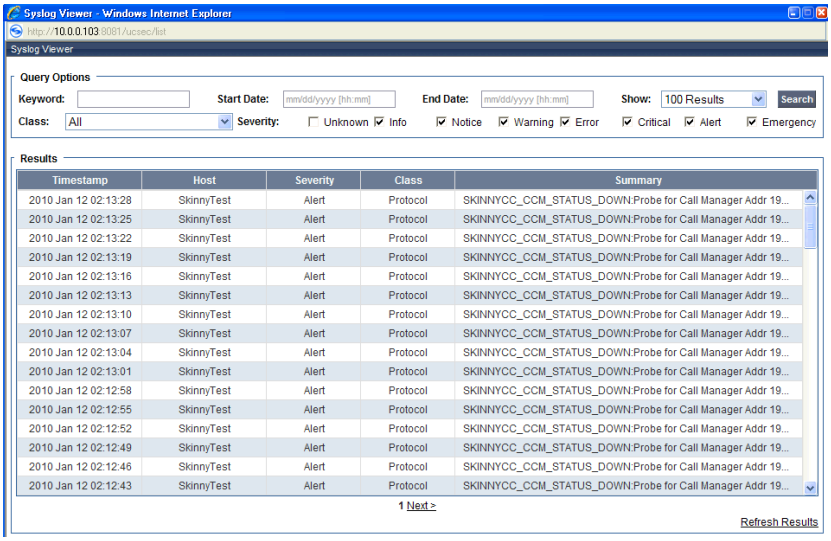


Figure 9-9. Syslog Viewer.

3. In the **Query Options** **Start Date** field and **End Date** field, You can filter the results displayed in a search report to fall within starting and ending dates and times. In previous E-SBC **Syslog Viewer** windows there were four separate fields for Start Date, Start Time, End Date, and End Time.

Note:	With E-SBC Release 4.0, the date and time entries are now combined in a single field (mm/dd/yyyy [hh:mm]) with the time entry ([hh:mm]) being optional. Also with Release 4.0, an **End Date/Time** entry is no longer required when you enter a **Start Date/Time** as in previous product releases.

4. In the **Query Options** **Keyword** field in the top-left portion of the **Syslog Viewer**, enter one or more words to define the limits of the log report and click on the **Search** button on the right-hand portion of the viewer. The report is run and a report output is displayed similar to that in the example shown in **Figure 9-10** on the next page.

Note:	In the examples shown in Figure 9-9 and Figure 9-10, the initial **Syslog Viewer** window (Figure 9-9) displays all Syslog entries, while the entries displayed in the report (Figure 9-10) are the result of a search on the two keywords “siptest” and “decrypt.” Keyword searches are case-insensitive and tokenized (each keyword term entered in the **Keyword** field will be searched for separately), but all keyword terms that are entered in the **Keyword** field must be found in a log line in order for the log line to be included and displayed within a report.

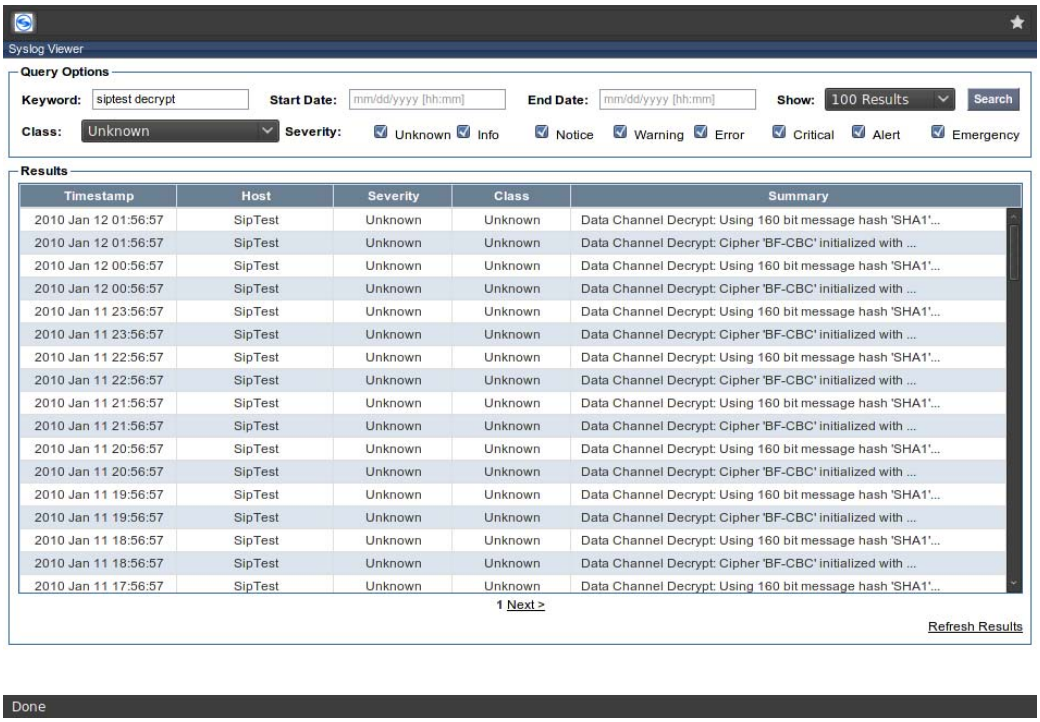


Figure 9-10. Example of Syslog Report Output.

Viewing Diagnostics Results

The **Diagnostics** screen provides a variety of tools to aid in troubleshooting E-SBC operation. Available tools include a full diagnostic test suite, as well as individual tabs to monitor certain functional aspects of the E-SBC, such as TCP and TLS activity.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Diagnostics**

icon from the **Tool Bar**.
   The **Diagnostics** screen is displayed (Figure 9-11).
3. Click the **Full Diagnostics** tab.
4. Click **Start Diagnostic**.
   The tests listed in the **Task Description** portion of the display are sequentially run, with the results of the test displayed in the **Status** column. If an error is encountered while running a particular test, the diagnostic will terminate and display the reason for the termination in the **Status** column (Figure 9-12).
5. Click the tab for any additional diagnostic test and view the results in the Content Area.

Figure 9-11. Diagnostics Display.

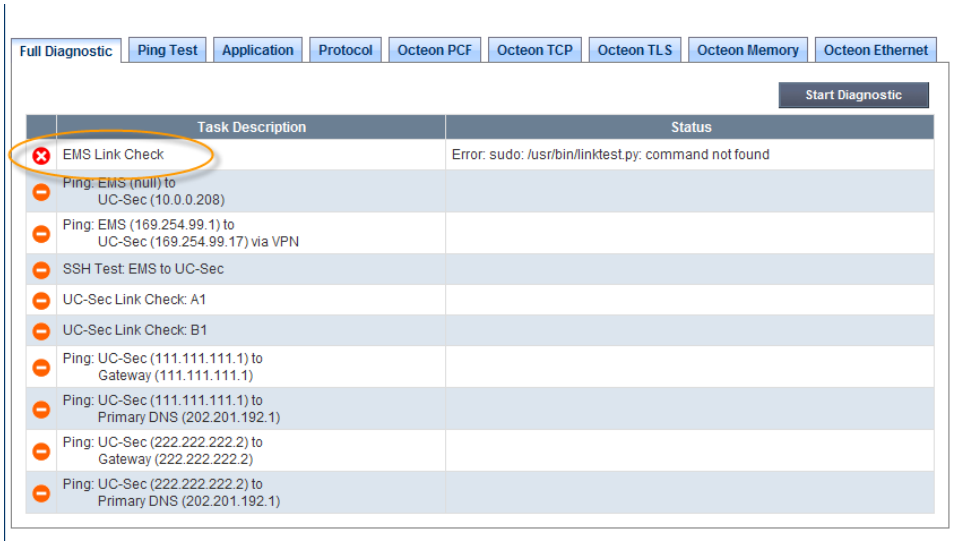


Figure 9-12. Terminated Diagnostic Display.

Viewing Administrative Users

The **Users** screen provides a summary of all active system administrative accounts currently logged into the E-SBC Control Center.

Note Logged-in Users account information can only be viewed; it cannot be modified in any way.

Use the following procedure to view which system administrative accounts are currently logged into the E-SBC Control Center.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Users** Users icon from the **Tool Bar**.
   The **Users** screen is displayed (Figure 9-13).

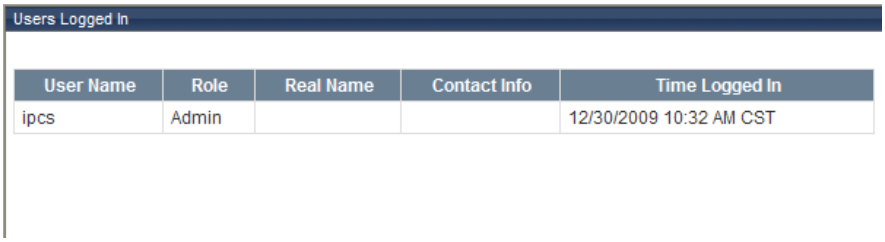


Figure 9-13. Users Screen

Trace Settings

The Trace Settings function allows you to trace an individual packet or group of packets comprising a call through the E-SBC. The information gathered shows how the packet (or call) traversed the E-SBC-secured network.

Packet Trace

The Packet Control Function (PCF) packet trace provides information on how the packet is being handled by the PCF (e.g., dropped, flow matched, actors applied, etc.). Packet trace information is sent from the PCF as log messages, which can be viewed on E-SBC in the location:
/archive/syslog/ipcs/octeon.log

Note: Refer to the section titled, "Viewing Packet Trace and Call Trace Data," for complete instructions on how to log into the E-SBC device and how to navigate to the **/archive/syslog/ipcs** directory to view the **octeon.log** file.

Use the following procedures to manage **Packet Trace** profiles.

Adding a New Packet Trace Profile

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Trace Settings** function of the **Troubleshooting** feature from the Task Pane (Figure 9-14).

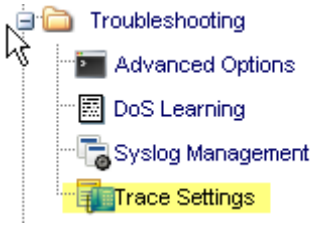


Figure 9-14. Selecting the Trace Settings Function

3. From the Applications Pane, select the E-SBC device to which you want to add a packet trace profile (Figure 9-15).
4. Select the **Packet Trace** tab, as shown in Figure 9-15

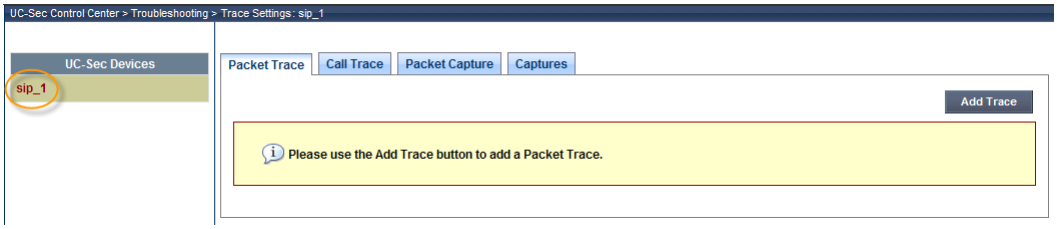


Figure 9-15. Selecting a E-SBC Device and Packet Trace Tab.

5. Select the **Add Trace** button in the upper right-hand portion of the screen. The **Add Packet Trace** pop-up window is displayed (Figure 9-16).

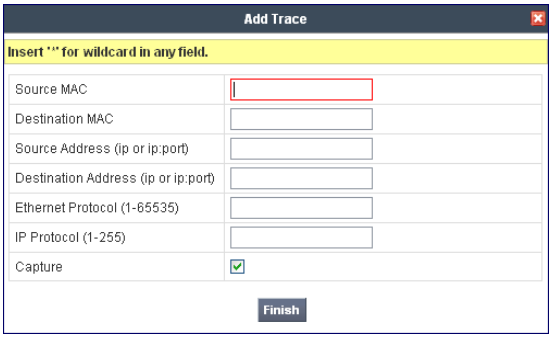


Figure 9-16. Add Packet Trace Pop-up Window

6. Enter the requested information into the appropriate fields.
   Table 9-18 describes each user-definable field displayed in the **Add Packet Trace** pop-up window.

Table 9-18. Add Packet Trace Pop-up Window Field Descriptions.

Field	Description
Source MAC	The MAC device address originating the packet to be traced.
Destination MAC	The MAC address of the device to which the packet is destined.
Source Address (ip or ip:port)	The IP address from which the packet originated.
Destination Address (ip or ip:port)	The IP address to which the packet is destined.
Ethernet Protocol **(1 – 65535)**	The Ethernet protocol of the packet.
IP Protocol (1 – 255)	The IP protocol of the packet.
Capture	Checkbox indicating whether (☑) or not (☐) the route of the packet is to be captured.

7. Select **Finish.**
   The new Packet Trace profile is displayed in the **Packet Trace** tab display. A sample Packet Trace - Updated Traces screen is shown below.

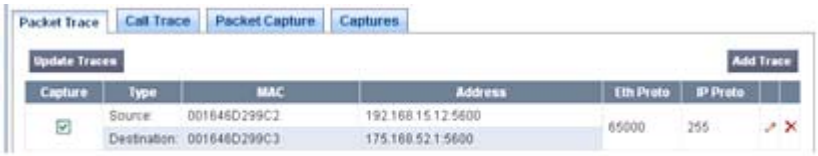


Figure 9-17. Sample Updated Packet Trace Display.

Editing an Existing Packet Trace Profile

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Trace Settings** function of the **Troubleshooting** feature from the Task Pane (Figure 9-14).
3. From the Application Pane, select the E-SBC device whose packet trace settings you want to edit, as shown previously in Figure 9-15.
   The screen defaults to the **Packet Trace** tab display.

4. Select the **Edit** icon (on the right-hand side of the screen) corresponding to the packet trace profile you want to edit.
   The **Edit Packet Trace** pop-up window is displayed (Figure 9-18).

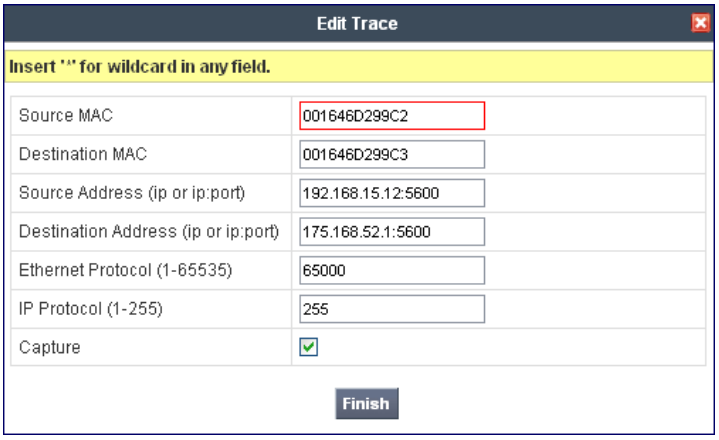


Figure 9-18. Edit Trace Pop-up Window.

5. Edit the desired fields according to the information contained in Table 9- and press **Finish** when done or **Cancel** to close the pop-up window without saving your changes.
   Your changes are saved and the **Packet Trace** profile is updated and the **Trace Settings** screen is redisplayed.

Deleting an Existing Packet Trace Profile

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Trace Settings** function of the **Troubleshooting** feature from the Task Pane (Figure 9-14).
3. From the Application Pane, select the E-SBC device whose packet trace settings you want to delete, as shown previously in Figure 9-15.
   The screen defaults to the **Packet Trace** tab display.

4. Select the **Delete** icon corresponding to the **Packet Trace** profile you want to delete (Figure 9-19).
   A confirmation pop-up window is displayed similar to that shown in Figure 9-20 asking you to confirm your decision.

5. Click **OK**.

The selected **Packet Trace** profile is deleted.

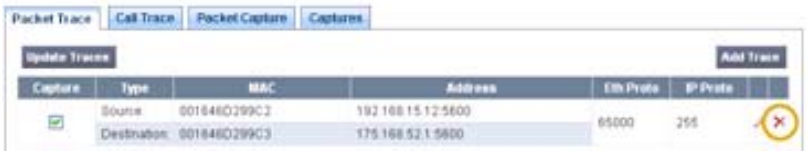


Figure 9-19. Deleting an Existing Packet Trace Profile.

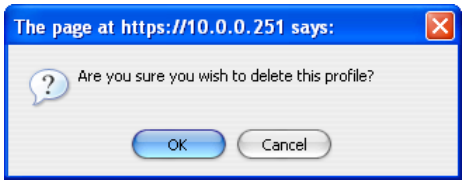


Figure 9-20. Delete Confirmation Pop-up Window.

Call Trace

The Call Trace is a signaling level trace for a given URI and direction (From/To/Any) that displays SIP message flow information sent in syslog messages. The syslog messages containing Call Trace information can be seen with the log viewer function that is activated by the **Logs** button (Figure 9-21) at the top of the E-SBC GUI screen. Clicking on the **Logs** button displays the **Logs Viewer** screen (Figure 9-22) and
(Figure 9-23).

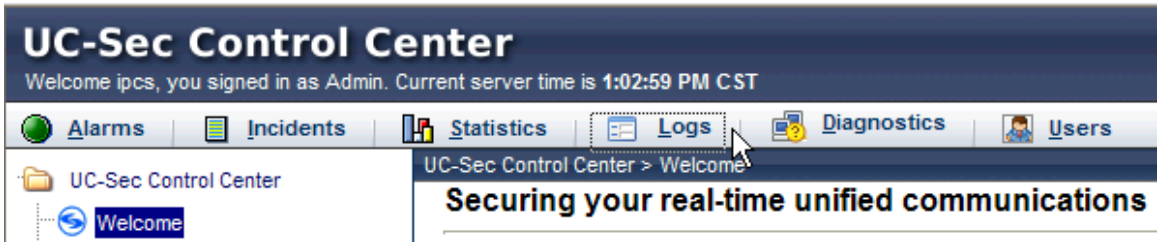


Figure 9-21. Logs Button.

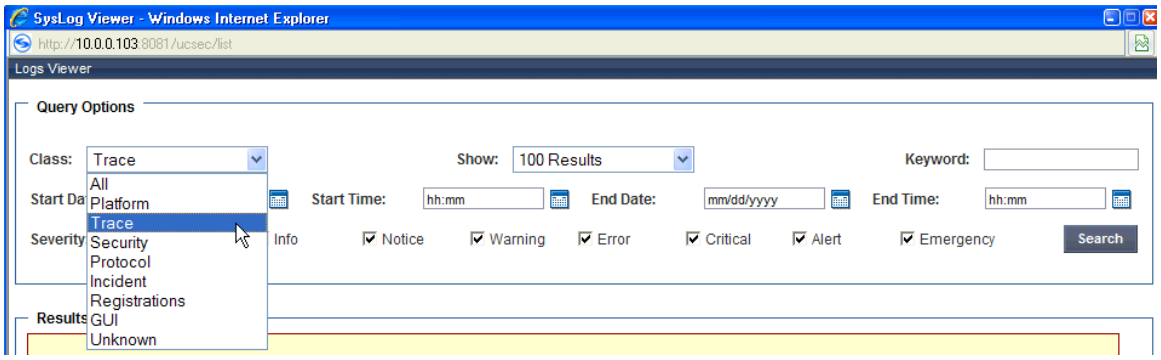


Figure 9-22. Logs Viewer Screen.

Note:	In the **Logs Viewer** screen, select the **Trace** option from the **Class** drop-down list, as shown above in Figure 9-22, to view Call Trace information. Select additional options in the L**ogs Viewer** screen to limit the Call Trace information that is displayed. See a Call Trace example in Figure 9-23.

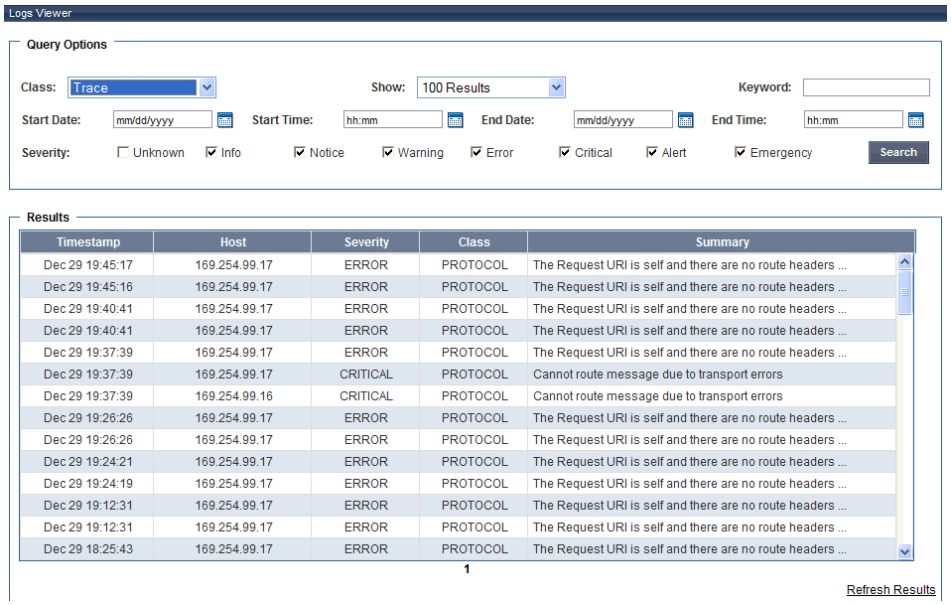


Figure 9-23. Call Trace Logs Viewer Display Example.

Clicking on an item in the Call Trace Logs Viewer display (Figure 9-23) will provide additional information in a Call Trace **Details** pop-up screen. (See the examples in Figure 9-24 and Figure 9-25.)

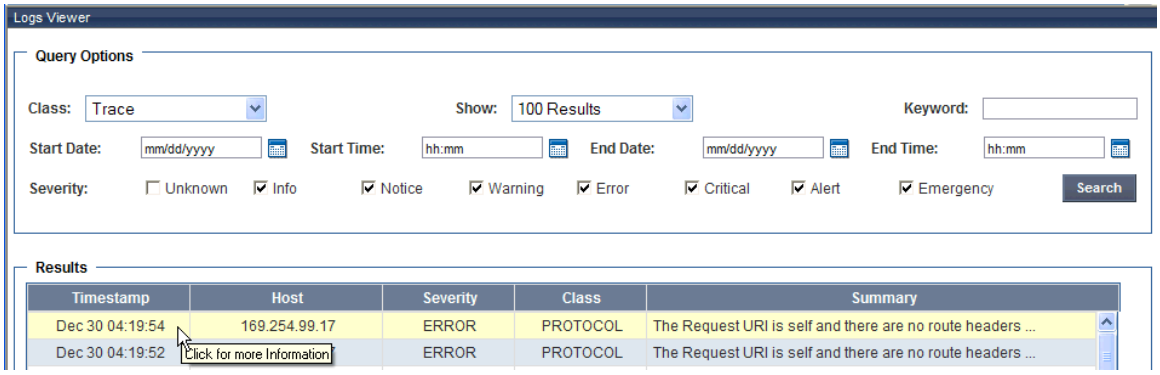


Figure 9-24. Call Trace – More Information.

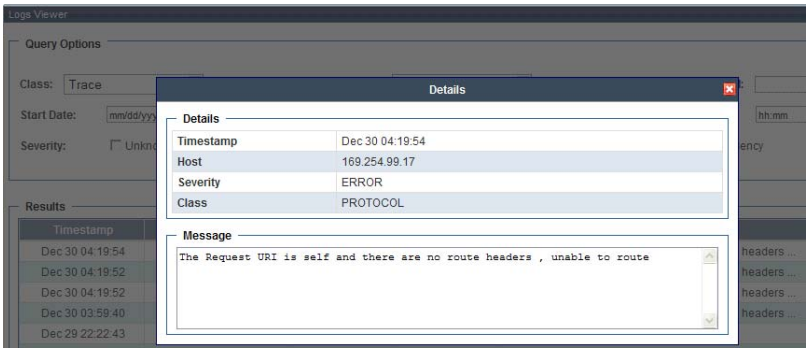


Figure 9-25. Call Trace – Details Pop-Up Screen.

Use the following procedures to manage **Call Trace** profiles.

Adding a New Call Trace Profile

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Trace Settings** function of the **Troubleshooting** feature from the Task Pane (Figure 9-14).
3. From the Application Pane, select the E-SBC device to which you want to add a new call trace profile.
   The screen defaults to the **Packet Trace** tab display.

4. Select the **Call Trace** tab.
5. Select the **Add Trace** button in the upper right-hand portion of the screen.
   The **Add Capture Profile** pop-up window is displayed (Figure 9-26).

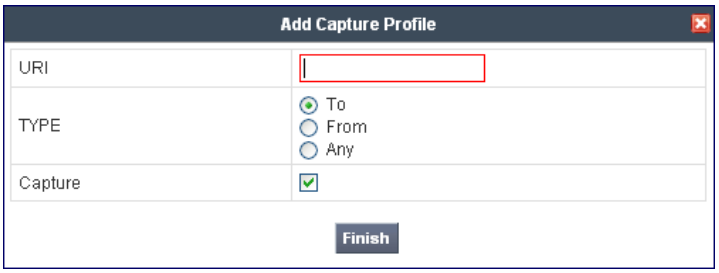


Figure 9-26. Add Capture Profile Pop-up Window.

6. Enter the requested information into the appropriate fields.
   Table 9-19 describes each user-definable field displayed in the **Add Packet Trace** pop-up window.

Table 9-19. Add Capture Profile Pop-up Window Field Descriptions.

Field	Description
URI	The Uniform Resource Locator (URI) of the call.
Type	The type of call to capture: **To**, **From**, and **Any**.
Capture	Checkbox indicating whether (☑) or not (☐) the path of the call through the E-SBC system is to be captured.

7. Select **Finish**.
   The new **Call Trace** profile is displayed.

Editing an Existing Call Trace Profile

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Trace Settings** function of the **Device Specific Settings** feature from the Task Pane (Figure 9-14).
3. From the Application Pane, select the E-SBC device whose call trace profile you want to edit.
   The screen defaults to the **Packet Trace** tab display.
4. Select the **Call Trace** tab.
   The **Call Trace** screen is displayed.
5. Select the **Edit** icon corresponding to the **Call Trace** profile you want to edit.
   The **Add Trace** pop-up window is displayed (Figure 9-27).

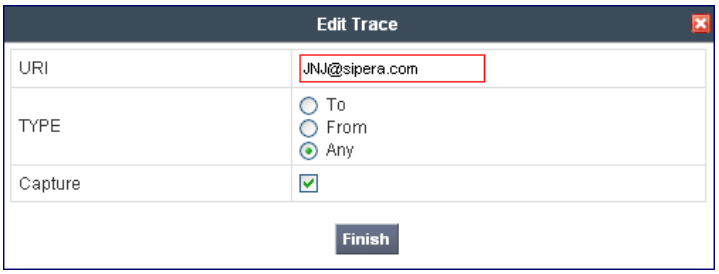


Figure 9-27. Edit Trace Pop-up Window.

6. Edit the desired fields according to the information contained in Table 9-19 and press **Finish** when done or **Cancel** to close the pop-up window without saving your changes.
   Your changes are saved and the **Call Trace** profile is updated and the **Call Trace** screen is redisplayed.

Deleting an Existing Call Trace Profile

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Trace Settings** function of the **Device Specific Settings** feature from the Task Pane (Figure 9-14).
3. From the Application Pane, select the E-SBC device whose call trace profile you want to delete.
   The screen defaults to the **Packet Trace** tab display.

4. Select the **Call Trace** tab.
   The **Call Trace** screen is displayed.

5. Select the **Delete** icon corresponding to the **Call Trace** profile you want to delete.
   A confirmation pop-up window is displayed similar to that shown in Figure 9-28 asking you to confirm your decision.

6. Click **OK**.
   The selected **Packet Trace** profile is deleted.

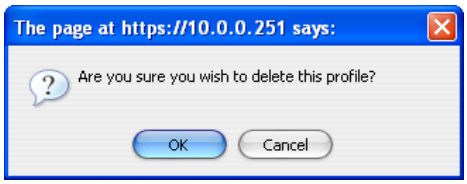


Figure 9-28. Delete Confirmation Pop-up Window.

Viewing Packet Trace and Call Trace Data

Both packet trace and call trace information is directed to the Sipera management interface device into the following file path: **/archive/syslog/ipcs/octeon.log**

Use the following procedure to access and view packet trace and call trace information.

1. Using a Secure Shell (SSH) Client (such as PuTTY), connect to the Sipera management interface device. A sample ssh command string is shown below in Figure 9-29.

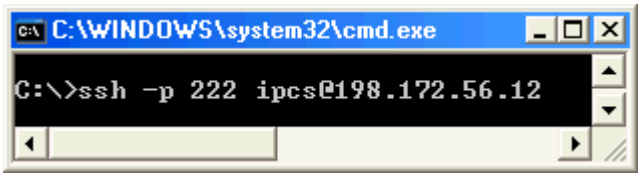


Figure 9-29. SSH Command String Example

Note:	To determine the Management IP address, select the **System Management** feature from the Task Pane and select the **View Config** button for a specific device to display a System Configuration screen similar to the example shown in Figure 9-30 on the next page. A list of Management IPs is displayed in the lower-right portion of the screen.

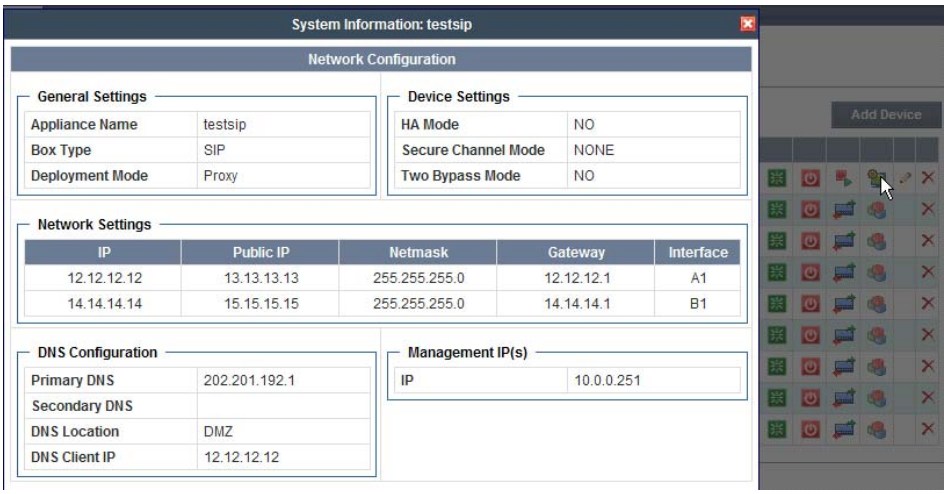


Figure 9-30. System Configuration Screen

2. Once connected, from the prompt (**login as:)** enter the account name **ipcs** and then enter the password when prompted for it to display the E-SBC Welcome screen as shown in the example in Figure 9-31.

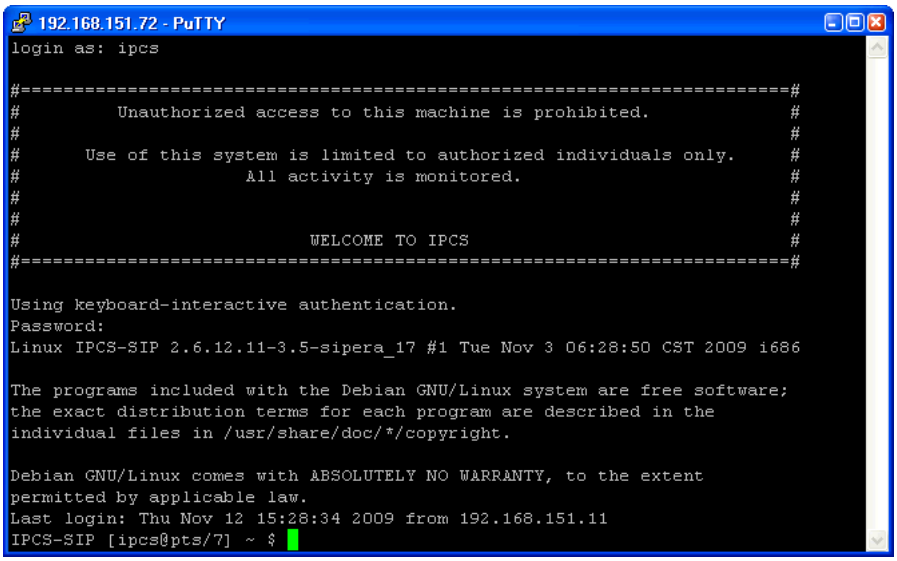


Figure 9-31. E-SBC Welcome Screen

3. From the dollar sign prompt (**$**), enter sudo su and then from the pound sign prompt (**#**) that appears enter the change directory (**cd**) command to navigate to the **/archive/syslog/ipcs** directory, as shown in the example in Figure 9-32 on the next page.

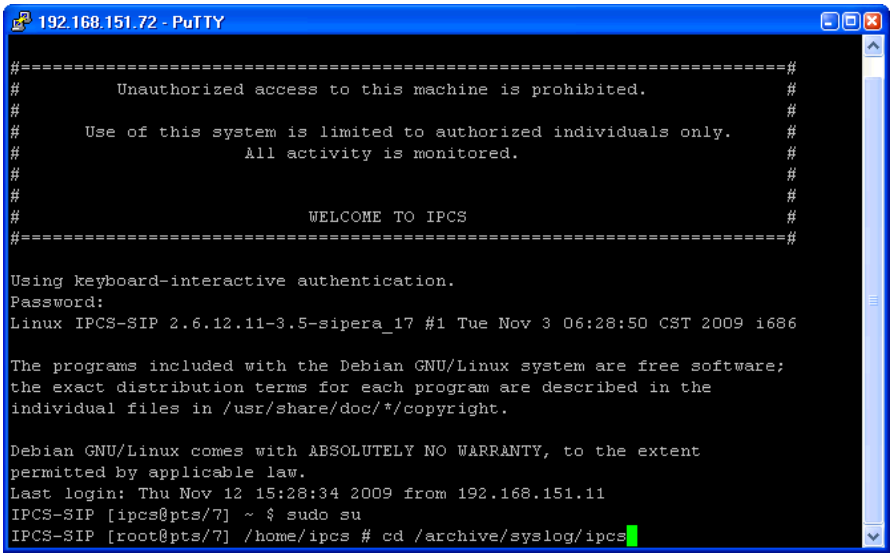


Figure 9-32. Navigating to the syslog/ipcs Directory

4. The log file (**octeon.log**) is contained in the **/archive/syslog/ipcs** directory. From this directory from the pound sign (**#**) prompt, you can use the VI editor to view this file by entering the command as follows: **# vi octeon.log**
5. The Packet Trace and Call Trace filtered information set up previously in the Packet Trace and Call Trace profiles will be contained in the **octeo.log** log file and viewable in a vi editor screen similar to the example shown in Figure 9-33 below.

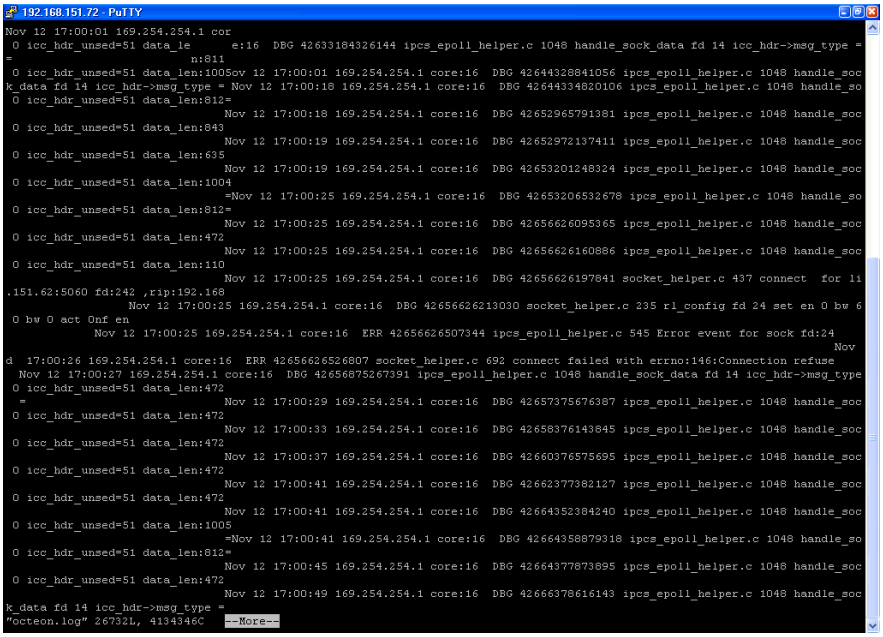


Figure 9-33. VI Editor Screen Display of an octeon.log Log File

Packet Capture

1. Select the **Packet Capture** tab to display a Packet Capture Configuration pop-up screen (see example in Figure 9-34) containing filtering options for configuring a packet capture.

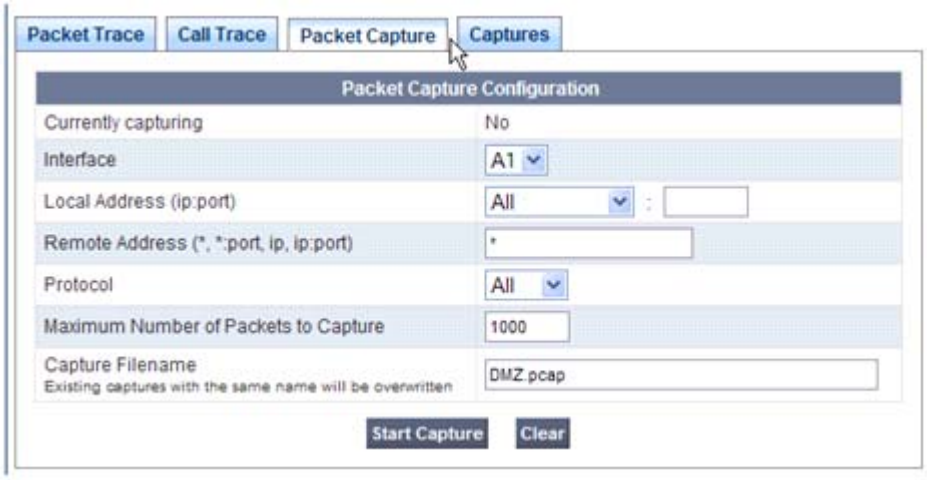


Figure 9-34. Packet Capture Configuration Pop-Up Screen

2. In the Packet Capture Configuration screen (Figure 9-34), enter the appropriate capture information and then click on the Start Capture button to start the capture and then display a Packet Capture information pop-up screen similar to the example shown below in Figure 9-35.

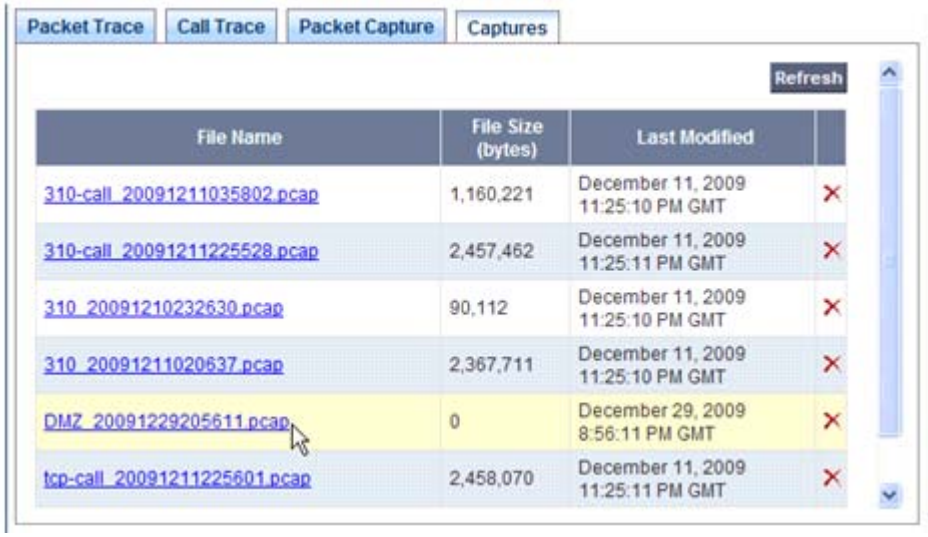


Figure 9-35. Packet Capture Information Pop-Up Screen

3. In the Packet Capture information screen, select the file name of the capture to display a File Download pop-up screen similar to the example shown in Figure 9-36.

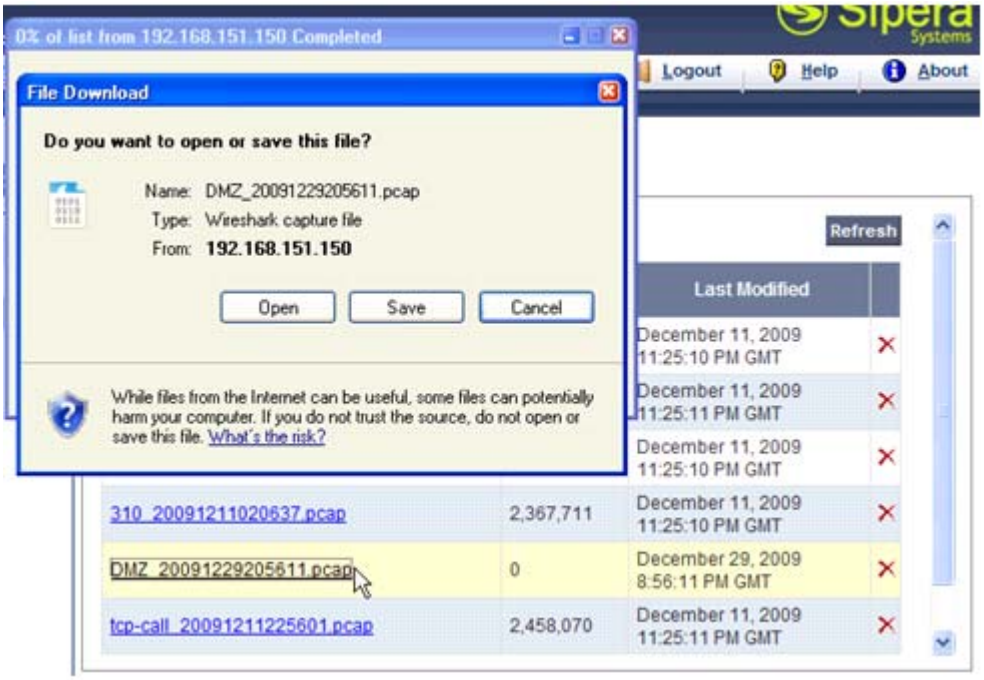


Figure 9-36. File Download Pop-Up Screen

4. In the File Download pop-up screen, click on the **Save** button to display a **Save As** pop-up screen similar to the example shown in Figure 9-37 below.

   The Packet Capture feature saves captures in the **pcap** format that is viewable using **Wireshark** (originally named **Ethereal**), a free and open-source packet analyzer application used for network troubleshooting, analysis, and software protocol development.

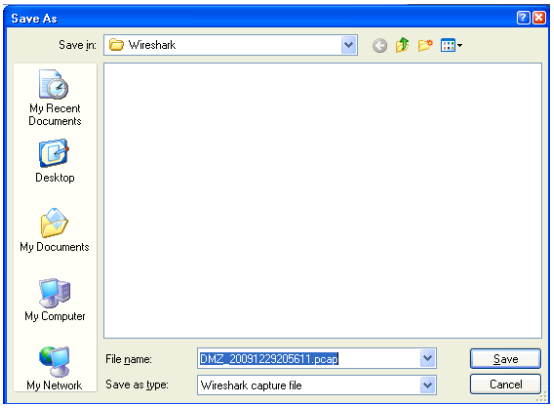


Figure 9-37. Save As Pop-Up Screen

5. In the **Save As** pop-up screen, use the **Save In** drop-down list to navigate to a directory for saving the Packet Capture (**pcap**) file and click on the **Save** button to save the file to the new directory.

Note:	You will need to download and install **Wireshark**, or a similar network analyzer program, in order to view the Packet Capture (**pcap**) file.

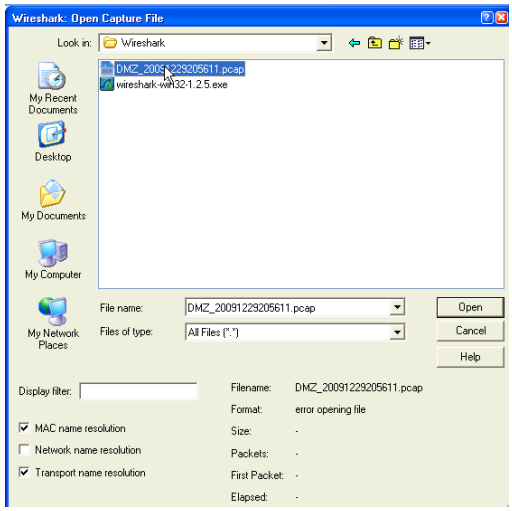


Figure 9-38. Opening the Capture File

6. In the save directory, use Wireshark or a similar application to open up the Packet Capture (**pcap**) file. If Wireshark is already running, you can double-click on the file to open it with Wireshark. Otherwise, you will need to start Wireshark first and then either open the file from within the Wireshark application or double-click on the Packet Capture file in the save directory.

   A sample Packet Capture is shown in Figure 9-39 below.

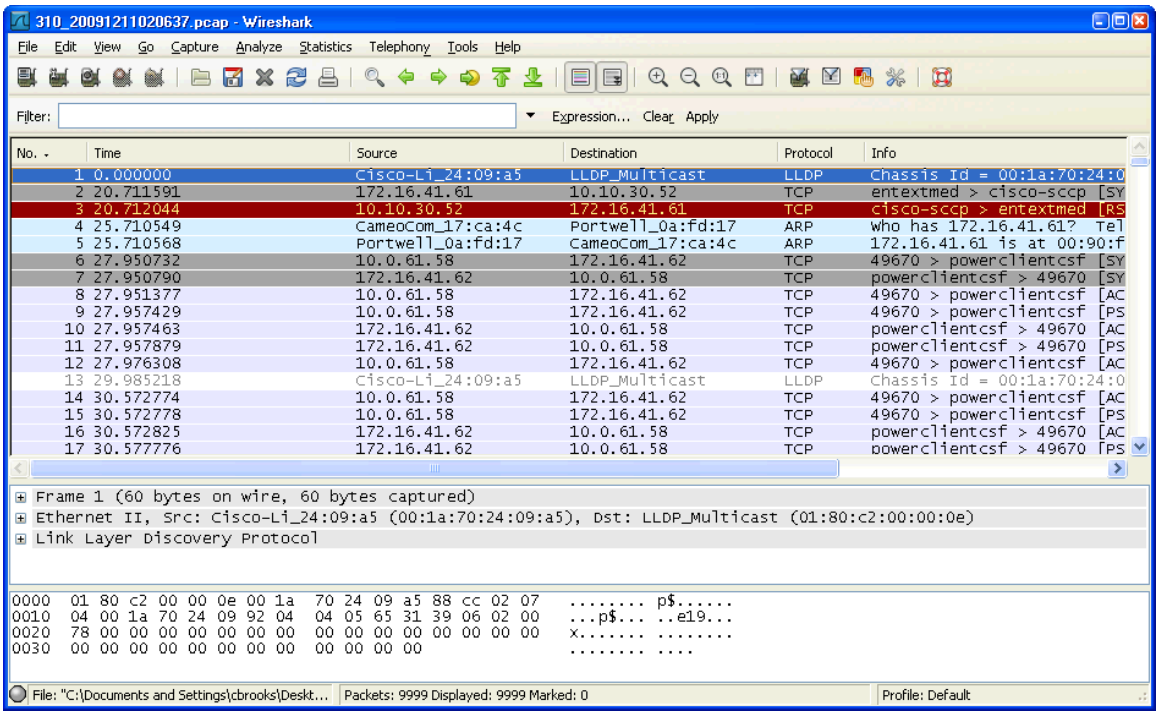


Figure 9-39. Sample Capture File Display

Audit Logs

A new feature with E-SBC Product Release 4.0 is audit logging. The **Audit Log Viewer** displays the contents of the audit log, which contains a record of security related events, such as logins, session starts, session ends, new user additions, password attempts/retries/changes, etc.

1. Login to the E-SBC Control Center as the **Admin**.
2. Select the **Logs** Logs icon from the Tool Bar (Figure 9-40) and select the **Audit Logs** menu option to display the Audit Log Viewer (Figure 9-41).

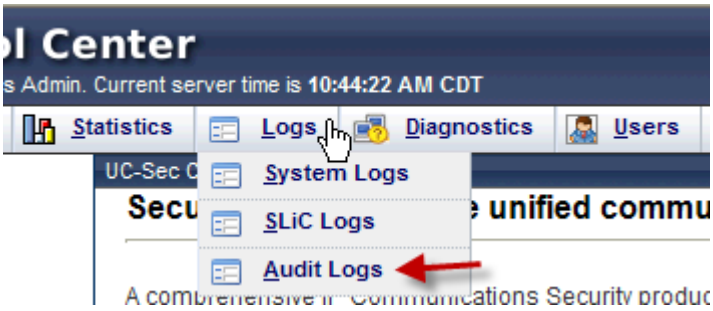


Figure 9-40. Audit Logs Menu Option

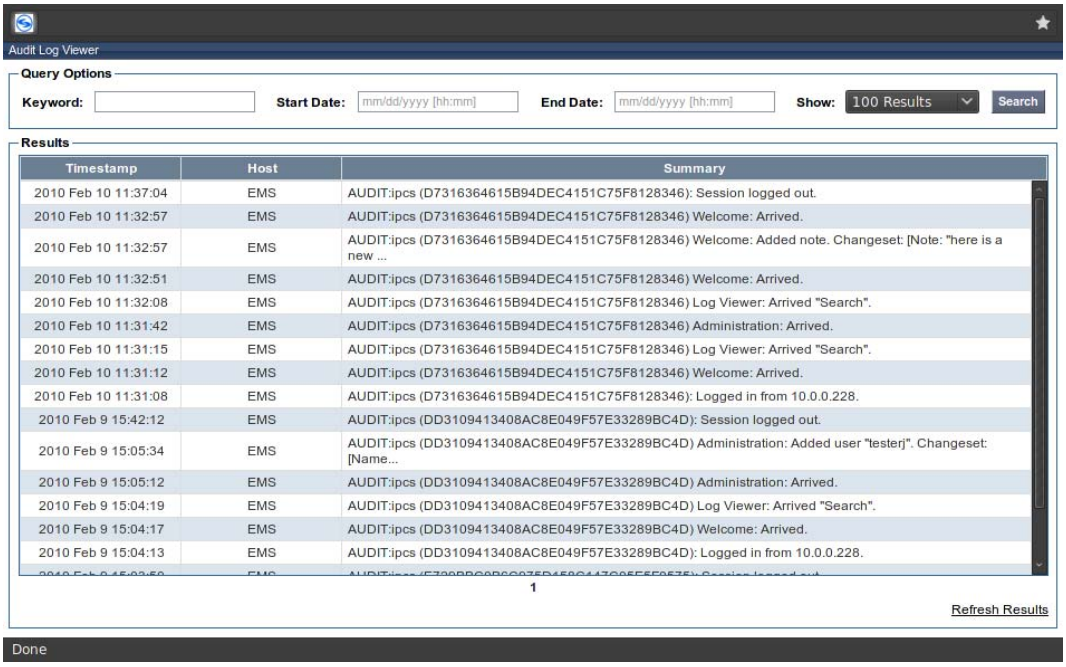


Figure 9-41. Audit Log Viewer

3. In the **Query Options** **Start Date** field and **End Date** field in the **Audit Log Viewer** (Figure 9-41), you can filter the results displayed in a search report to fall within starting and ending dates and times.

4. In the **Query Options** **Keyword** field in the top-left portion of the **Audit Log Viewer**, enter one or more words to define the limits of the log report and click on the **Search** button on the right-hand portion of the viewer. The report is run and a report output is displayed similar to that in the example shown in Figure 9-10 on the next page.
5. To see additional details about a particular log line in a report, select the log line (Figure 9-42) to display the Audit Log Details screen (Figure 9-43).

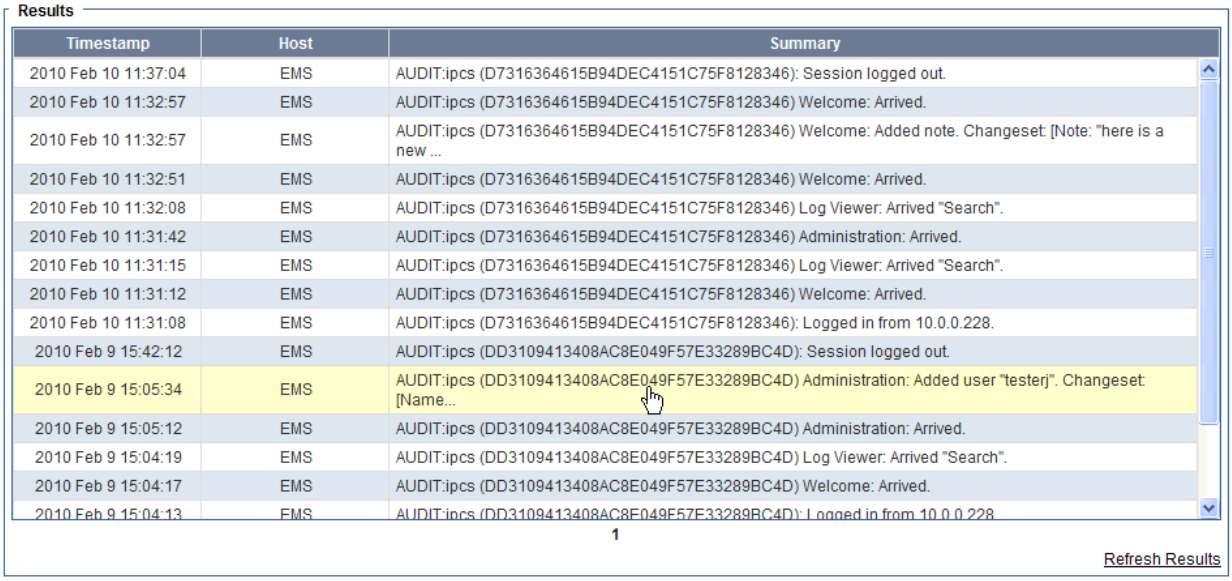


Figure 9-42. Selecting a Log Line

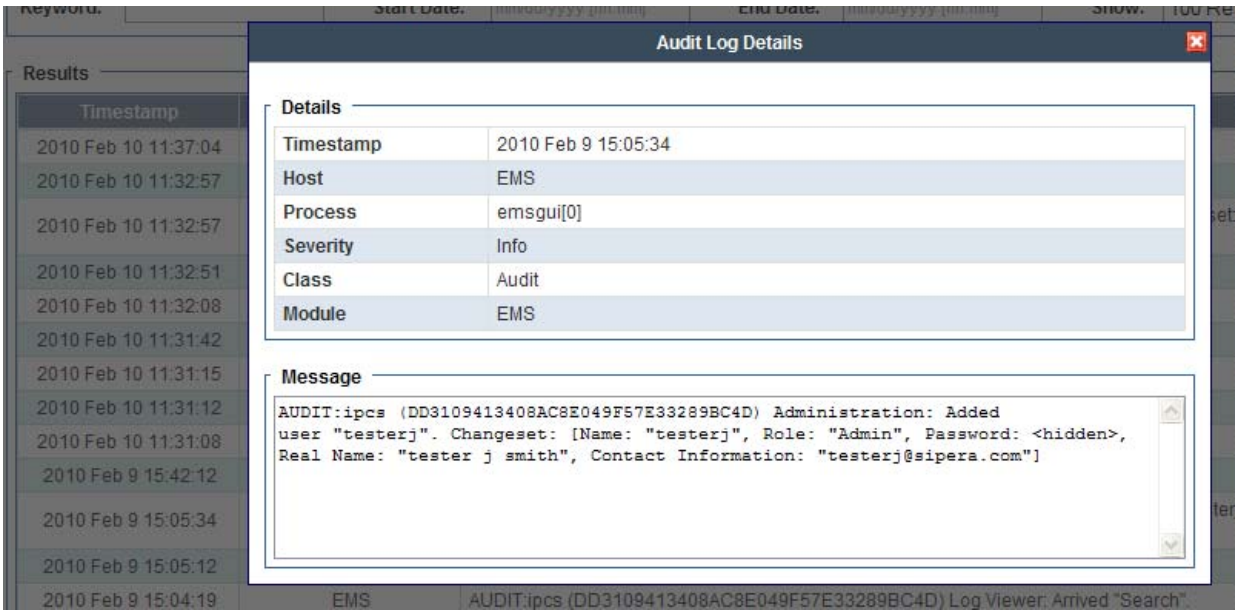


Figure 9-43. Audit Log Details

Note: The Log Level rules for the Audit Log and other logs are set from the Task Pane by selecting: **Troubleshooting → Syslog Management.**

Audit Logging is enabled in the Log Level row for:
Class: Audit
Facility: **LOG_LOCAL6**

The Log Level Facility name **LOG_LOCAL6** is reserved for Audit Logging and the Facility name **LOG_LOCAL7** is reserved for SLiC Logging.

Both of the above Facility names are reserved and cannot be changed. Their file path destinations cannot be changed either.

This page intentionally left blank.

Command Line Interface 10

Overview

The Command Line Interface (CLI) is a high-speed serial management interface that provides direct (local or remote) access to the E-SBC security device for performing various administrative and operational tasks. These tasks are executed using a robust assortment of commands entered via a terminal emulator such as Telnet or another commonly available serial application like HyperTerminal.

The **CLI** for **E-SBC** (hereafter referred to as **clipcs**) interface is available whenever the E-SBC chassis is running. Security is provided through a combination of account login and user access privileges.

Command Structure

clipcs commands are grouped according to two modes of operation: *console* and *instance*. The *console* mode is the top-level command structure from which basic E-SBC system-wide commands can be executed. The *instance* mode is the next level of administrative control which provides direct access to a particular E-SBC functional node (*signaling*, *media*, or *intelligence*).

Note

All **clipcs** commands and arguments (including user passwords) are case sensitive.

Console Commands

Console commands are one level deep are used to display certain basic information about E-SBC system configuration and status.

Table 10-1 contains a summary list of these commands. This list can be displayed from any console prompt by entering the **clipcs** (in lowercase) command to start the E-SBC console and then entering the **help** command, as shown below.

```
SS310 [root@pts/3] / # clipcs
       Starting E-SBC Console...Please wait.
       E-SBC Version 3.8.0.Q32 (C) Sipera Systems Inc.
       E-SBC# help
```

Table 10-1. clipcs Commands Available at the Console Prompt.

Command	Description
Toggles port by-pass feature: enable / disable.	
`clear`	Clears the display screen.

Command	Description
clock	Displays, sets, and clears the internal system clock.
exit	Moves command level from instance mode to console mode.
help	Displays a list of available commands and their descriptions.
refresh	Displays the current refresh interval.
spool	Directs output to a file or device.
status	If entered in the Console mode, it displays the status of E-SBC nodes; if entered from the Instance mode, it displays the detailed operational status of the node being accessed.
select	Selects a particular E-SBC node for access and activated the instance mode.
show	A command used in combination with those shown below to display certain system-, node-, or operational-specific information.

SHOW Command	Description
certinstall	Installs certificates.
certsync	Synchronizes certificates.
certupdate	Updates the certificate key.
ip interface all	Displays IP-related information about physical E-SBC system interfaces.
ip route	Displays E-SBC routing information.
Flow dynamic	The show flow dynamic command displays the media Relay Information for the given active session phone IP. (See the section below titled, "Show Flow Dynamic."
E-SBC cpu	Displays CPU-specific information.
E-SBC global cluster	Displays E-SBC global cluster information.
E-SBC interface status	Displays the status of physical E-SBC system interfaces.
E-SBC memory	Displays memory usage statistics for all E-SBC processes.
E-SBC processes	Displays all currently running processes.
iptables version	Displays the version of the IP tables.
linux version	Displays the version of Linux.
octeon status	Displays the status of the executables running on the Octeon processor

Command	Description	
	`uptime`	Displays the amount of time the system has been in operation since last power-up.
`quit`	Terminates the current CLI session.	
`version`	Displays the current version of the CLI server.	

Show Flow Dynamic

The "**flow dynamic**"option for the E-SBC CLI **show** command is useful for debugging network problems in an active session where media is only received in one direction or where media is not received in either direction.

The **show flow dynamic** command displays the media Relay Information for the given active session phone IP.

Command Syntax:

show flow dynamic [x.x.x.x (ip addr) || x.x.x.x:y (ip addr:port)] [RTP/RTCP/SRTP/SRTCP]

Note: If a port number is specified in the command line, then a protocol entry at the end of the command line will not be considered.

Instance Commands

Instance commands, also referred to as *top* commands, are two levels deep and are used to display detailed information about a specific E-SBC node (Figure 10-1 Instance Commands Example).

Table 10-1 contains a summary list of these commands. Instance commands are only available within the *instance* mode, which is enabled whenever the `select` command has been invoked. Instance or top commands communicate directly with the active (selected) E-SBC node and provide output from that node only.
Screen displays (see login example below) presented by these commands are automatically refreshed at a rate determined by the `refresh` command (default: 5 seconds).

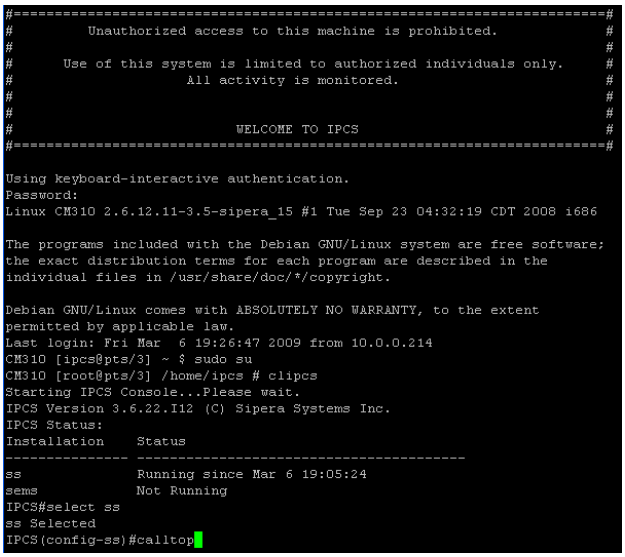


Figure 10-1 Instance Commands Example

Table 10-2. CLI (Top) Commands Available from the Instance Mode.

Command	Description
`top`	Displays a detailed functional status of the selected E-SBC node. The display is automatically refreshed every 5 seconds.

Accessing the CLI

There are three methods for accessing **clipcs**: *remote*, *local*, and *GUI*.

- To establish a remote SSH session, go to the section, *Remote clipcs Access*.
- To establish a local SSH session, refer to the section, Local *clipcs Access*.
- To establish an SSH session using the EMS GUI, refer to the section *Establishing a Secure Shell Session* in Chapter 6, *System Configuration*.

Remote clipcs Access

clipcs may be accessed remotely using any SSH client using the following procedure.

1. Start the SSH client and enter the following information to establish a secure connection with the E-SBC equipment chassis.

Parameter	Value
IP Address	The IP address of the E-SBC equipment chassis to which you want to establish a secure connection.
Port	222

Protocol	SSH

2. When the session is established, from the login prompt (Figure 10-2), login as **savon** and press **Enter**.
   The password prompt will be displayed (Figure 10-3).

Figure 10-2 SSH Login to clipcs.

Figure 10-3. clipcs Password Prompt.

3. Enter the password provided by Sipera and press **Enter**.
   The top-level E-SBC system prompt is displayed, similar to that shown in Figure 10-4.

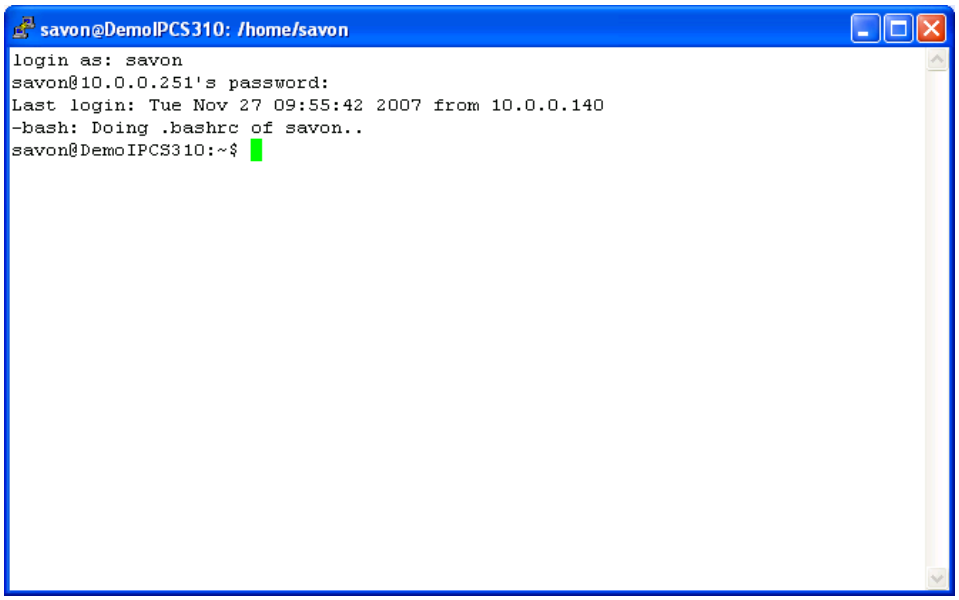


Figure 10-4. Top-level clipcs Prompt.

4. Enter the **su** command to access super user privileges and press **Enter**.
   You will be prompted for the super user password (Figure 10-5).
5. Enter the super user password and press **Enter**.
   The super user command prompt is displayed (Figure 10-6).

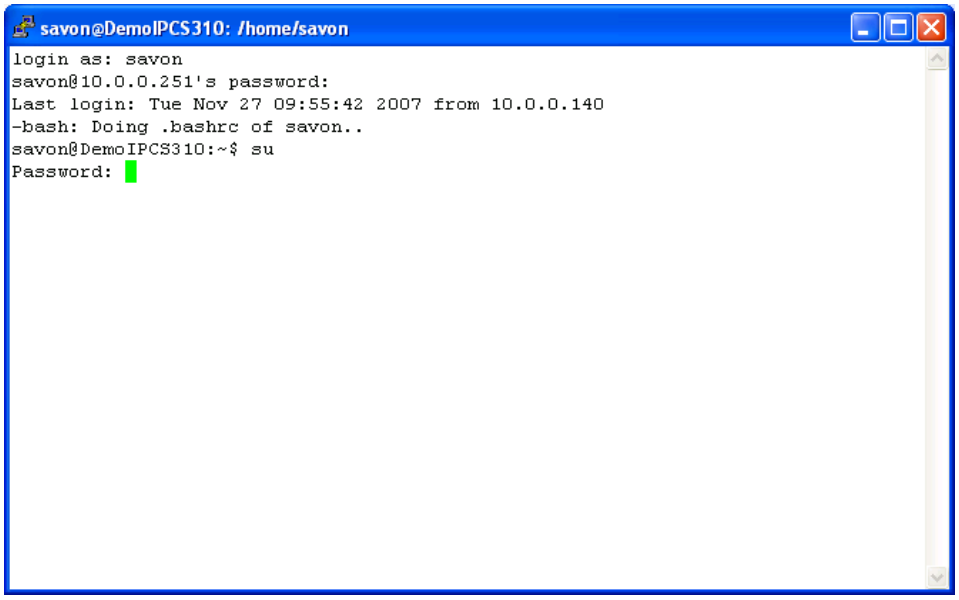


Figure 10-5. Super User Password Prompt.

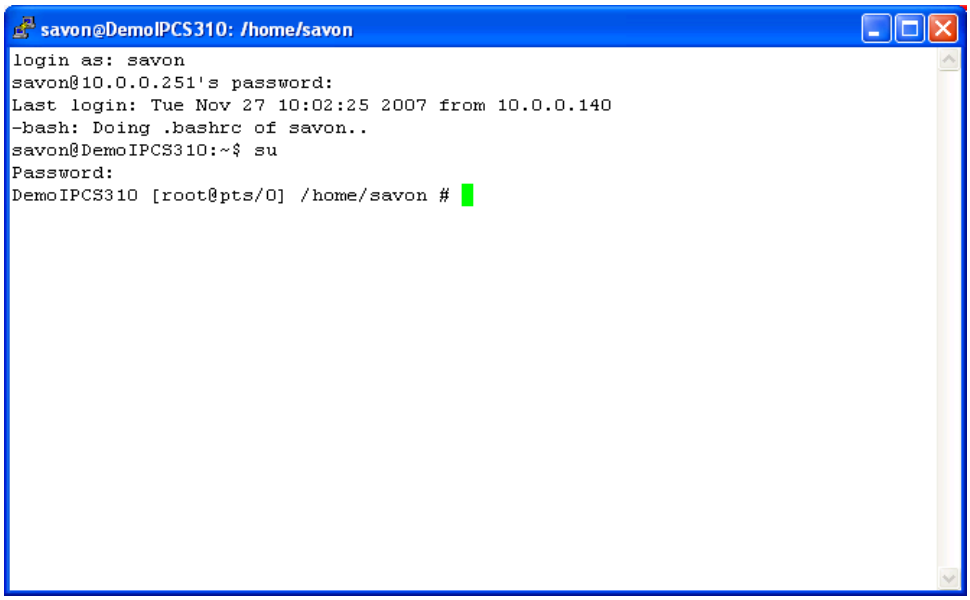


Figure 10-6. Super User Command Line Prompt.

6. Start **clipcs** by entering the **clipcs** command and press **Enter**. **clipcs** is started and the command line displayed (Figure 10-7).

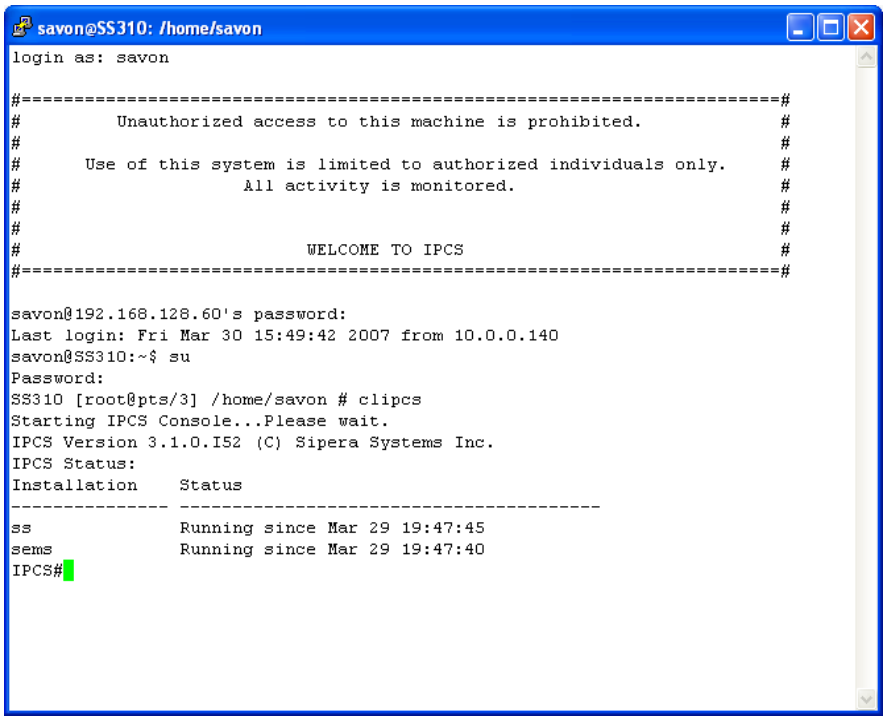


Figure 10-7. clipcs Command Line.

Local clipcs Access

To access **clipcs** locally by connecting directly to the E-SBC chassis, you must perform the following steps:

- Physically connect your terminal device to the **Console** port on the front of the E-SBC equipment chassis.
- Establish a communications session with the command shell.
- Login to the command shell.

Connecting a Terminal Device to the E-SBC Equipment Chassis

Use the following procedure to physically connect a communications device to the E-SBC equipment chassis.

1. Locate the **Console** port on the E-SBC equipment chassis or, in the case of the Element Management System (EMS), the **UART** (serial COM) port.
   The **UART** port for the EMS is located on the back panel of the equipment chassis (See the *Sipera E-SBC EMS Installation Guide*, 100-5224-400 for more information).
   The **Console** port for the E-SBC 1U equipment chassis is located on the front panel. (See the *E-SBC 1U Installation Guide*,101-5224-400 for more information).
2. Connect an RJ45-terminated serial communications cable or a DB-9 cable (depending on the chassis model) from the terminal device to the **Console** or **UART** port as shown in the following figures.

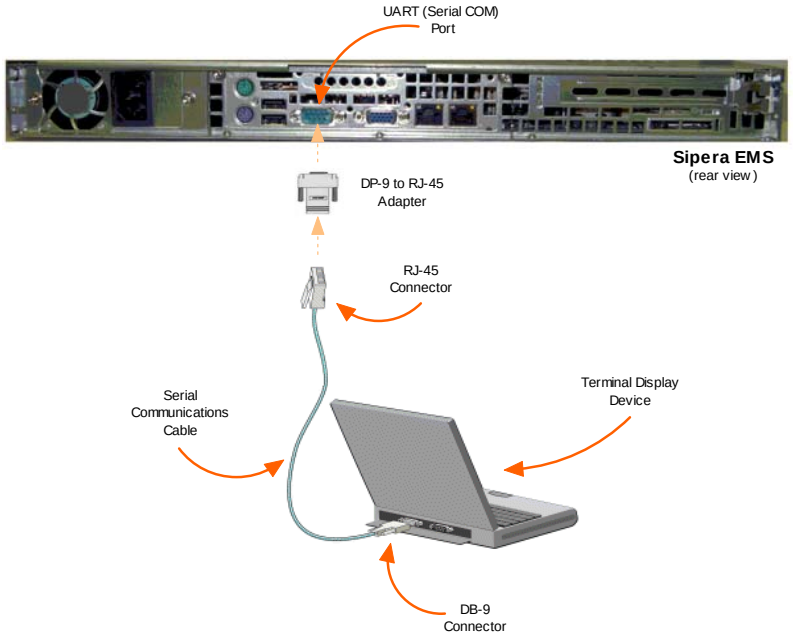


Figure 10-8. Connecting a Terminal Device to the Sipera E-SBC EMS.

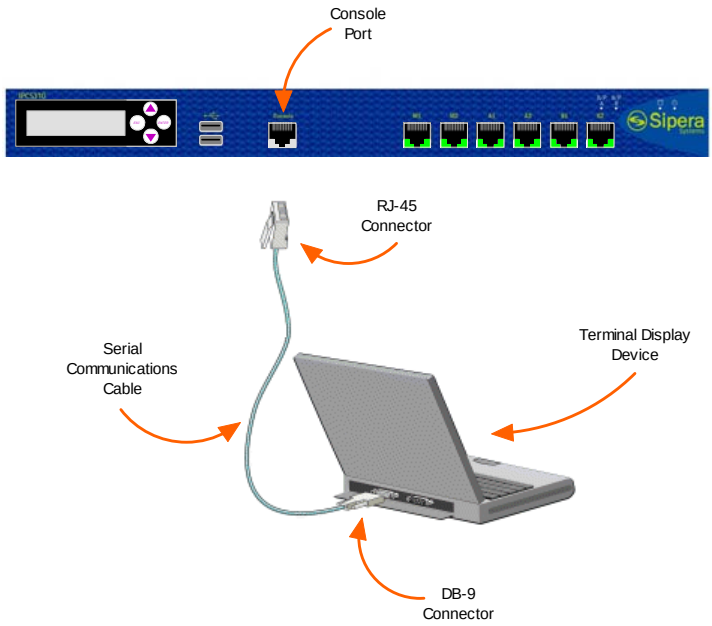


Figure 10-9. Connecting a Terminal Device to the E-SBC 1U.

Establishing a Communications Session

Use the following procedure to establish a communications session with the E-SBC command shell.

1. Configure the communications parameters of your terminal program to the settings contained in the table below.

Figure 10-1 Instance Commands Example

Table 10-2. Console Port Communications Settings.

Parameter	Value
Baud rate	19200
Parity	None
Data bits	8
Stop Bits	1
Connection Setting	Direct to Com1

2. Press **Enter** to establish the communications session.
   A prompt asking for your **User Name** and **Password** will be displayed.

Logging in to the Command Shell

Use the following procedure to log in to the E-SBC command shell to begin a CLI session.

1. Logon to the command shell using Administrator's user name and password. The command shell prompt will be displayed.

   ```
   [savon@localhost bin] $
   ```

2. Enter the following command:

   ```
   [savon@localhost bin] $  clipcs
   ```

3. The CLI prompt will be displayed as shown in Figure 10-10. The CLI is now ready for use.

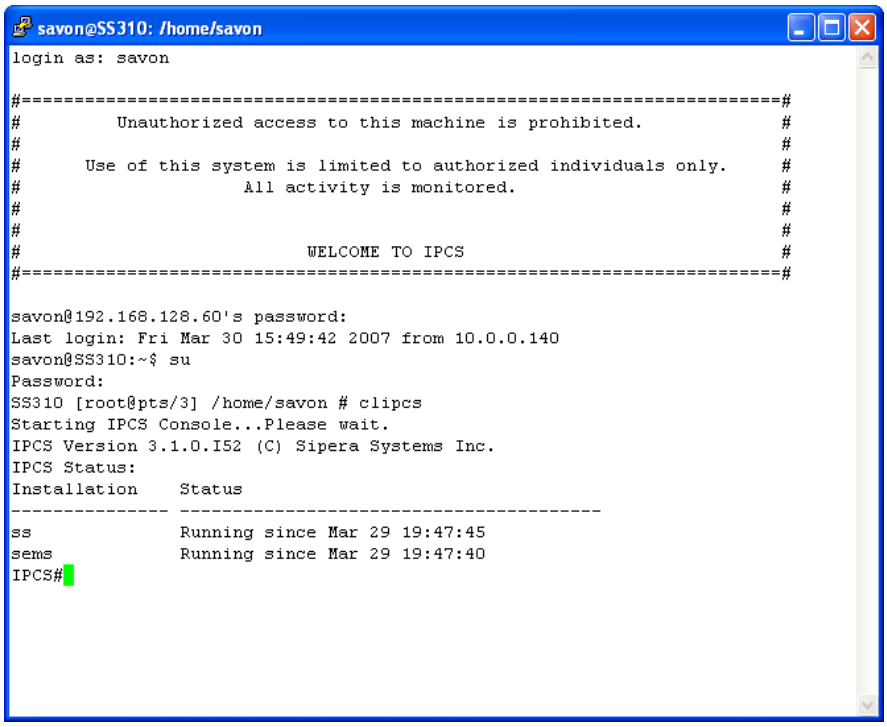


Figure 10-10. Console Screen.

Configuration Workflows for SIP Trunking 11

SIP Trunking Overview

The *SIP Trunking* feature of E-SBC security devices allow SIP trunk-enabled enterprises to completely secure SIP connectivity over the Internet via SIP trunking services obtained through an Internet Telephony Service Provider (ITSP).

The E-SBC provides a well-defined demarcation point between the core and the access network, and enables network privacy for all calls traversing the enterprise network.
In addition, the SIP Trunking feature in E-SBC allows an enterprise to maintain granular control through well-defined domain policies securing customers' SIP implementations/servers from known SIP and Media vulnerabilities.

Because the E-SBC security device is deployed in the enterprise DMZ as a trusted host, all SIP signaling traffic destined for the enterprise is received by the external firewall and sent to the E-SBC device for processing (Figure 11- 1).

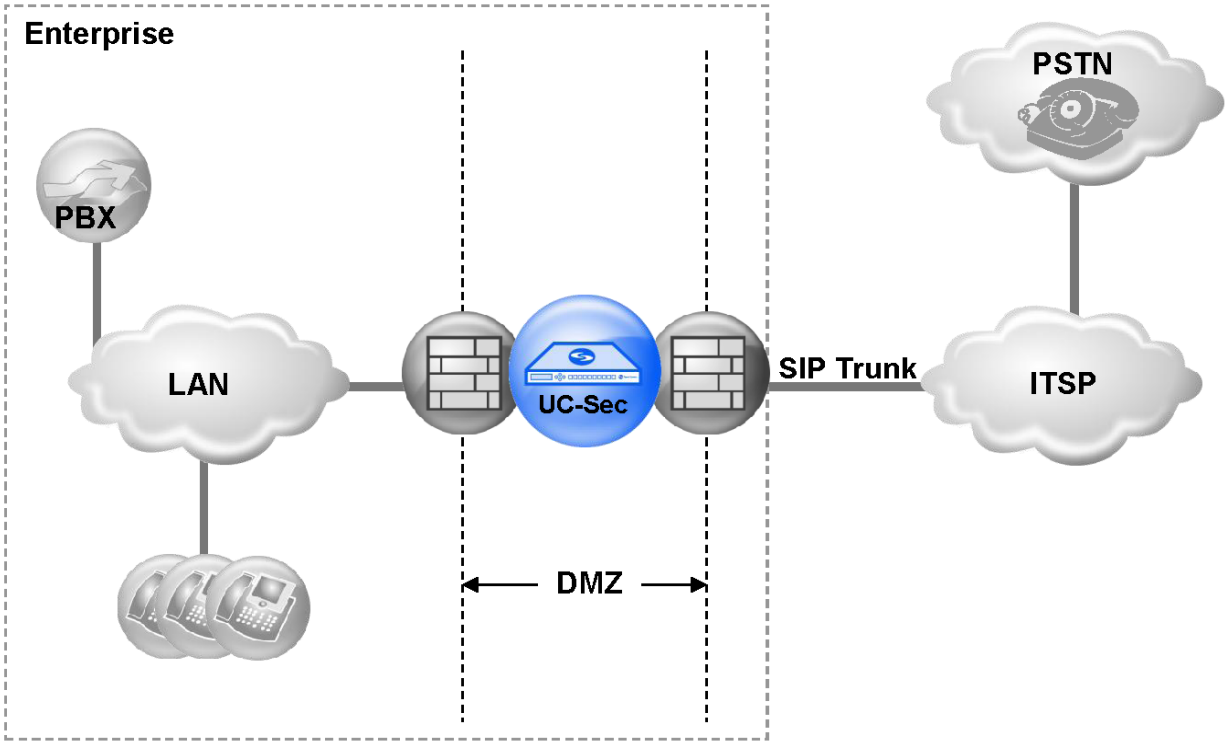


Figure 11- 1 SIP Trunking Diagram

E-SBC Configuration for Generic SIP Trunk

This section details the procedure for configuring a generic E-SBC SIP trunk. The generic SIP trunk configuration consists of the following steps:

1. Create Routing Profiles
    a. Create Routing Profile for Call Server
    b. Create Routing Profile for Trunk Server
2. Create Topology Hiding Profiles
    a. Create Hiding Profile for Call Server
    b. Create Hiding Profile for Trunk Server
3. Create Interworking profiles
4. Create Server Profiles
    a. Create Server Profile for Call Server
    b. Create Server Profile for Trunk Side Server
5. Create Signaling Interfaces
    a. Create External Signaling Interface Toward Trunk Server
    b. Create Internal Signaling Interface Toward Call Server
6. Create Media Interfaces
    a. Create External Media Interface Toward Trunk Server
    b. Create Internal Media Interface Toward Call Server
7. Create Server Flows
    a. Create Flow Toward Call Server
    b. Create Flow Toward Trunk Server
8. Server-Specific Configuration for SIP Trunking

Step-1 Create Routing Profiles

Create Routing Profile for Call Server

This procedure will create a routing profile with next hop as a call server address.

Note:	**Use the following profile name:**	**Route_to_Call_Svr**

1. Login to the E-SBC Control Center as the Admin.
2. Select the **Routing** function of the **Global Profiles** feature from the Task Pane (Figure 11-2).

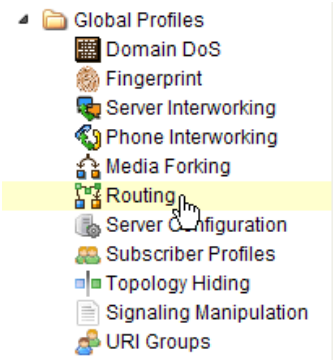


Figure 11-2 Selecting the Routing Function

3. In the Routing Profile screen that is displayed, click on the **Add Profile** button, which displays the Add Routing Profile pop-up screen similar to the example shown in Figure 11-3 below.

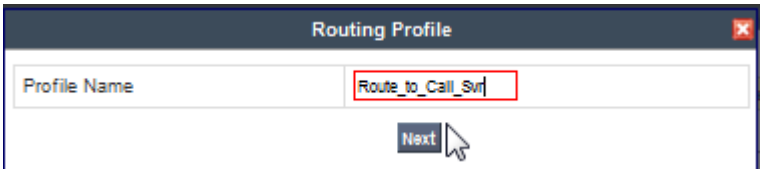


Figure 11-3 Add Routing Profile Pop-up Screen 1

4. In the Profile Name field, type the profile name: **Route_to_Call_Svr**
5. Click **Next** to display a second Add Routing Profile screen similar to the one shown in Figure 11-4 below.

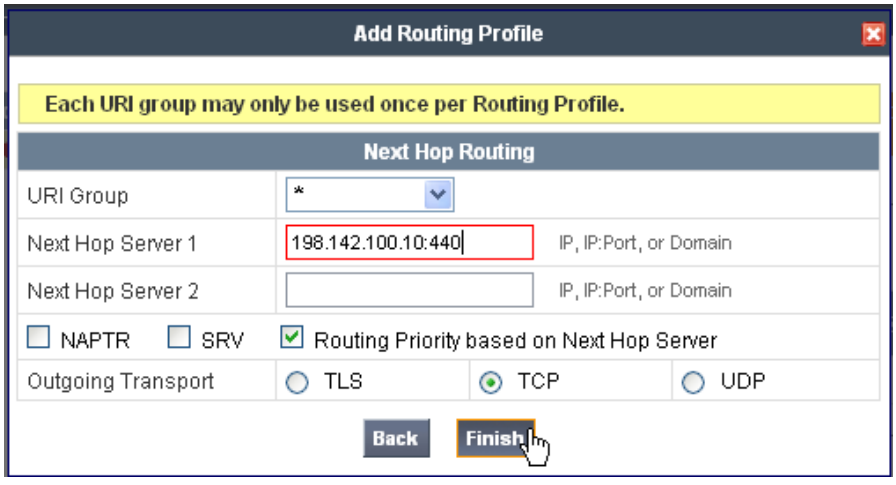


Figure 11-4 Add Routing Profile Pop-up Screen 2

6. In the second Add Routing Profile screen, in the Next Hop Server 1 field, enter either the Domain Name of the Call server, IP address, or enter the IP address and port number (for non-default ports) separated by a colon, as shown in Figure 11-4.

7. Select the checkbox labeled Routing Priority based on Next Hop Server.

Note:	**If the Call server domain is to be selected from the DNS server either by NAPTR or SRV, select the appropriate checkbox. If you want to use next hop instead of route header for routing in-dialog and/or out-of-dialog messages, check the appropriate checkbox.**

8. Select the transport type (i.e., TLS, TCP, or UDP.)
9. Click **Finish** to save the configuration and exit.
   This displays the Routing Profile screen, similar to the example shown below in Figure 11-5 showing the newly created **Route_to_Call_Svr** Routing Profile.

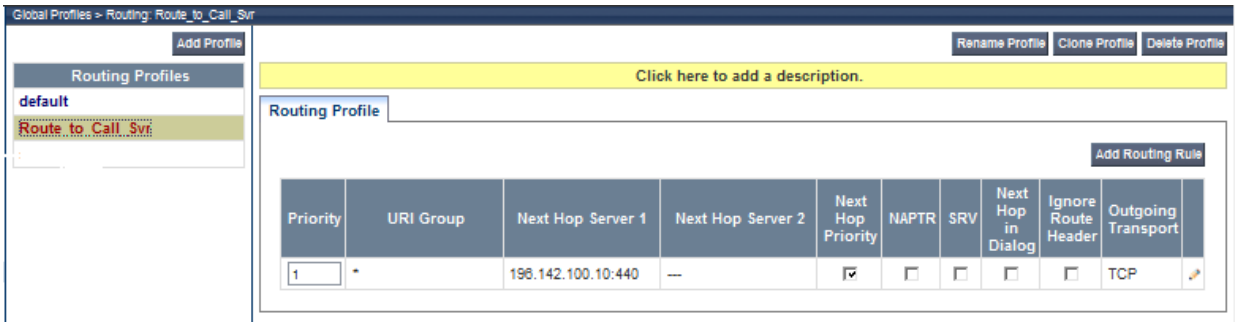


Figure 11-5 Routing Profile Screen

Create Routing Profile for Trunk Server

This procedure will create a routing profile with next hop as a Trunk side Server IP address.

Note:	**Use the following profile name:**	**Route_to_Trunk_Svr**

1. Login to the E-SBC Control Center as the Admin.
2. Select the **Routing** function of the **Global Profiles** feature from the Task Pane (Figure 11-2).
3. In the Routing Profile screen that is displayed, click on the **Add Profile** button, which displays the Add Routing Profile pop-up screen similar to the example in Figure 11-6.

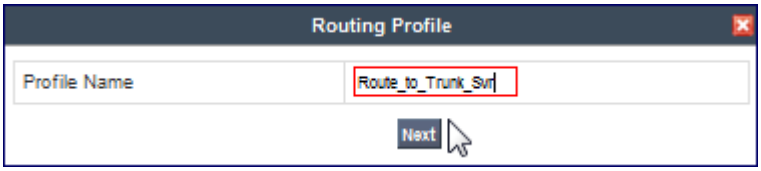


Figure 11-6 Add Routing Profile Pop-up Screen 1

4. In the Profile Name field, type the profile name: **Route_to_Trunk_Svr**

5. Click **Next** to display a second Add Routing Profile screen similar to the one shown below in Figure 11-7.

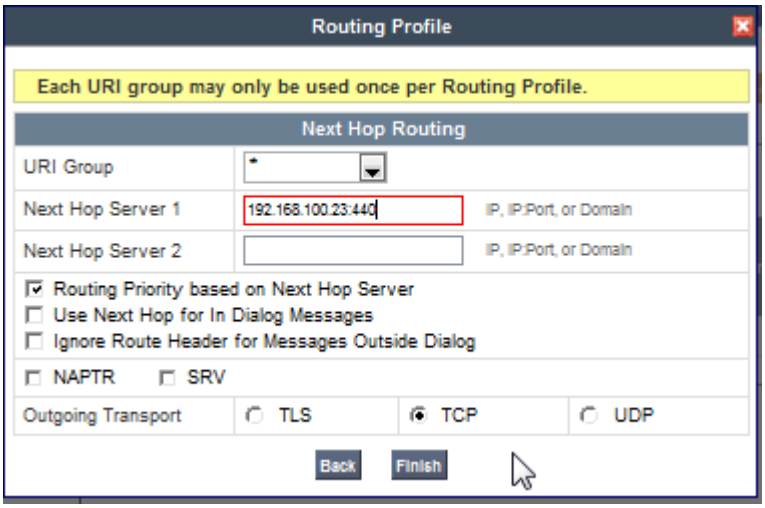


Figure 11-7 Add Routing Profile Pop-up Screen 2

6. In the second Add Routing Profile screen, in the Next Hop Server 1 field, enter either the Domain Name of the Line server or enter the IP address and port number separated by a colon, as shown in the example above.
7. Select the checkbox labeled Routing Priority based on Next Hop Server.

Note:	**If the Call server domain is to be selected from the DNS server either by NAPTR or SRV, select the appropriate checkbox. If you want to use next hop instead of route header for routing in-dialog and/or out-of-dialog messages, check the appropriate checkbox.**

8. Select the transport type (i.e., TCP or UDP).
9. Click **Finish** to save the configuration and exit.
   This displays the Routing Profile screen, similar to the example in Figure 11-8, showing the newly created Route_to_Trunk_Svr routing profile along with the Route_to_Call_Svr routing profile created by the procedure described in the previous sub-section.

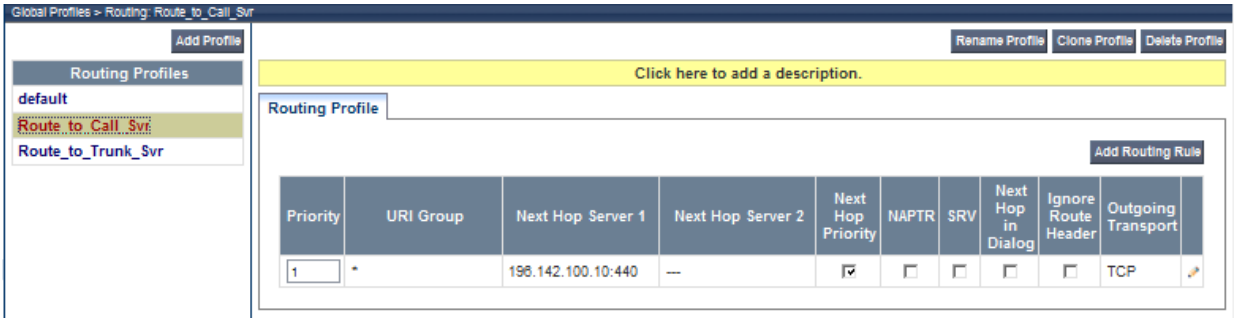


Figure 11-8 Routing Profile Screen

Step-2 Create Topology Hiding Profiles

Note:	Refer to Chapter 7, "Security Configuration," and the section titled, "Topology Hiding Settings Examples," for descriptions of the various Topology Hiding parameters combinations and their resulting actions.

Topology Hiding Profile for Call Server

1. Login to the E-SBC Control Center as the Admin.
2. Select the **Topology Hiding** function of the **Global Profiles** feature from the Task Pane (Figure 11-9).

Note:	A default topology profile can be used. For any specific topology hiding profile, proceed to Step 3.

3. In the Topology Hiding Profile screen that is displayed, click on the **Add Profile** button, which displays the Add Topology Hiding Profile pop-up screen (Figure 11-10).

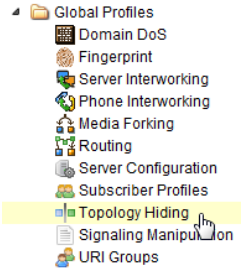


Figure 11-9 Selecting the Topology Hiding Function

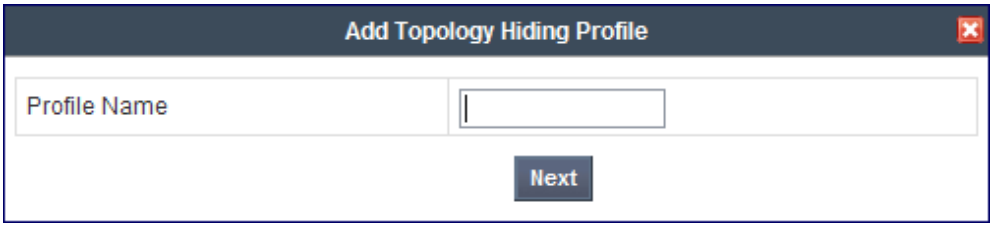


Figure 11-10 Add Topology Hiding Profile Pop-up Screen 1

4. In the Profile Name field, enter a profile name such as: **E-SBC_to _Call_Svr**
5. Click **Next** to display a second Add Topology Hiding Profile pop-up screen similar to the example shown in Figure 11-11.

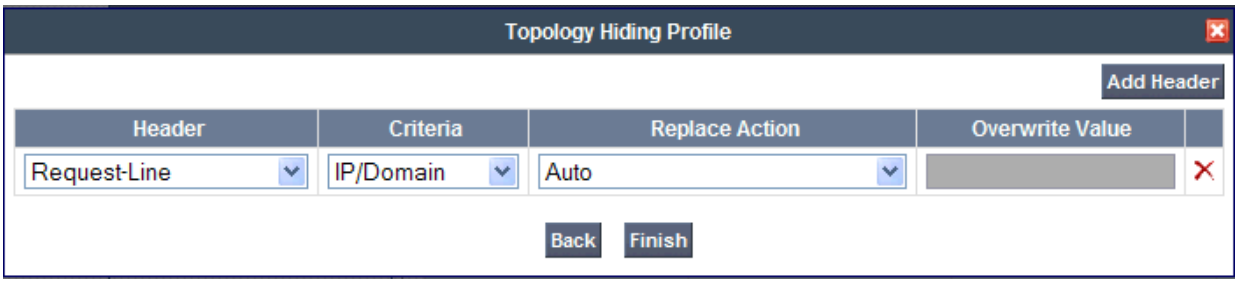


Figure 11-11 Add Topology Hiding Profile Pop-up Screen 2

6. In the second Topology Hiding Profile screen (Figure 11-11), begin to select the chosen parameters by selecting the drop-down list of Header parameters to choose one of the parameters for the new profile as shown in Figure 11-12.

Figure 11-12. Topology Hiding Profile Header Parameters

7. In the second Topology Hiding Profile screen (Figure 11-11), next select the drop-down list of Criteria parameters to choose one of the parameters for the new profile as shown in Figure 11-13.

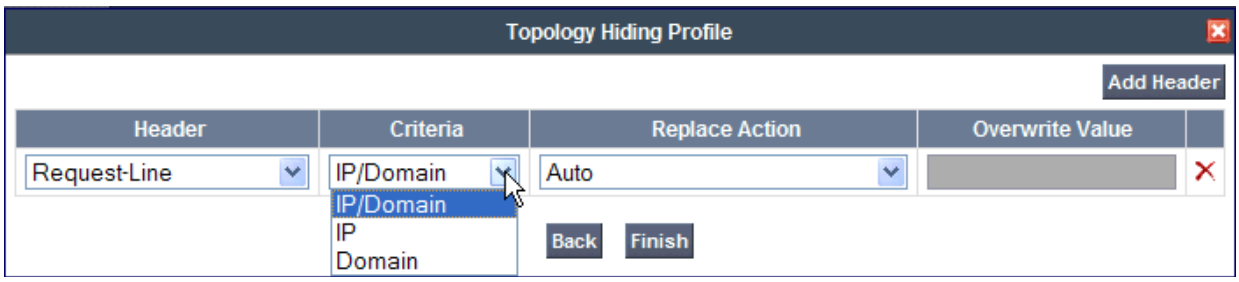


Figure 11-13. Topology Hiding Profile Screen 2 Criteria Parameters

8. In the second Topology Hiding Profile screen (Figure 11-11), next select the drop-down list of Replace Action parameters to choose one of the parameters for the new profile as shown in Figure 11-14.

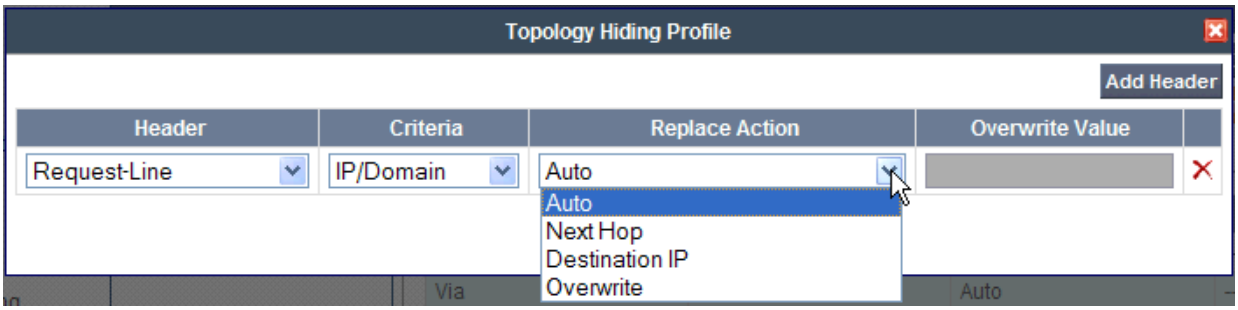


Figure 11-14. Topology Hiding Profile Screen 2 Replace Action

Note:	In the drop-down list in the Replace Action field, shown in Figure 11-14, if you select the action, "Overwrite," the Overwrite Value field to the right will accept entry of a value (i.e., an IP address).

9. After selecting the appropriate values in the Topology Profile fields, select **Finish** to save, submit, and exit.

Topology Hiding Profile for Trunk Server

1. Login to the E-SBC Control Center as the Admin.
2. Select the **Topology Hiding** function of the **Global Profiles** feature from the Task Pane (Figure 11-15).

Note:	A default topology profile can be used. For any specific topology hiding profile, procede to Step 3.

3. In the Topology Hiding Profile screen that is displayed, click on the **Add Profile** button, which displays the Add Topology Hiding Profile pop-up screen similar to the example shown in Figure 11-16.

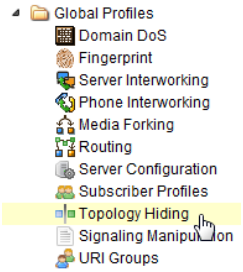


Figure 11-15 Selecting the Topology Hiding Function

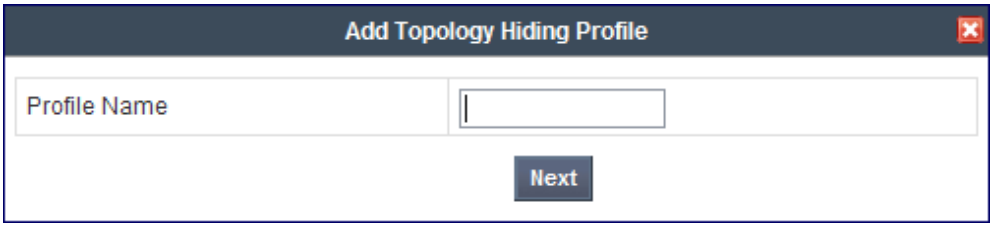


Figure 11-16 Add Topology Hiding Profile Pop-up Screen 1

4. In the Profile Name field, enter the profile name such as: **E-SBC_to _Trunk**
5. Click **Next** to display a second Add Topology Hiding Profile pop-up screen similar to the example shown in Figure 11-17.

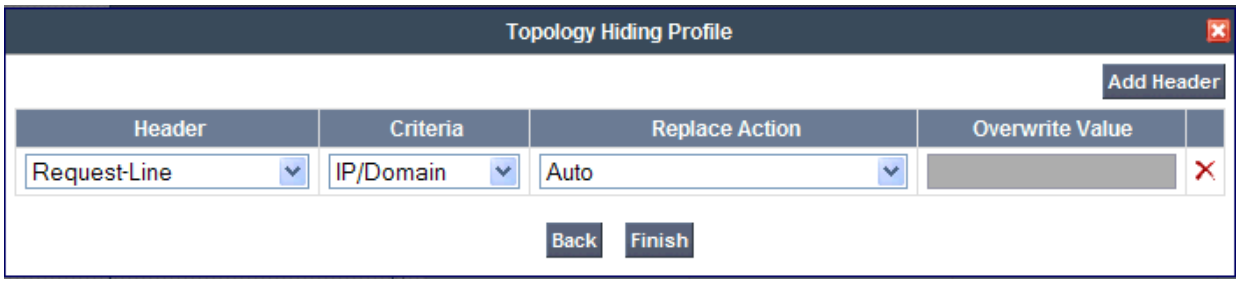


Figure 11-17 Add Topology Hiding Profile Pop-up Screen 2

6. In the second Topology Hiding Profile screen (Figure 11-17), begin to select the chosen parameters by selecting the drop-down list of Header parameters to choose one of the parameters for the new profile as shown in Figure 11-18.

Figure 11-18. Topology Hiding Profile Header Parameters

7. In the second Topology Hiding Profile screen (Figure 11-17), next select the drop-down list of Criteria parameters to choose one of the parameters for the new profile as shown in Figure 11-19.

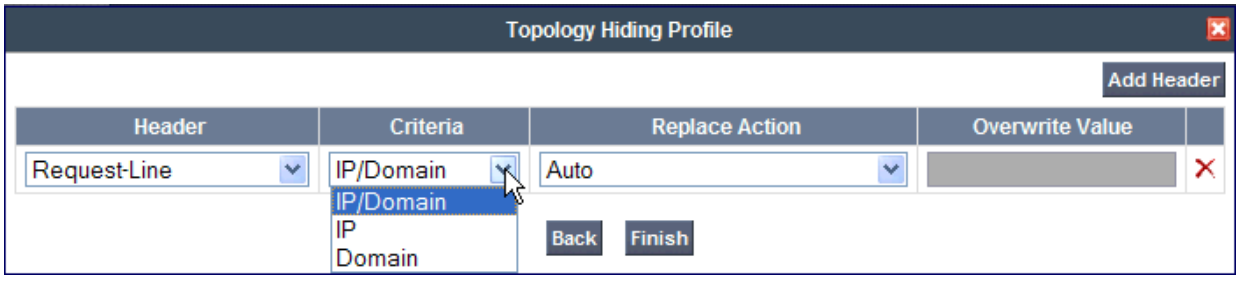


Figure 11-19. Topology Hiding Profile Screen 2 Criteria Parameters

8. In the second Topology Hiding Profile screen (Figure 11-11), next select the drop-down list of Replace Action parameters to choose one of the parameters for the new profile as shown in Figure 11-20.

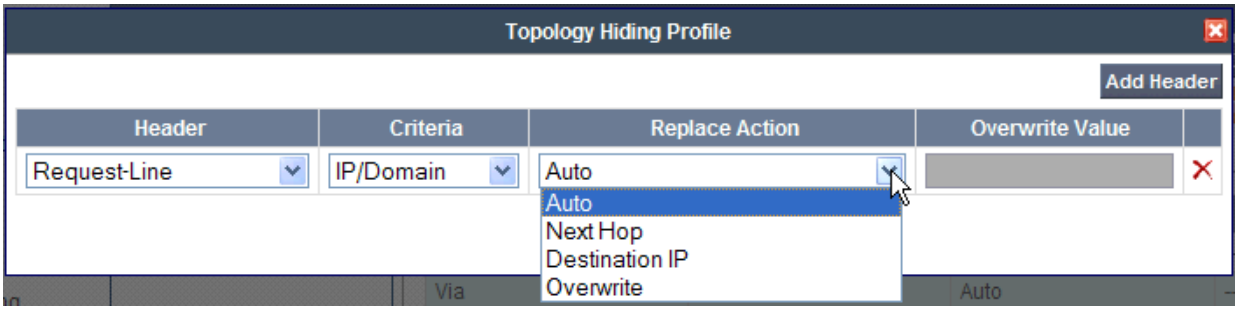


Figure 11-20. Topology Hiding Profile Screen 2 Replace Action

Note:	In the drop-down list in the Replace Action field, shown in Figure 11-20, if you select the action, "Overwrite," the Overwrite Value field to the right will accept entry of a value (i.e., an IP address).

9. After selecting the appropriate values in the Topology Hiding Profile fields, select **Finish** to save, submit, and exit.

Step-3 Create Interworking Profiles

Interworking Profile features are configured based on different Call and Trunk Servers (e.g., Avaya, Cisco, Nortel, etc.).

Note:	**The procedures before and after this section provide generic instructions for SIP trunking configuration that apply to all implementations. Specific instructions are included in a section located at the end of this chapter titled, "Step-8 Server-Specific Configuration for SIP Trunking." Refer to that section for specific instructions applicable to the Trunk Server used in your network.**

1. Login to the E-SBC Control Center as the Admin.
2. Select the **Server Interworking** function of the **Global Profiles** feature from the Task Pane (Figure 11-21).
3. The default Trunk Server profiles, shown in Figure 11-22, can be used as is or modified or a new Trunk Server Profile can be created beginning by clicking on the **Add Profile** button and editing a series of five pop-up edit screens followed by editing another edit pop-up screen that is accessible on the Advance tab of the Global Profiles Server Interworking screen.

Note:	**For details on creating Interworking Profiles see the section titled, "Adding a New Interworking Profile" in Chapter 8.**

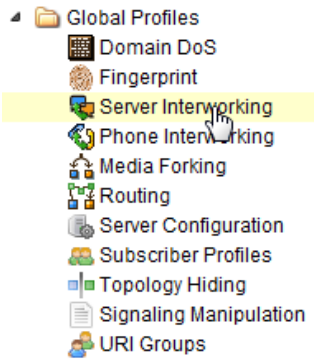


Figure 11-21 Selecting the Server Interworking Function

Figure 11-22. Global Profiles Server Interworking Screen

Step-4 Create Server Profiles

Create Server Profile for Call Server

1. Login to the E-SBC Control Center as the Admin.
2. Select the **Server Configuration function** of the **Global Profiles** feature from the Task Pane (Figure 11-23).
3. In the Server Configuration Profile screen that is displayed, click on the **Add Profile** button, which displays the Add Server Configuration Profile pop-up screen similar to the example shown below in Figure 11-24.

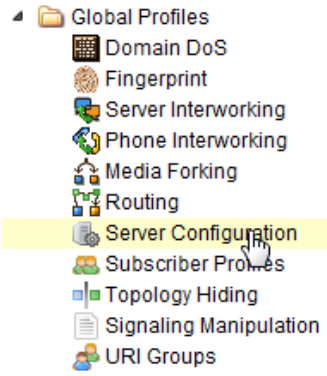


Figure 11-23 Selecting the Server Configuration Function

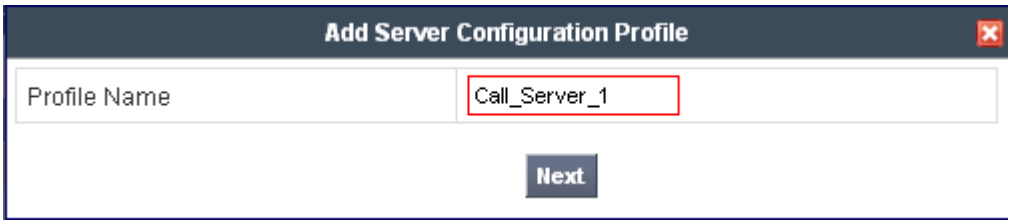


Figure 11-24 Add Server Configuration Profile Pop-up Screen 1

4. In the Add Server Configuration Profile pop-up screen, enter a server name (e.g., Call_Server_1) in the Profile Name field, as shown in the example in Figure 11-24, and click **Next** to display a second Add Server Configuration Profile pop-up screen, similar to the example in Figure 11-25.

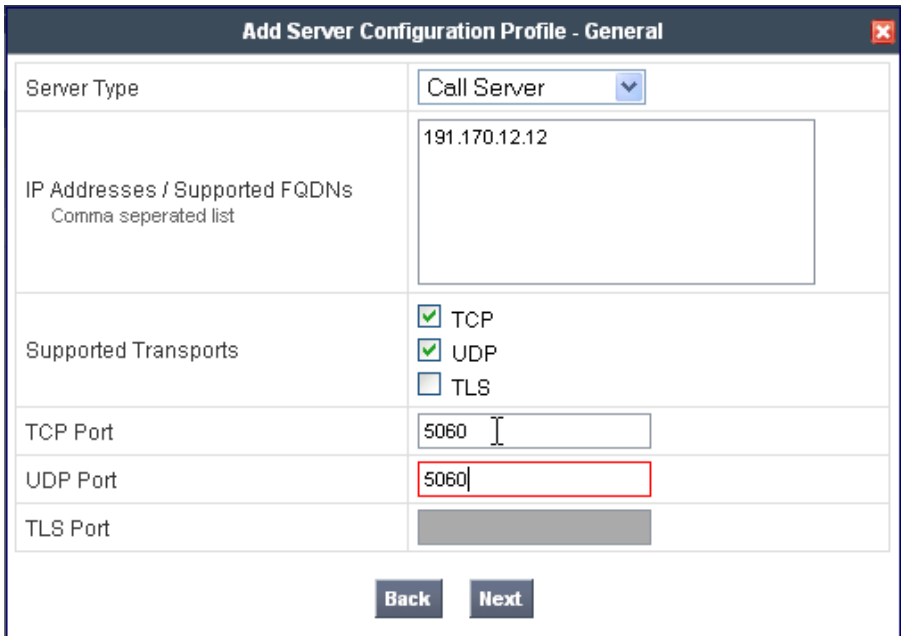


Figure 11-25 Add Server Configuration Profile Pop-up Screen 2

5. In the second Add Server Configuration Profile pop-up screen, in the Server Type field drop-down menu, select **Call Server**.
6. In the IP Addresses / Supported FQDNs edit field, enter the IP address of the call server or its FQDN.
7. In the Supported Transports fields, select the checkboxes for both TCP and UDP.
8. In the TCP Port field enter 5060 and in the UDP Port field enter 5060. Leave the TLS Port field blank. Click Next to display the Add Server Configuration Profile – Authentication screen shown in Figure 11-26.

Note:	**Port number 5060 is the default port number that is used for both TCP and UDP. If your call server uses a different port, enter that value in the Port fields for TCP and UDP.**

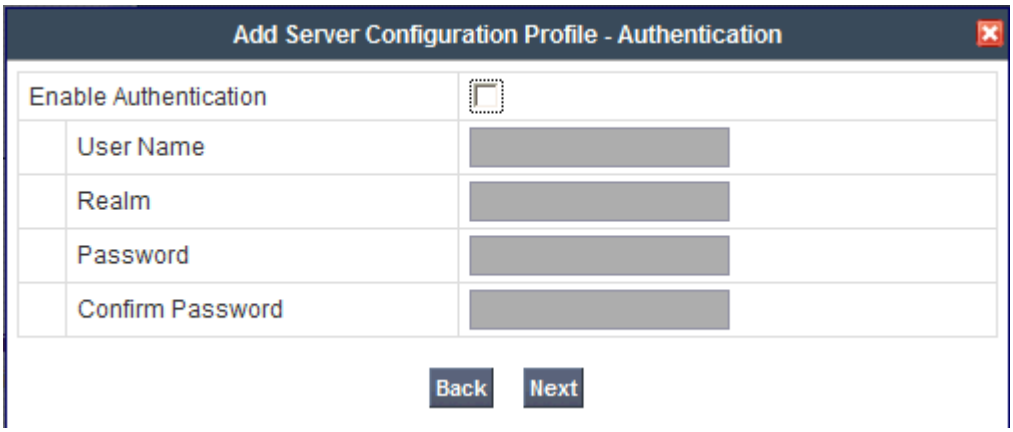


Figure 11-26 Add Server Configuration Profile – Authentication Pop-up Screen

9. Completion of the Add Server Configuration Profile – Authentication screen is optional. If you are using server authentication, enter the related information in this screen. Otherwise, click on **Next** to skip this screen and display the Add Sever Configuration Profile – Heartbeat pop-up screen shown in Figure 11-27 below.

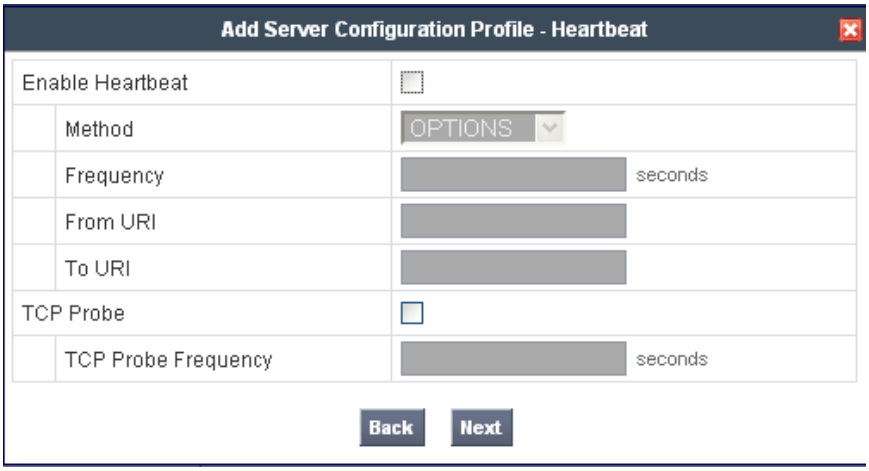


Figure 11-27 Add Server Configuration Profile – Heartbeat Pop-up Screen

10. Completion of the first Add Server Configuration Profile – Heartbeat screen (Figure 11-27) is optional. If you are using the heartbeat feature, enter the related information in this screen. Otherwise, click on **Next** to skip this screen and display the Add Sever Configuration Profile – Advanced pop-up screen shown in Figure 11-28.

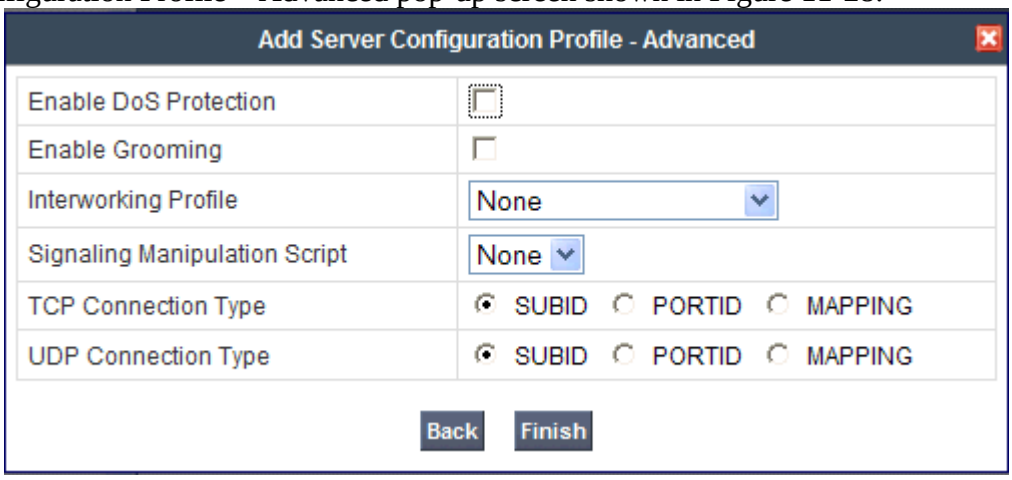


Figure 11-28 Add Server Configuration Profile – Advanced Pop-up Screen

Note:	For more information about DoS protection, see Chapter 7, "Security Configuration." For more information about Signaling Manipulation, see Chapter 12, "Signaling Manipulation."

11. In the Add Server Configuration Profile – Advanced screen (Figure 11-28), in the Interworking Profile drop-down menu, select the profile name (either the name of a default interworking profile or newly-created interworking profile) for your type of call server. In the example shown below in
Figure 11-29, the default interworking profile of **avaya-ru** is selected.

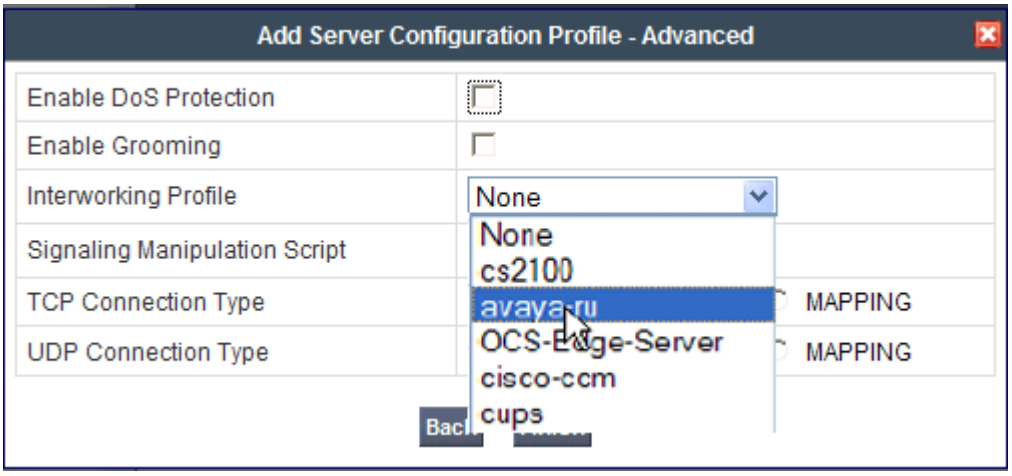


Figure 11-29 Add Server Configuration Profile – Advanced Pop-up Screen (cont)

12. Click the **Finish** button to display an updated Server Configuration Profile information screen, similar to the example in Figure 11-30.

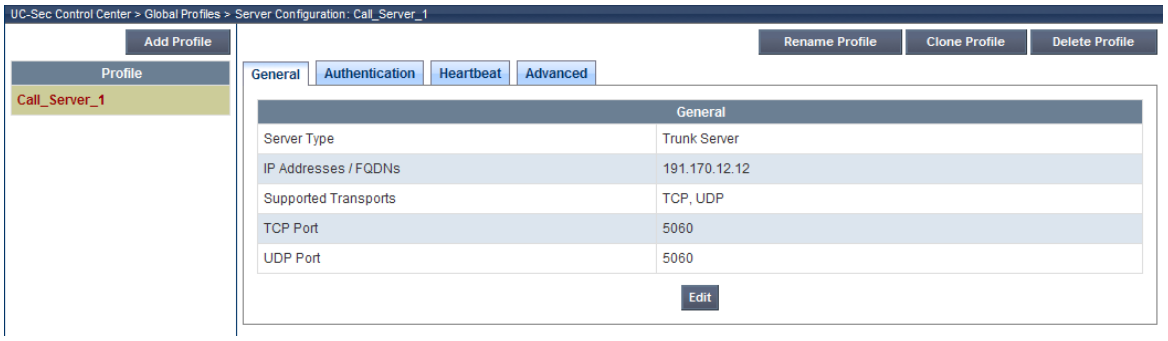


Figure 11-30 Server Configuration Profile Screen

Create Server Profile for Trunk Side Server

1. Login to the E-SBC Control Center as the Admin.
2. Select the **Server Configuration** function of the **Global Profiles** feature from the Task Pane (Figure 11-23).
3. In the Server Configuration Profile screen that is displayed, click on the **Add Profile** button, which displays the Add Topology Hiding Profile pop-up screen similar to the example shown below in Figure 11-31.

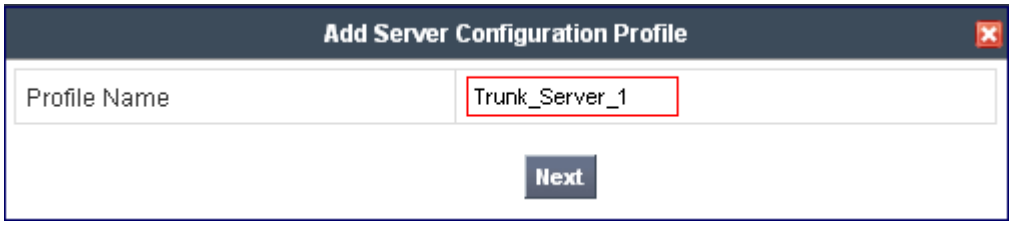


Figure 11-31 Add Server Configuration Profile Pop-up Screen 1

4. In the Add Server Configuration Profile pop-up screen, enter a server name (e.g., Trunk_Server_1) in the Profile Name field, as shown in the example in Figure 11-31, and click **Next** to display a second Add Server Configuration Profile pop-up screen, similar to the example below in Figure 11-32.

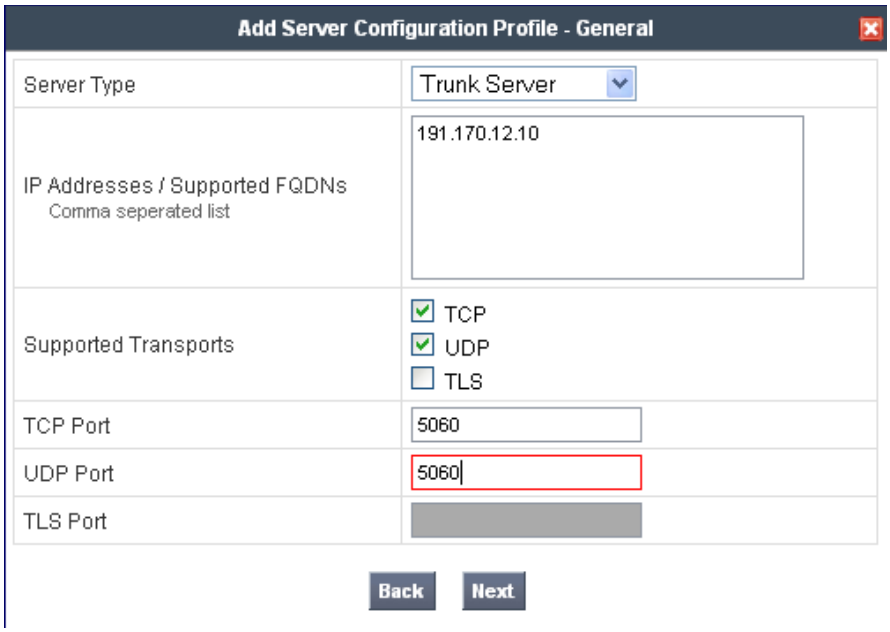


Figure 11-32 Add Server Configuration Profile Pop-up Screen 2

5. In the second Add Server Configuration Profile pop-up screen, in the Server Type field drop-down menu, select **Trunk Server.**
6. In the IP Addresses / Supported FQDNs edit field, enter the IP address of the trunk-side server or its FQDN.
7. In the Supported Transports fields, select the checkboxes for both TCP and UDP.
8. In the TCP Port field enter 5060 and in the UDP Port field enter 5060. Leave the TLS Port field blank. Click Next to display the Add Server Configuration Profile – Authentication screen shown in Figure 11-33.

Note:	**Port number 5060 is the default port number that is used for both TCP and UDP. If your call server uses a different port, enter that value in the Port fields for TCP and UDP.**

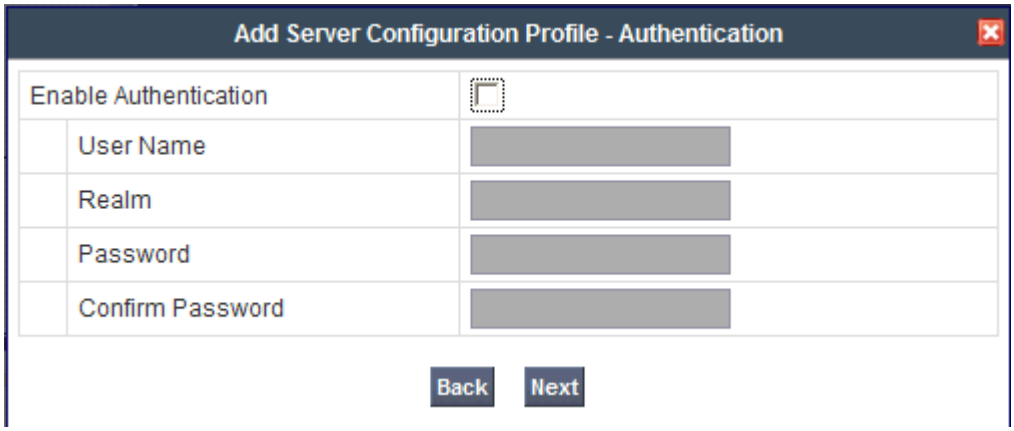


Figure 11-33 Add Server Configuration Profile Authentication Pop-up Screen

9. Completion of the Add Server Configuration Profile – Authentication screen (Figure 11-33) is optional. If you are using server authentication, enter the related information in this screen. Otherwise, click on **Next** to skip this screen and display the Add Sever Configuration Profile – Heartbeat pop-up screen shown in Figure 11-34.

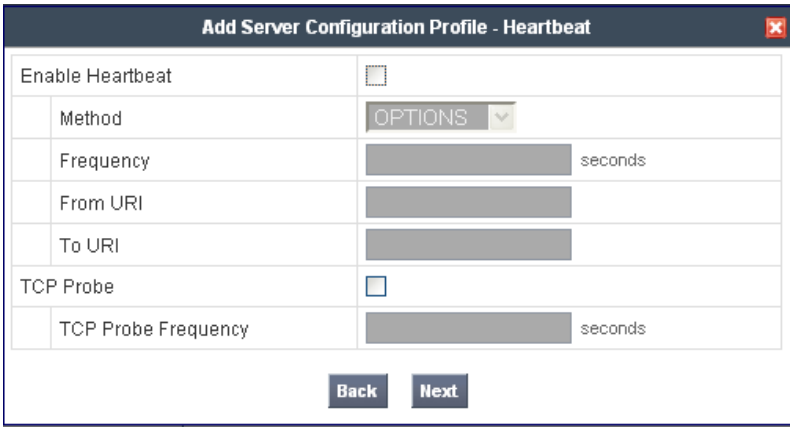


Figure 11-34 Add Server Configuration Profile Heartbeat Pop-up Screen

10. Completion of the Add Server Configuration Profile – Heartbeat screen (Figure 11-34) is optional. If you are using the heartbeat feature, enter the related information in this screen. Otherwise, click on **Next** to skip this screen and display the Add Sever Configuration Profile – Advanced pop-up screen shown in Figure 11-35.

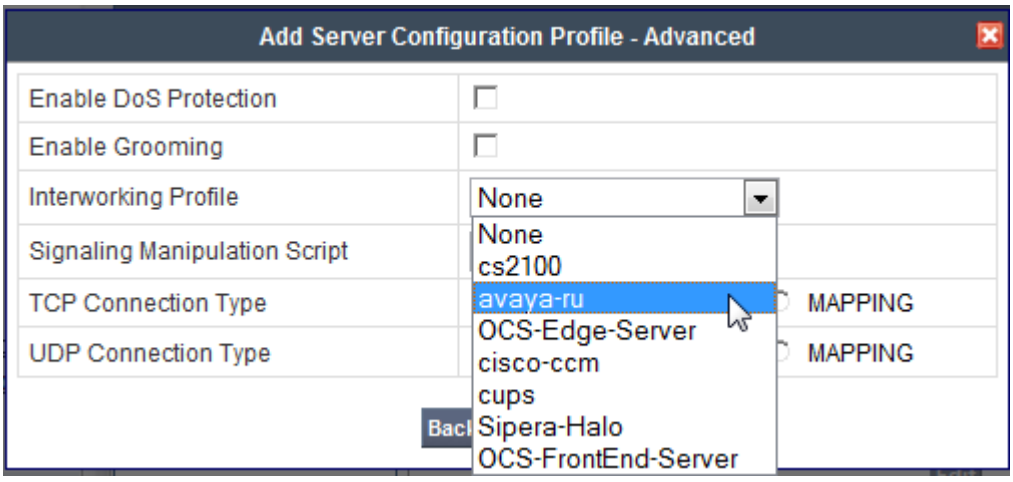


Figure 11-35 Add Server Configuration Profile Advanced Pop-up Screen

Note:	For more information about DoS protection, see Chapter 7, “Security Configuration.” For more information about Signaling Manipulation, see Chapter 12, “Signaling Manipulation.”

11. In the Add Server Configuration Profile – Advanced screen, in the Interworking Profile field drop-down menu, select the profile name (either the name of a default interworking profile or newly-created interworking profile) for your type of call server. In the example in Figure 11-35, the custom interworking profile of **avaya-ru** is selected.

    Click the **Finish** button to display an updated Server Configuration Profile information screen (Figure 11-36).

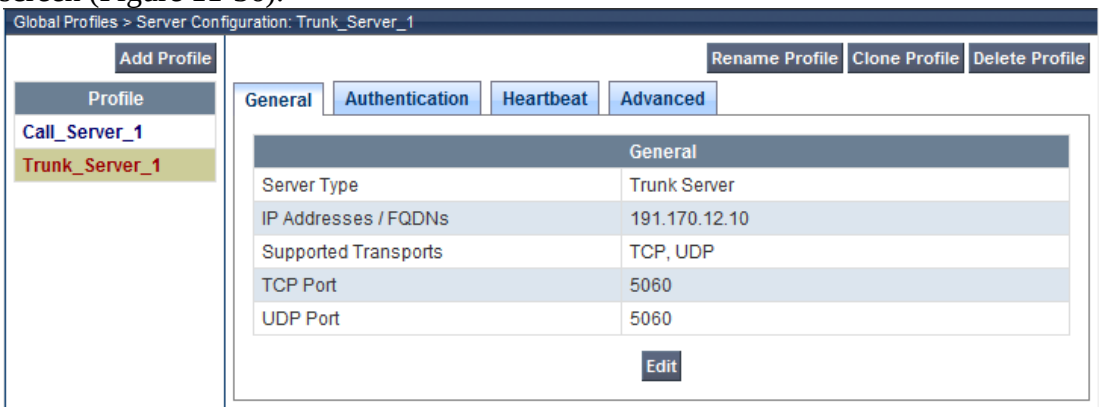


Figure 11-36 Add Server Configuration Profile Screen

Step-5 Create Signaling Interfaces

Create External Signaling Interface toward Trunk Server

1. Login to the E-SBC Control Center as the Admin.
2. Select the **Signaling Interface** function of the **Device Specific Settings** feature from the Task Pane (Figure 11-37).
3. In the Signaling Interface screen that is displayed, click on the **Add Signaling Interface** button on the right-hand side of the screen to display the first Add Signaling Interface pop-up screen similar to the example shown in Figure 11-38 below.

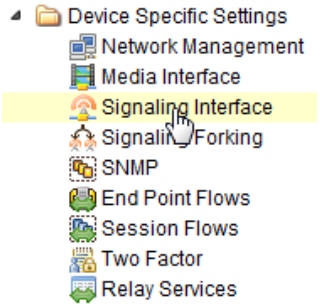


Figure 11-37 Selecting the Signaling Interface Function

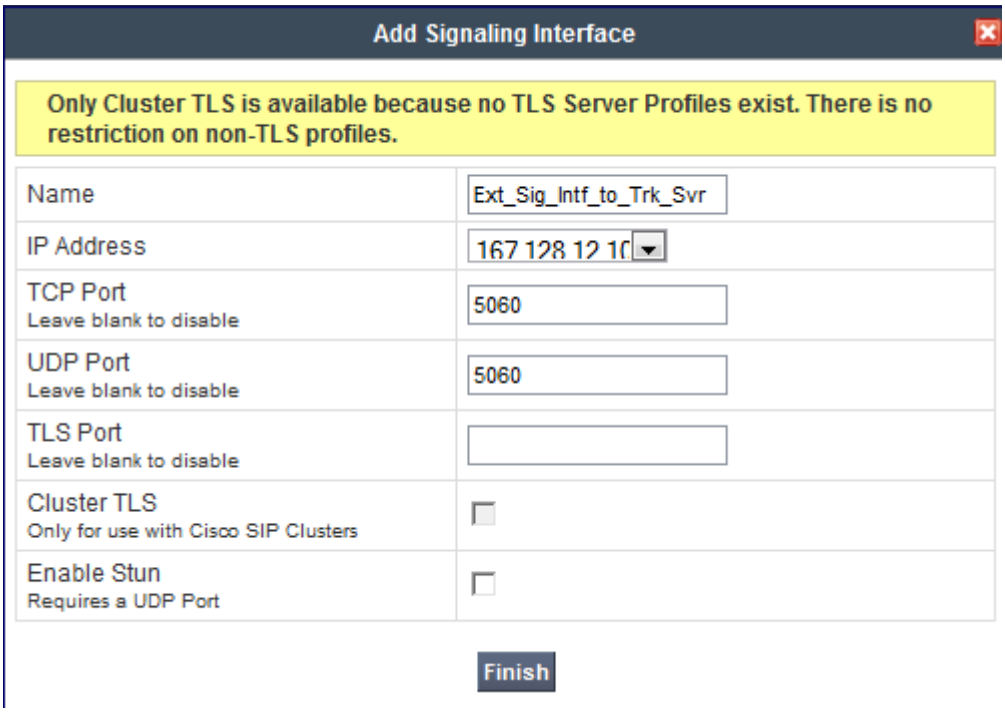


Figure 11-38 Add Signaling Interface Pop-up Screen 1

4. In the first Add Signaling Interface pop-up screen, in the Name edit field, enter a descriptive name for the external signaling interface toward the trunk server.
5. In the IP Address edit field drop-down menu, select the IP address of the external signaling interface.
6. In the TCP Port field enter 5060 and in the UDP Port field enter 5060. Leave the TLS Port field blank. Click **Next** to save and exit.

Note:	**Port number 5060 is the default port number that is used for both TCP and UDP. If your call server uses a different port, enter that value in the Port fields for TCP and UDP.**

Create Internal Signaling Interface Toward Call Server

1. Login to the E-SBC Control Center as the Admin.
2. Select the **Signaling Interface** function of the **Device Specific Settings** feature from the Task Pane (Figure 11-37).
3. In the Signaling Interface screen that is displayed, click on the **Add Signaling Interface** button on the right-hand side of the screen to display the second Add Signaling Interface pop-up screen similar to the example shown in Figure 11-39 below.

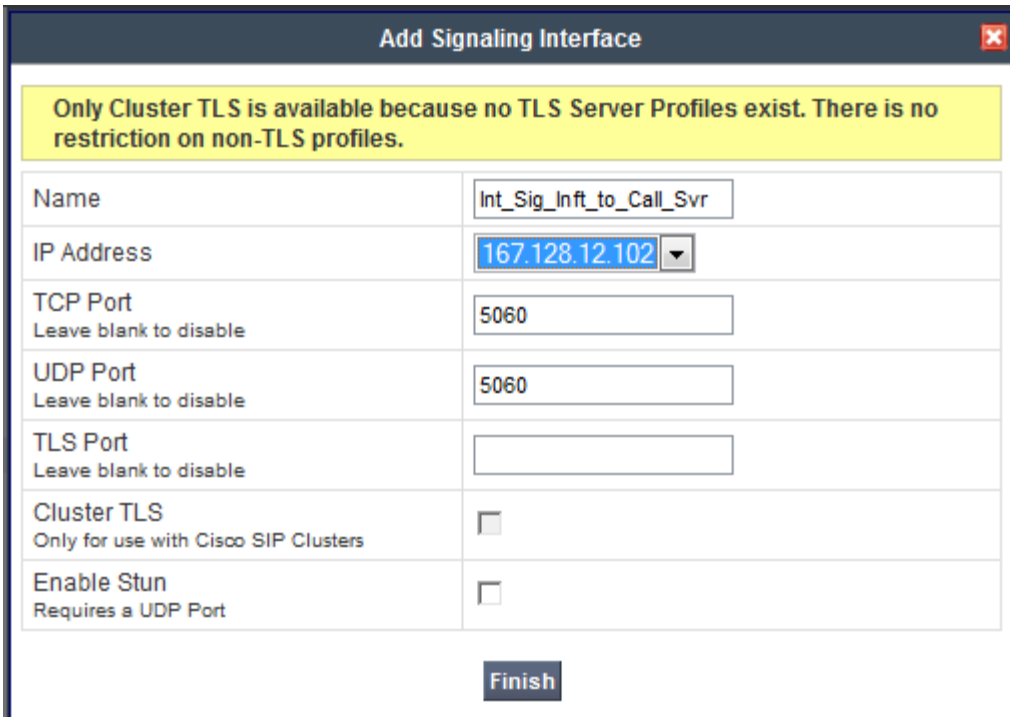


Figure 11-39 Add Signaling Interface Pop-up Screen 2

4. In the second Add Signaling Interface pop-up screen, in the Name edit field, enter a descriptive name for the internal signaling interface toward the call server.
5. In the IP Address edit field drop-down menu, select the IP address of the internal signaling interface.
6. In the TCP Port field enter 5060 and in the UDP Port field enter 5060. Leave the TLS Port field blank. Click **Next** to save, exit, and display the Signaling Interface screen, showing the newly-created internal and external signaling interfaces, similar to the example below in Figure 11-40.

Note:	**Port number 5060 is the default port number that is used for both TCP and UDP. If your call server uses a different port, enter that value in the Port fields for TCP and UDP.**

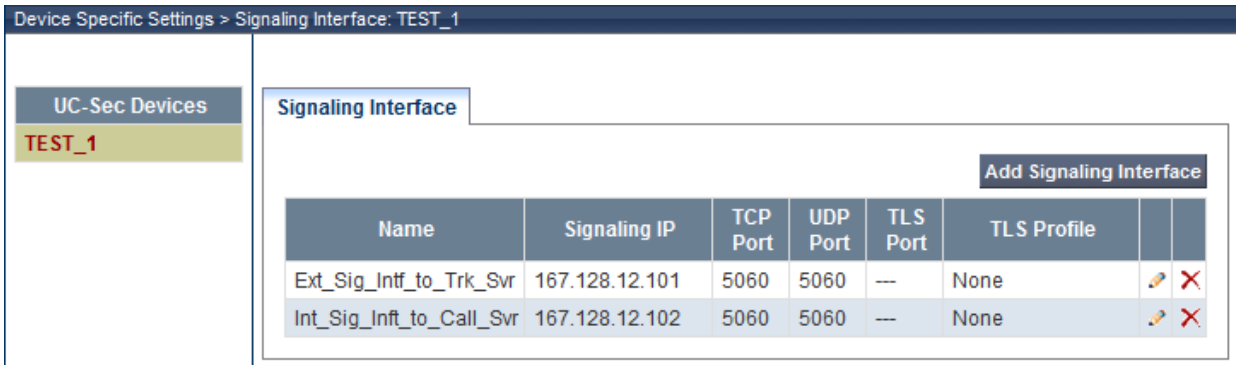


Figure 11-40 Signaling Interface Screen

Step-6 Create Media Interfaces

Create External Media Interface toward Trunk Server

1. Login to the E-SBC Control Center as the Admin.
2. Select the **Media Interface** function of the **Device Specific Settings** feature from the Task Pane (Figure 11-41).
3. In the Media Interface screen that is displayed, click on the Add Media Interface button on the right-hand side of the screen to display the first Add Media Interface pop-up screen similar to the example shown in Figure 11-42 below.

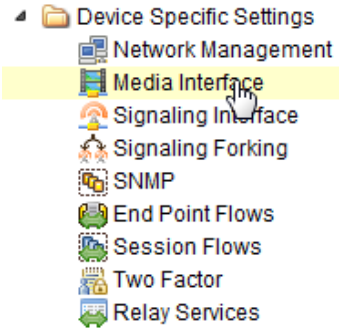


Figure 11-41 Selecting the Media Interface Function

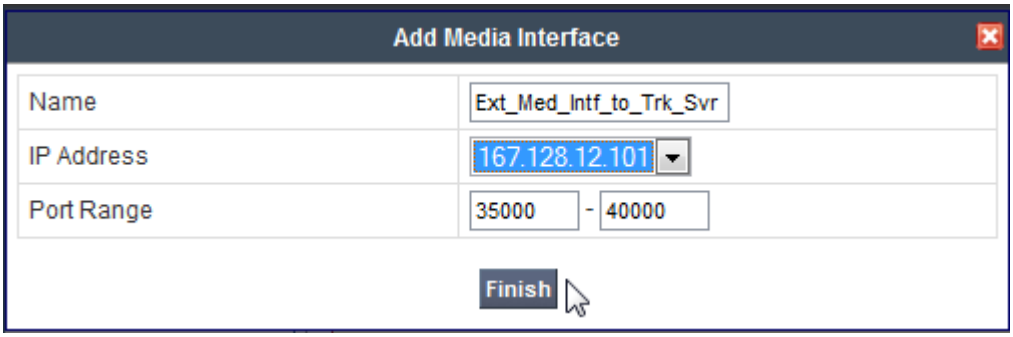


Figure 11-42 Add Media Interface Pop-up Screen 1

4. In the first Add Media Interface pop-up screen similar to the example in Figure 11-42, in the **Name** edit field, enter a descriptive name for the external media interface toward the trunk server.
5. In the IP Address edit field drop-down menu, select the IP address of the external media interface.
6. In the Port Range fields enter starting and ending port range numbers.
7. Click **Finish** to save and exit.

Create Internal Media Interface Toward Call Server

1. Login to the E-SBC Control Center as the Admin.
2. Select the **Media Interface** function of the **Device Specific Settings** feature from the Task Pane (Figure 11-37).
3. In the Media Interface screen that is displayed, click on the Add Media Interface button on the right-hand side of the screen to display the second Add Media Interface pop-up screen, similar to the example shown in Figure 11-43 below.

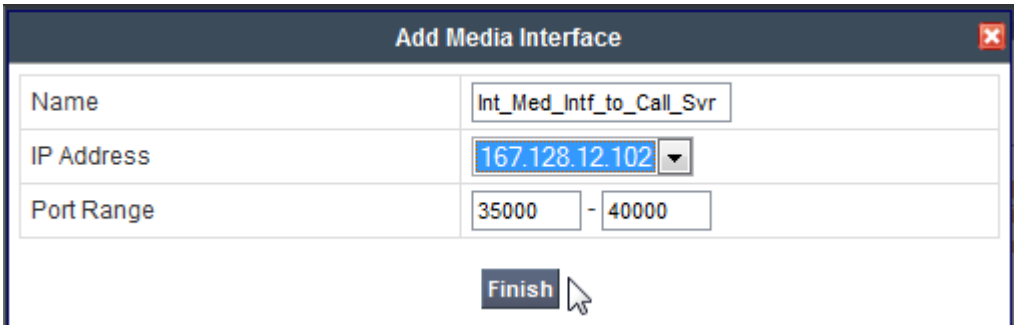


Figure 11-43 Add Media Interface Pop-up Screen 2

4. In the second Add Media Interface pop-up screen, similar to the example in Figure 11-43, in the Name edit field, enter a descriptive name for the internal media interface toward the call server.
5. In the IP Address edit field drop-down menu, select the IP address of the internal media interface.
6. In the Port Range fields enter starting and ending port range numbers.
7. Click **Finish** to save, exit, and display the Media Interface screen, showing the newly-created internal and external media interfaces, similar to the example in Figure 11-44 below.

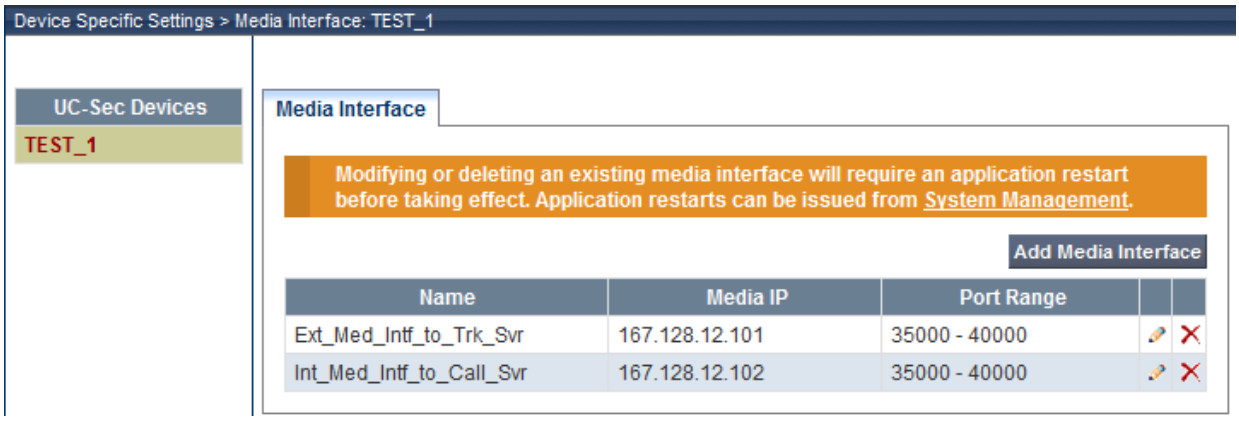


Figure 11-44 Media Interface Screen

Step-7 Create Server Flows

Create Flow toward Call Server

1. Login to the E-SBC Control Center as the Admin.
2. Select the **End Point Flows** function of the **Device Specific Settings** feature from the Task Pane (Figure 11-45) to display the End Point Flows screen.
3. In the End Point Flows screen that is displayed with the default Subscriber Flows tab selected, click on the Server Flows tab to display the Server Flows information screen, as shown in the example below in Figure 11-46.

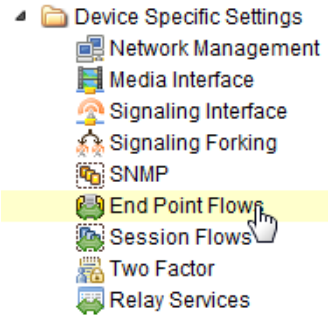


Figure 11-45 Selecting the End Point Flows Function

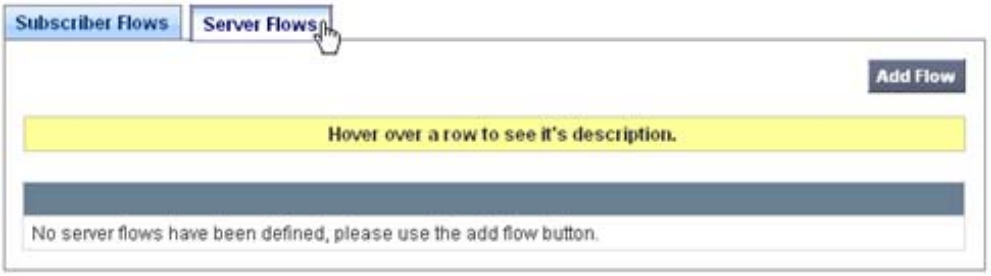


Figure 11-46 End Point Server Flows Information Screen

4. Click on the Add Flow button on the right-hand side of the screen to display the **Add Flow** pop-up screen, similar to the example shown in Figure 11-47.

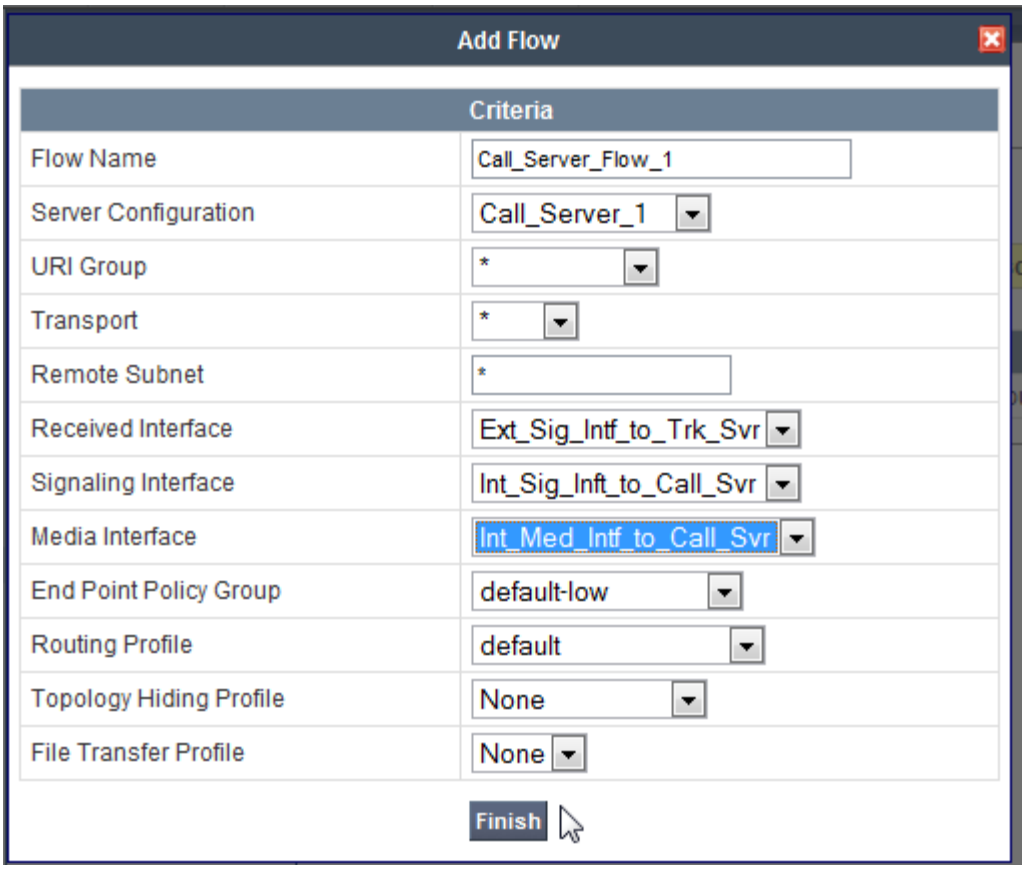


Figure 11-47 Add Flow Pop-up Screen

5. In the Add Flow Criteria pop-up screen, in the Flow Name field, enter the Flow name as "Call_Server_Flow_1."
6. In the Server Configuration field drop-down menu, select the profile name (e.g., **Call_Server_1**) of the call (line side) server profile, as shown in the example in Figure 11-47.
7. Leave the URI Group, Transport, and Remote Subnet fields set to the default (*). The fields are changed based on customer requirements.
8. In the Received Interface field drop-down menu, select the name (e.g., **Ext_Sig_Intf_to_Trk_Svr**) of the interface pointing toward the trunk server, as shown in Figure 11-47.
9. In the Signaling Interface field drop-down menu, select the name (e.g., **Sig_Intf_Int_to_Call_Server**) of the interface pointing toward the call server, as shown in Figure 11-47.
10. In the Media Interface field drop-down menu, select the name of the interface (e.g., **Int_Med_Intf_to_Call_Svr)** pointing toward the call server, as shown in Figure 11-47.
11. Leave the End Point Policy Group field set to the default (i.e., default-low). The fields are changed based on customer requirements.
12. In the Routing Profile field drop-down menu, select the name of your previously created Routing Profile.

13. In the Topology Hiding Profile field drop-down menu, select the name of your previously created Topology Hiding Profile or select the default (i.e., None).
14. Leave the File Transfer Profile field set to the default (i.e., None).
15. Click **Finish** to save, exit, and re-display the Server Flows information screen showing the newly-created server flow, similar to the example shown in Figure 11-48.

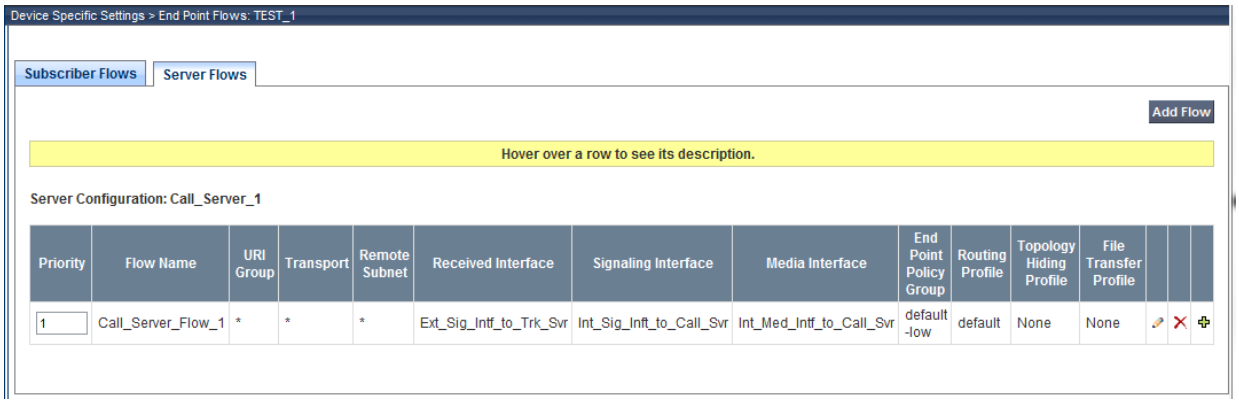


Figure 11-48 Updated Add Flow Pop-up Screen

Create Flow Toward Trunk Server

1. Login to the E-SBC Control Center as the Admin.
2. Select the **End Point Flows** function of the **Device Specific Settings** feature from the Task Pane (Figure 11-45) to display the End Point Flows screen.
3. In the End Point Flows screen that is displayed with the default Subscriber Flows tab selected, click on the Server Flows tab to display the Server Flows information screen.
4. In the Server Flows information screen, click on the Add Flow button on the right-hand side of the screen to display the **Add Flow** pop-up screen, similar to the example in Figure 11-49 shown below.
5. In the Flow Name field, enter a name (e.g., Trunk_Server_Flow_1) for the call server flow toward the call server.

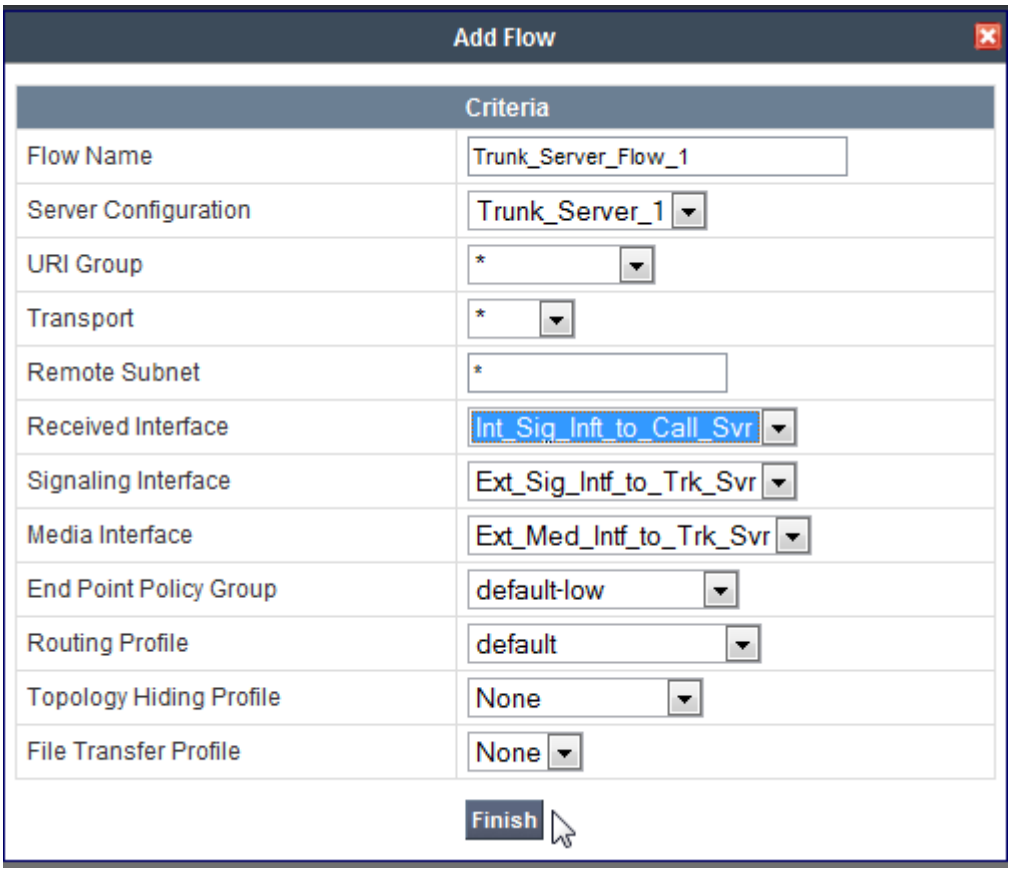


Figure 11-49 Add Flow Pop-up Screen

6. In the Server Configuration field, from the drop-down menu, select the call server profile that you created previously in the first part of Step-4 (i.e., Config_Server_2).
7. Leave the From URI Group, Transport, and Remote Subnet fields set to the default (*).The fields are changed based on customer requirements.
8. In the Received Interface field drop-down menu, select the name (e.g., **Int_Sig_Intf_to_Call_Svr**) of the interface pointing toward the call server, as shown in Figure 11-49.
9. In the Signaling Interface field, from the drop-down menu, select the external signaling interface toward the trunk-side server that was created previously in the first part of Step-5 (i.e., **Ext_Sig_Intf_to_Trk_Svr**, shown selected in Figure 11-49).
10. In the Media Interface field, from the drop-down menu, select the internal media interface toward the phone network that was created previously in the first part of Step-6 (i.e., **Ext_Med_Intf_to_Trk_Svr**, shown already selected in Figure 11-49).
11. Leave the End Point Policy Group field set to the default (i.e., default-low). The fields are changed based on customer requirements.
12. In the Routing Profile field drop-down menu, select the name of your previously created Routing Profile.
13. In the Topology Hiding Profile field drop-down menu, select the name of your previously created Topology Hiding Profile or select the default (i.e., None).

14. Leave the File Transfer Profile field set to the default (i.e., None).
15. Click **Finish** to save and exit, and then click on the Server Flows tab to display the Server Flows information screen, showing the newly-created call server and trunk-side server flows, similar to the example in Figure 11-50 below.

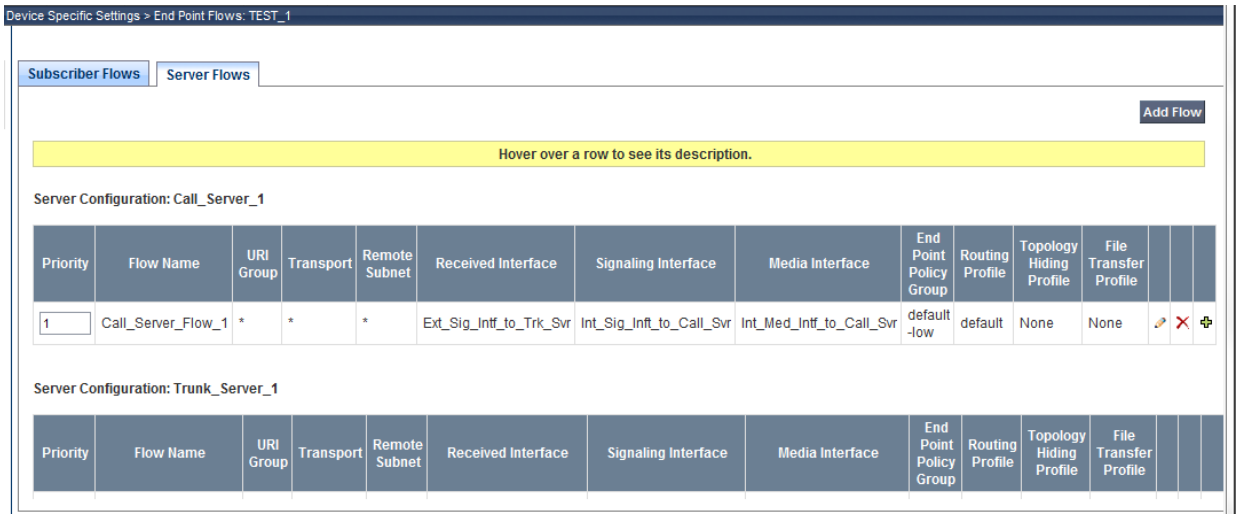


Figure 11-50 Server Flows Information Screen

Step-8 Server-Specific Configuration for SIP Trunking

E-SBC Configuration for Avaya Trunk

1. Perform all of the previous steps (i.e., Step-1 through Step-7), needed for all trunk configurations, including a SIP trunk with Avaya. One particular parameter setting (i.e., Interworking Profile) must be specifically selected, as detailed below.

Note:	**Topology Hiding, described in Step-2 of the generic SIP trunking procedure, is a requirement for Avaya SIP trunking.**

2. Login to the E-SBC Control Center as the Admin.
3. Select the **Server Configuration** function of the **Global Profiles** feature from the Task Pane (Figure 11-51).

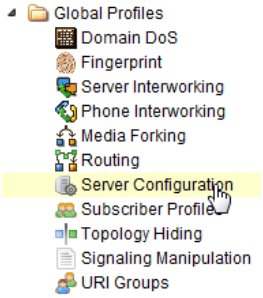


Figure 11-51. Selecting the Server Configuration Function

4. Server Configuration screen that is displayed with the default General tab selected, in the profile list, select the trunk server name (e.g., **Trunk_Server_1**) of the server previously created in part two of Step-4.
5. Click on the **Advanced** tab to display the trunk server information screen, as shown in the example below in Figure 11-52.

Note:	**In the server configuration screen example below, the Interworking Profile field already has the correct profile (e.g., avaya-ru) selected for the Avaya server. If the correct profile is not selected for Avaya, continue with the remaining steps.**

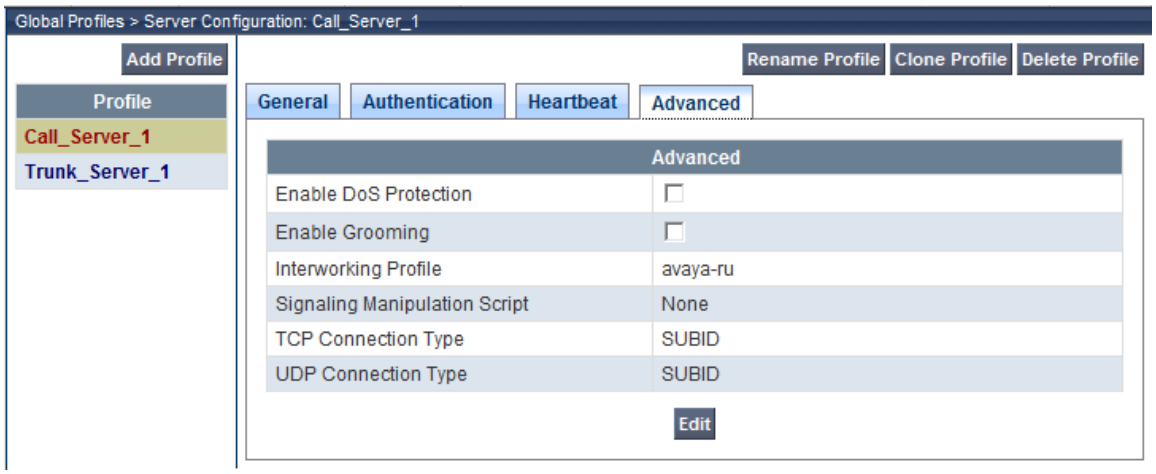


Figure 11-52 Server Configuration Advanced Tab Screen

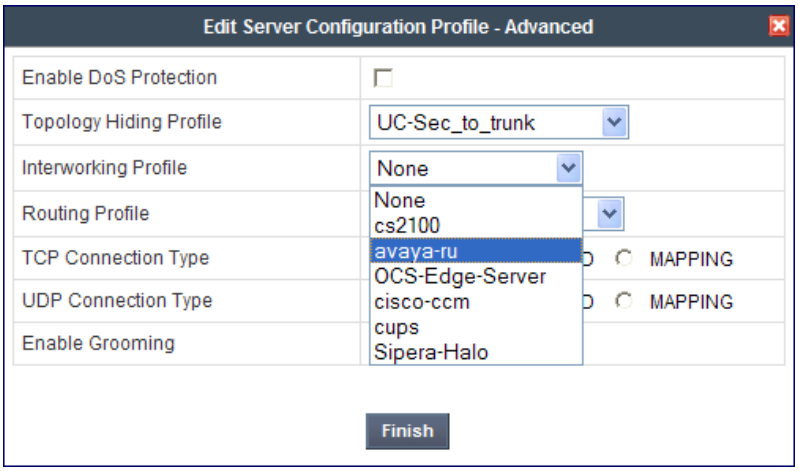


Figure 11-53 Server Configuration Advanced Edit Pop-up Screen

6. If the correct Interworking Profile name for Avaya is not selected in the Advanced Tab screen (Figure 11-52), click the **Edit** button to display the Advanced Edit Pop-up screen (Figure 11-53), and select the profile name for the Avaya Interworking Profile.
7. Click **Finish** to save and exit.
8. Select the **Server Interworking** function of the **Global Profiles** feature from the Task Pane (Figure 11-54).

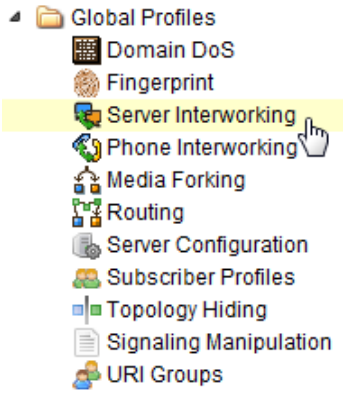


Figure 11-54. Selecting the Server Interworking Function

9. Select the **avaya-ru** default Interworking Profile from the Interworking Profiles list on the left and select the Advanced Tab in the Server Interworking screen (Figure 11-55).

Figure 11-55. Server Interworking Advanced Tab

10. Click the Edit button at the bottom of the screen to display the Advanced Edit window (Figure 11-56).

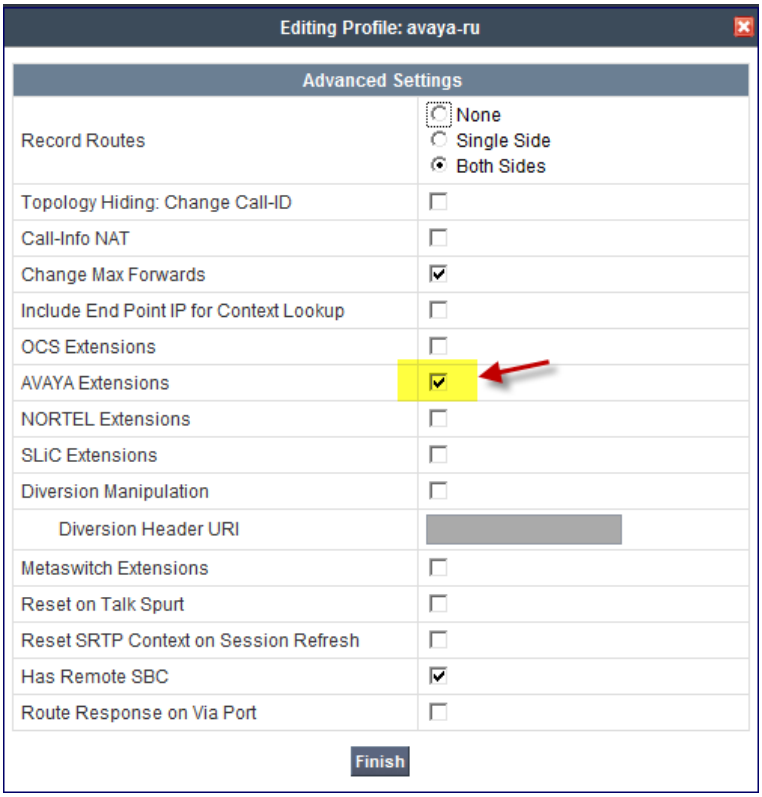


Figure 11-56. Server Interworking Advanced Edit Window

11. Deselect the **Avaya Extensions** checkbox.
12. Click **Finish** to save and exit.

13. Select the General Tab in the Server Interworking screen (Figure 11-57).

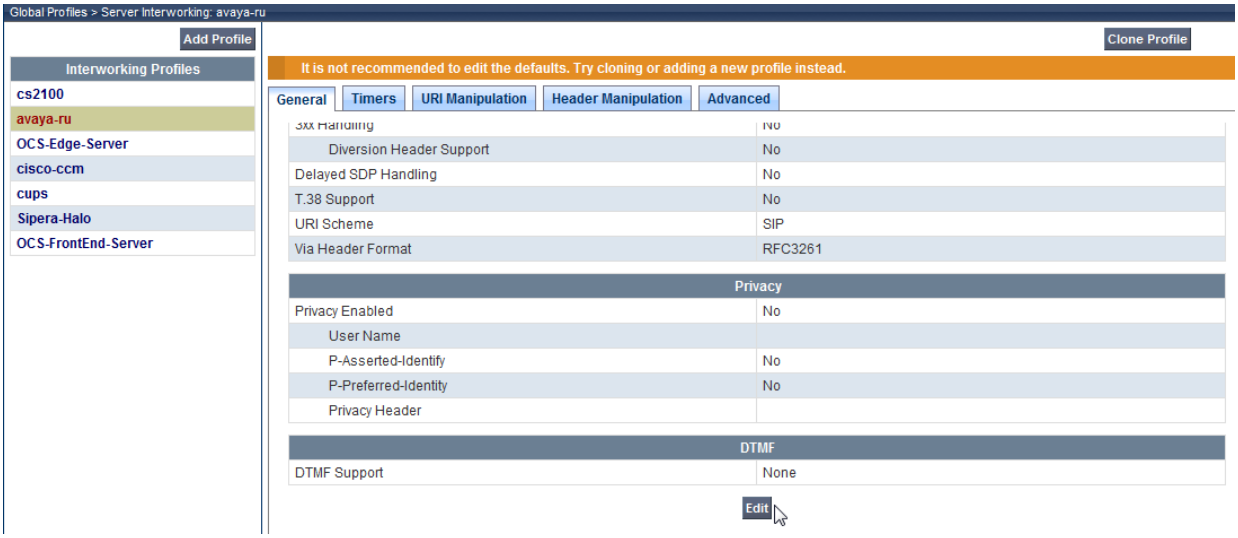


Figure 11-57. Server Interworking General Tab

14. Click the Edit button at the bottom of the screen to display the General Edit window (Figure 11-58).

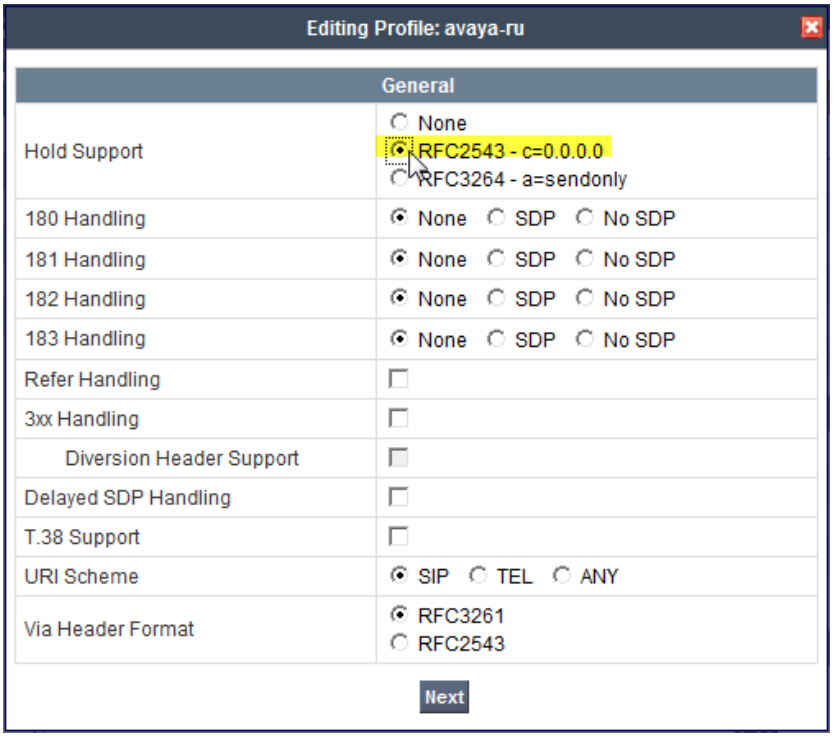


Figure 11-58. Server Interworking General Edit Window

15. In the **Hold Support** parameter field, select **RFC2453** checkbox.
16. Click **Next** in this screen and click **Finish** in the next screen to save and exit.

E-SBC Configuration for Cisco

1. Perform all of the previous steps (i.e., Step-1 through Step-7), needed for all trunk configurations while replacing some of the steps with the exceptions which follow.
2. In Step 4 – "Create Server Profiles," in the sub-section, "Create Server Profile for Call Server," in sub-step 11, instead of selecting the **avaya-ru** Interworking Profile, select the **cisco-ccm** Interworking Profile.

3. In Step 4 – "Create Server Profiles," in the sub-section, "Create Server Profile for Trunk Side Server," in sub-step 10, instead of selecting the **avaya-ru** Interworking Profile, select the **cisco-ccm** Interworking Profile.

E-SBC Configuration for Other Trunks

Perform all of the previous steps (i.e., Step-1 through Step-7), needed for all trunk configurations, including parameter settings that are specific to the type of trunk server being configured.

Different server interworking features will need to be enabled for different trunk servers based on customer requirements. If a default Interworking Profile is not available, then a new one must be configured by following the instructions in the section titled, "Adding a New Interworking Profile," in Chapter 8.

Signaling Manipulation 12

Signaling Manipulation

This application note provides an overview of Sipera's SIP signaling header manipulation feature for the E-SBC product. This feature adds the ability to add, change and delete any of the headers and other information in a SIP message. The feature will add the ability to configure such manipulation at each flow level in a highly flexible manner using a proprietary scripting language that will be presented in sections that follow.

This application note describes Sipera's SIP signaling header manipulation feature as follows:

- **SigMa Scripting Language** – The proprietary scripting language developed by Sipera to define any SIP message manipulation that will be performed by E-SBC.
- **Packet Path and Hook Points** – The packet path where a message transverses through the E-SBC stack and the hook points within the path where actions defined in a SigMa script can be acted upon.
- **E-SBC GUI SigMa Editor** – Access to the SigMa Editor for creating SIP signaling manipulation scripts is provided through the standard E-SBC Configuration/Management Graphical User Interface.

SigMa Scripting Language

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the E-SBC. Using this language, one can write a script and tie it to a given flow through the EMS GUI. The E-SBC appliance then interprets this script at the given "hook point" (See Hook Points on page 10).

SigMa Primer

A SigMa script consists of one or more "Within Session" statements. Each of these statements represents transformations to be applied to signaling messages in a given session. A Session is defined as a SIP dialog and has the same lifetime as that of a dialog. These transformations can be applied on any given header including SDP elements. The transformations also include addition and deletion of headers, not just the ability to update the headers.

Session Statement

The Session Statement has three parts:

- **Method** – The Method statement is where you specify the SIP request method that initiates the session.
- **Where Clause** – The Where Clause statement is used to specify the Session selection criteria on top of the Method for which the *Code Block* needs to be executed.
  The Session selection criteria can be augmented using AND / OR conjunctions.
  The variables that can be used within the Where Clause are given in the table below.

Table 12-1 Where Clause Variables

Variable	Description
%INITIAL_REQUEST	**This is a Boolean variable ("TRUE" or "FALSE") denoting if the code applies to the first request within a session.**

- **Code Block** – The Code Block is where the operations are written and encapsulated with a set of braces {}. The operations may include further selection criteria and actual operations on headers themselves.
  There are three different statements that can be written within the code block:
  - `act on message where <extra criteria> { <code> }` – Tells the interpreter to run the given code on all messages within the SigMa session that match the criteria.
  - `act on request where <extra criteria> { <code> }` – Tells the SigMa interpreter to run the given code on all request messages within the session that match the criteria.
  - `act on response where <extra criteria> { <code> }` – Tells the interpreter to run the given code on all response messages within the session that match the criteria.

Note: There can be as many of the above statements written in a given session code block, as needed for a given script.

Act On Statements

Act On statements define the actions to be taken for each type of a method/methods within a session. Act On message statement tells the code interpreter to execute the given code block for all messages within the given session that match the criteria. Similarly, the Act On request and response statements tell the interpreter to execute the given code for all requests and responses respectively if the given criteria in the Where Clause has matched. The Where Clause specifies this criteria. Much like the Session's Where Clause, several Session Variables can be checked against to specify the matching criteria. The Session Variables that are valid in this clause are given in the table below.

Table 12-2 Session Variables

Variable	Description	Applicable For
%DIRECTION	This value can be "INBOUND" for incoming messages or "OUTBOUND" for outgoing messages from E-SBC.	act on message act on request act on response
%ENTRY_POINT	Values can be: • PRE_ROUTING • POST_ROUTING • AFTER_NETWORK These values are explained in a separate section below.	act on message act on request act on response
%METHOD	Values can be: • INVITE • REGISTER • ACK • PRACK • BYE • CANCEL, and • etc The method name could be any method either already part of standards or proprietary.	%METHOD

Variable	Description	Applicable For
%IN_DIALOG	This is a Boolean variable. Takes either "TRUE" or "FALSE". This indicates if the given message is a in-dialog message or a dialog creating message.	act on request
%RESP_CODE	Represents a valid SIP response code. Any value between [100, 600] is a valid one.	act on response
%REQ_METHOD	Same as METHOD. But it represents for which method the given response corresponds to.	act on response

Code Blocks

The code blocks for the act on statements will contain the code necessary to carry out actions. There are three kinds of statements that can go into the code block:

- **Assignment Statement**. For Example:
  - %var = "1";
  - %var = HEADERS["From"][0];
  - HEADERS["From"][0] = "From: Alice <sip:alice@atlanta.com>;tag=1928301774"
  - HEADERS["To"][0] = %val;
- **Conditional Statement**. This statement takes the following form:

```
if (%var = "value") then
{
        …Code…
}
else
{
        …Code…
}
```

  - The operators can be:
    - == for equality
    - != for negation of equality
  - Either side of the operators can be a variable, a quoted string, any of the built-in arrays' values or a regular expression `get()/match()` call.
  - If the condition is true then the code in the `then {}` block is executed otherwise the `else {}` block will be executed.
- **Function Call**. A function call is usually called on a built-in function. They are the following:
  - `remove()`: to remove a header
  - `append()`: to append string to a header
  - `regex_replace()`: to replace text within a header using a regular expression.
- **Print Statement**. A Print statement prints the parameters given into the log file of the process as an INFO level log. The parameters need to be separated by commas and can be any of – free string in quotes, variables or any of the built-in variables.
  - `print "foo", "bar";`
  - `print "Body(1) is - ", %BODY[1];`

Built-In Variables and Arrays

There are several built-in variables and arrays in SigMa, each representing a data element concerning the session and its messages. The most important ones are the `%HEADERS[]` and `%SDP[]` arrays that are used to retrieve the headers and SDP elements for a given message. They also have a built-in hierarchy to represent the various elements within headers and SDP specification.
They are explained Table 12-3, Table 12-4, and Table 12-5.

Table 12-3 Built-In Variables and Arrays - %HEADERS[] Variable

Variable	Valid Forms	Description
%HEADERS[]	%HEADERS[“Name”][n]	Used to retrieve an entire header. The second dimension ‘n’ denotes the nth instance of the header in the message. Value of n can be 1...∞
	HEADERS[“Name”][n].PARAMS[“Name”]	Used to retrieve parameters within a header.
	%HEADERS[“Name”][n].DISPLAY_NAME	Refers to display name within a header.
	%HEADERS[“Name”][n].URI	Refers to the URI within a header.
	%HEADERS[“Name”][n].URI.USER, %HEADERS[“Name”][n].URI.HOST, %HEADERS[“Name”][n].URI.PORT, %HEADERS[“Name”][n].URI.SCHEME, %HEADERS[“Name”][n].URI.PARAMS[“Name”]	Refer to various elements within a URI.

Note: See the illustration and examples of the %HEADERS[] variable in Figure 12- 1.

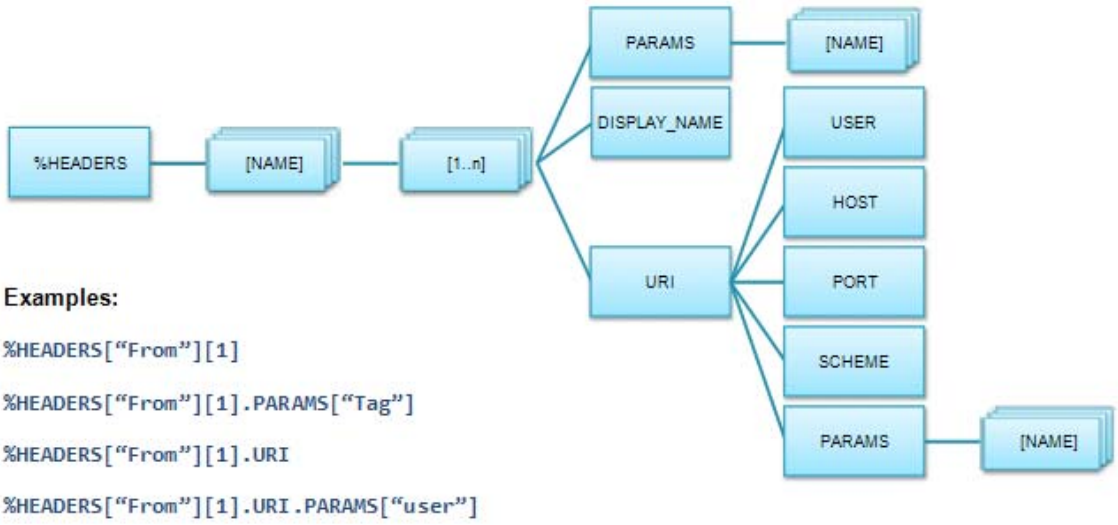


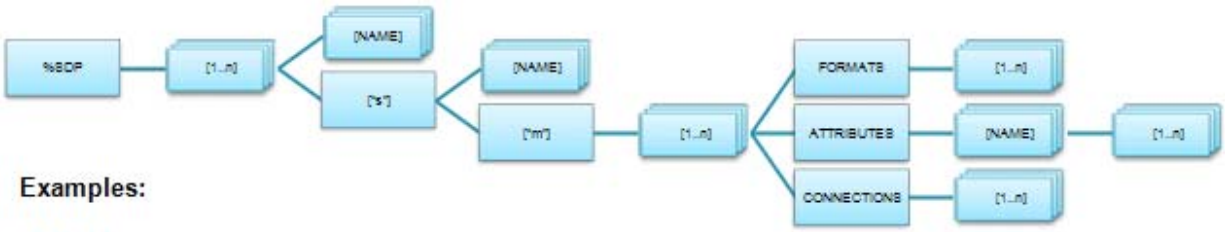
Figure 12- 1 Built-In Variables and Arrays - %HEADERS[] Variable

Table 12-4 Built-In Variables and Arrays - %SDP[] Variable

Variable	Valid Forms	Description
%SDP[]	%SDP[n]	Refers to an entire nth SDP specification. Index n can be 1…∞.
	%SDP[n]["Name"]	Refers to a header within an SDP.
	%SDP[n]["Name"]["SessionHdrName"]	Refers to a session header (like media) within an SDP session.
	%SDP[m]["s"]["m"][n]	Refers to nth media specification.

Variable	Valid Forms	Description
	%SDP[1]["s"]["m"][n].FORMATS[n]	Refer to nth media format specification.
	%SDP[j]["s"]["m"][k].ATTRIBUTES["Name"][n]	Refer to nth instance of "Name" attribute in the kth media specification.
	%SDP[m]["s"]["m"][n].CONNECTIONS[k]n]	kth connection from nth media specification.

Note: See the illustration and examples of the %SDP[] variable in Figure 2 .



Examples:

```
%SDP[1]
%SDP[1]["v"]
%SDP[1]["s"]["t"]
%SDP[1]["s"]["m"][k].FORMATS[1]
%SDP[1]["s"]["m"][k].ATTRIBUTES["fmtp"][1]
```

Figure 12-2 Built-In Variables and Arrays - %SDP[] Variable

Table 12-5 Built-In Variables and Arrays - Other Variables

Variable	Valid Forms	Description
%INITIAL_REQUEST		Set to “TRUE” or “FALSE” based on the request being the first one in the session or not.
%REMOTE_IP		Set to the remote IP within the message.
%BODY	%BODY[n]	Returns the nth mime from the body of the message. Returns the entire body (by mime instance) of the message.

Built-In Functions

There are several built-in functions available mostly for doing regular expression operations. They are explained in Table 12-6.

Table 12-6 Built-In Functions

Function	Valid Forms	Description
exists()	exists(%HEADERS[“Header”])	Returns “TRUE” or “FALSE” based on the existence of a header, or a param in the message.
	exists(%HEADERS[“Header”].PARAMS[“Param”])	
remove()	remove(%HEADERS[“Header”])	Removes a header or a parameter from the message.
	remove(%HEADERS[“Header”].PARAMS[“Param”])	
regex_match()	%HEADERS[“Header”].regex_match(“regex”)	Returns “TRUE” or “FALSE” based on the regular expression found a match in the text or not.
	%HEADERS[“Header”].PARAMS[“Param”].regex_match(“regex”)	
regex_get()	%HEADERS[“Header”].regex_get(“regex”)	Returns the extracted

Function	Valid Forms	Description
	%HEADERS[“Header”].PARAMS[“Param”].regex_get(“regex”)	string by the regular expression. The return value will be empty string if no match was found.
regex_replace()	HEADERS[“Header”].regex_replace(“regex”, “string”)	Replaces a given match with the provide string within the header string or a param
	%HEADERS[“Header”].PARAMS[“Param”].regex_replace(“regex”, “string”)	

User-Defined Variables

User defined variables are simply a storage area for holding a certain string. These can be used within assignment and conditional statements. All of the user defined variables are of string type. The variables names must all start with a ‘%’ sign and can have alpha numeric characters in their names. The only other valid extra character allowed within the variable name is the ‘_’ (underscore).

Hook Points

There are several hook points (described in Table 12-7) within the packet path that is illustrated in Figure 12-3 **Packet Path**.

Hook points are points within the E-SBC processing where given actions can be executed. These hook points can be specified by using the `%ENTRY_POINT` built-in variable within a where clause.

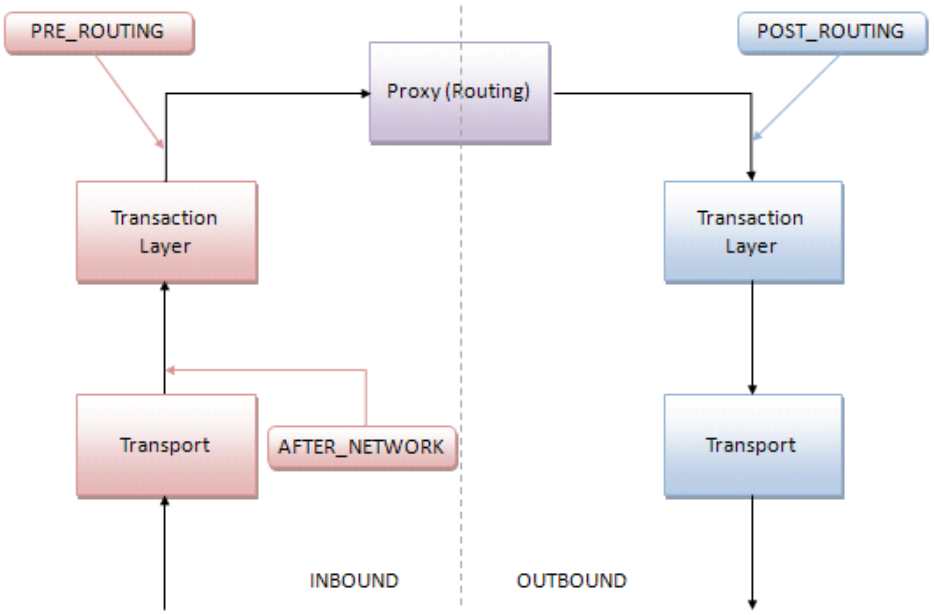


Figure 12-3 Packet Path

Table 12-7 Hook Points

Hook Point	Description
AFTER_NETWORK	This is a point in packet path soon after the packet is received from network.
PRE_ROUTING	After the transaction layer, before target destination for the packet is determined.
POST_ROUTING	After target destination is determined, before the transaction layer.

SigMa Scripting Examples

The SigMa scripting language is best demonstrated using some examples. Table 12-8 provides some examples that explain some use cases and how they can be represented in a SigMa script.

Table 12-8 SigMa Scripting Examples

Description	Scripting Example

Reverting From and To tags in all responses to REGISTER method.	within session "REGISTER"
	{
	act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
	{
	%from_tag = %HEADERS["From"][1].PARAMS["Tag"];
	%HEADERS["From"][1].PARAMS["Tag"] = %HEADERS["To"][1].PARAMS["Tag"];
	%HEADERS["To"][1].PARAMS["Tag"] = %from_tag;
	}
	}

Updating p-asserted-identity field with the value of From header if P-Asserted-Identity field value is anonymous	within session “ALL”
	{
	act on message where %DIRECTION=”OUTBOUND” and %ENTRY_POINT=”POST_ROUTING”
	{
	if (%HEADERS[“P-Asserted-Identity”][1].URI.USER = “anonymous”) then
	{
	%aor = %HEADERS[“From”][1].URI;
	%HEADERS[“P-Asserted-Identity”][1] = %aor;
	}
	}
	}

Description	Scripting Example

Adding a media attribute in SDP	within session “ALL”
	{
	act on message where %DIRECTION=”OUTBOUND” and %ENTRY_POINT=”POST_ROUTING”
	{
	%SDP[1][“s”][“m”][1].ATTRIBUTES[“fmtp”] = “101 0-16”;
	}
	}

Adding a header	within session “ALL”
	{
	act on message where %DIRECTION=”OUTBOUND” and %ENTRY_POINT=”POST_ROUTING”
	{
	%HEADERS[“SLiC-Version”][1] = “3.2.2”;
	}
	}

Trunking: Removing phone_context param from Request Uri, To and From headers	within session “ALL”
	{
	act on message where %DIRECTION=”OUTBOUND” and %ENTRY_POINT=”POST_ROUTING”
	{
	remove(%HEADERS[“Request_Line”][1].PARAMS[“phone-context”]);
	remove(%HEADERS[“From”][1].PARAMS[“phone-context”]);
	remove(%HEADERS[“To”][1].PARAMS[“phone-context”]);
	}
	}

Learn P-Asserted-Identity from INVITE and use this value to replace From URI in every Request.	within session “INVITE”
	
	{
	
	act on request where %DIRECTION=”OUTBOUND” and %ENTRY_POINT=”POST_ROUTING”
	
	{
	
	If (%INITIAL_REQUEST = ”TRUE”) then
	
	{
	
	%passert_val = %HEADERS[“P-Asserted-Identity”][1].URI;
	
	}
	
	else
	
	{
	
	%HEADERS[“From”][1].URI = %passert_val;
	
	}
	
	}
	
	}

Trunking: For all new calls, add diversion header if it doesn't exist.	within session “INVITE”
	
	{
	
	act on request where %DIRECTION=”OUTBOUND” and %ENTRY_POINT=”POST_ROUTING”
	
	{
	
	if (%INITIAL_REQUEST = “TRUE”) then
	
	{
	
	%HEADERS[“Diversion”][1] = “sip:333444555@”;
	
	append(%HEADERS[“Diversion”][1], %REMOTE_IP);
	
	}
	
	}
	
	}

SigMa Scripting Tutorial

The following section includes some additional examples of test cases and use cases with their associated SigMa scripts and explanations of what the scripts do.

Any limitations of each script are also included.

Test Case 1: Manipulation of P-Asserted-Identity Header

Use Case

The P-Asserted-Identity header field can be used to present the identity of the originator of a request within a trusted network. Since the “From” header field is populated by the originating User-Agent it may not contain the actual identity. It usually is established by means of authentication between the originating User-Agent and its outgoing proxy. The outgoing proxy then adds a P-Asserted-Identity header field to assert the identity of the originator to other proxies.

a. If there is no P-Asserted-Identity header field present, a proxy MAY add one containing at most one SIP or SIPS URI, and at most one telephone URL.
b. If the proxy received the message from an element that it does NOT trust and if there is a P-Asserted-Identity header present, the proxy MUST replace the SIP URI or remove it.

Script

```
within session "ALL"  //Looks into all the messages

{

  /* Message should be a request (act on request) and the messages coming towards the E-SBC should be
  considered, i.e. the destination of the message should be E-SBC ("%DIRECTION="INBOUND").The actions
  are invoked as soon as the message comes from the wire(%ENTRY_POINT="AFTER_NETWORK") */


    act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"

        {

        /*Checks if the first P-Asserted-Identity header is present/exists in the message. Each header
        is represented as %HEADERS["<Header-name>"][<Header position>].For headers such as From and
        Contact, the Header Position is always 1.For headers like Via and P-Asserted-Identity, the
        positions can range from 1 to n*/


            if(exists(%HEADERS["p-asserted-identity"][1]))then

            {

                remove(%HEADERS["p-asserted-identity"][1]); //Remove the header

            }


            /*If the P-Asserted-Identity header is not found in the message*/


            else

            {

                        /* Add a SIP and a telephone URI.*/

                %HEADERS["p-asserted-identity"][1] = "12345<sip:12345@192.168.150.150>";

                %HEADERS["p-asserted-identity"][2] = "tel:+14085264000";

            }


        }


}
```

Description

The script looks into each message that comes in (since the script acts on all sessions) and checks if:

c. It is a request message
d. The message is coming to the E-SBC

If both the above conditions are successful, as soon as the message comes from the wire, (and after the basic sanity checks and DoS checks are performed on the message), the action is performed. The script checks to see if a "P-Asserted-Identity" header exists. If it does, it removes it, else it adds the header.

Limitations

If you would like to remove all the P-Asserted-Identity headers, it is assumed that you know the *maximum* number of headers that would be present in the messages. You do not need to know the exact number of headers that come in because if you perform an operation on a header that does not exist, it is simply ignored.

Note:	If %HEADERS["<Header-Name>"][<Header Position>] is already present, then the operation %HEADERS["<Header-Name>"][<Header Position>] = <Val> will modify the header. If it is not present in the message, %HEADERS["<Header-Name>"][<Header Position>] = <Val> will add the header to the message.

Test Case 2: Adding a Media Attribute in SDP

Use Case

It might be required to add/modify SDP attributes or connection parameters for interoperability.

Script

```
/*Looks into messages in the INVITE session only (It includes all messages in the INVITE dialog)*/


within session "INVITE" {

  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"

  {


      /*The “m=” field in SDP contains information about the type of media session. It includes the format-list parameter for specifying the codecs.Assuming that the message comes in with 2 codecs, we add a third codec as 101 */


      %SDP[1]["s"]["m"][1].FORMATS[3]="101";


      /*The “a=” field contains attributes to provide more information on the codecs.Assuming that the message does not have any fmtp attribute,we add the first one as 101 0-16*/


      %SDP[1]["s"]["m"][1].ATTRIBUTES["fmtp"][1]="101 0-16";

  }


}
```

Description

The script looks into all the messages of the “INVITE” session. A session is defined as a SIP dialog and has the same lifetime as that of a dialog. A new format-type and an attribute is added corresponding to *fmtp*.

Limitations

We would need to know the number of codecs (number of formats in format-list parameter and attributes), or we would end up replacing an existing format-type.

Test Case 3: Changing Calling Party Presentation to Restricted

Use Case

Same.

Script

```
within session "ALL"
{
    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
    {

        /*Checks if the privacy header value matches with the regular expression given(“none”).
        If it matches, then the privacy header value is changed to “id”*/

        if(%HEADERS["Privacy"][1] = "none")then
        {
        %HEADERS["Privacy"][1] = "id";
        }
    }
}
```

Description

Same.

Limitations

None.

Test Case 4: Replace “From” Header For a Set of Users

Use Case

In an organization, there could be several phones used by the employees and each of them might have a unique “From URI” associated with them. It may be required that all calls going out from the organization have the same “From URI”. For this purpose, the following script can be used.

Script

```
within session "INVITE"{

/* For users whose Uri begins with the prefix 10, when the message comes towards the E-SBC, the
Uri is changed to “9000”<sip:9000@domain>. So, when the receiver answers the call, the From is
9000. */

    act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"

    {

        /*A Uri can be represented as “<diplay_name>”<scheme>:<user>@<host>:<port>, eg:
        ”shalini”<sip:shalini@sipera.com:5060>. URI.USER extracts the user portion of the URI.
        regex_match tries to match the string against the regular expression. It is of the form
        <string>.regex_match(“<regular expression>”).In this example,it is checked if the USER
        portion in the “From” Header starts with the prefix 10 */


        if(%HEADERS["From"][1].URI.USER.regex_match("^10"))then

        {

        /*The uri and display name of the actual user is stored in temporary variables*/

        %OriginalFromUri = %HEADERS["From"][1].URI.USER;

        %OriginalFromName = %HEADERS["From"][1].DISPLAY_NAME;


        /* The display name and uri is changed to the new values.*/

        %HEADERS["From"][1].DISPLAY_NAME = "9000";

        %HEADERS["From"][1].URI.USER = "9000";

        }

    }


/* When the response comes back, we need to change the URI USER and DISPLAY NAME to the actual
user. So,before the message is sent out to the wire from the E-SBC, it is checked if the
URI.USER is 9000. If yes, then change it back to the original user’s details. */

/* Message should be a response (act on response) and the messages going out from the E-SBC
should be considered (“%DIRECTION="INBOUND"). The actions are invoked before the message goes
out (%ENTRY_POINT="BEFORE_NETWORK") */
```

```
    act on response where %DIRECTION="OUTBOUND" and %ENTRY_POINT="BEFORE_NETWORK"
    {
       /*Check if the user portion of the From URI is 9000*/
        if(%HEADERS["From"][1].URI.USER = "9000")then
        {
        /*Change the URI.USER and display name to the original user's details, which are saved
        in the temporary variables*/
        %HEADERS["From"][1].URI.USER = %OriginalFromUri;
        %HEADERS["From"][1].DISPLAY_NAME = %OriginalFromName;
        }
    }

}
```

Description

The above example shows how to modify a message (request) on its way out and also modify a message (response) when it comes in.

Limitations

The example illustrates the use of *regex_match*. The regular expression provided within the parentheses, i.e., *regex_match(<regular expression>)*, can be any valid Perl regular expression. However, the "$" symbol can't be used in the regular expression.

Test Case 5: Editing the “Allow” Header

Use Case

The Allow header is used to indicate the methods supported by the user agent. Eg: Allow: INVITE, ACK, BYE, INFO, OPTIONS, CANCEL. The OPTIONS method is used to query a user agent or server about its capabilities

and discover its current availability. The response to the request lists the capabilities of the user agent or server. This may not be desired (probably due to security reasons). In this case, the E-SBC can strip the OPTIONS method from the Allow header before sending out the message.

Script

```
within session "INVITE"
{


/*Look for INVITE messages only.  This is specified with the extra condition %METHOD="INVITE" in the where clause*/
act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" and %METHOD="INVITE"
{

/*There could be i.multiple methods in Allow or ii. OPTIONS could be the only method in Allow. If there are multiple methods in Allow, OPTIONS could be i. in the beginning 2. in the middle/the end */



/*If OPTIONS is in the middle/end in Allow, it would be of the form Allow:<Methods>,OPTIONS,<More methods> or Allow:<Methods>,OPTIONS. So, we try to match Allow against the regex ,OPTIONS */


        if(%HEADERS["Allow"][1].regex_match(", OPTIONS"))then
        {

        /*<string1>regex_replace(“<regex1>”,”<string2>”) looks for regex1(regular expression) in string1 and replaces it with string2(plain string). Here we replace ,OPTIONS with an empty string, indirectly removing ,OPTIONS*/


            %HEADERS["Allow"][1].regex_replace(", OPTIONS","");
        }
        else
        {

        /*Nested if-else*/

        /*If OPTIONS is in the beginning in Allow, it would be of the form

        Allow: OPTIONS,<More methods>. So, we try to match Allow against the regex OPTIONS, */


            if(%HEADERS["Allow"][1].regex_match(" OPTIONS,"))then
            {
```

```
            /* We replace OPTIONS, with an empty string, indirectly removing OPTIONS,*/


                    %HEADERS["Allow"][1].regex_replace(" OPTIONS,", "");
                }
                else
                {

            /*If OPTIONS is the only method in Allow, it would be of the form

            Allow: OPTIONS. So, we try to match Allow against the regex OPTIONS */



                    if(%HEADERS["Allow"][1].regex_match(" OPTIONS"))then
                    {

                    /*Since OPTIONS is the only method in Allow, we remove the entire header*/

                    /*remove(%HEADERS[“<Header-name>”][<Posn>] removes the header specified in
                    <Header-name> in Position <Posn>.Here we remove the Allow header*/
                        remove(%HEADERS["Allow"][1]);
                    }
                }
            }
        }

    }
```

Description

This script can come in handy while operating on headers such as Allow, Supported, Content-Type etc, whose values can't be extracted individually as compared to headers like "From", "To", or "Contact".

Limitations

The regular expression in regex_replace can't have the $ symbol.

Test Case 6: Prefix Stripping

Use Case

Phone numbers may come in with a prefix. Sometimes, this needs to be stripped off before the call is routed. This is useful in scenarios where a call transfer is made and the number to which the call has to be transferred is entered with a prefix.

Script

```
within session "INVITE"

{

/*Look for REFER messages only.  This is specified with the extra condition %METHOD="REFER" in the where clause*/


    act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" and %METHOD="REFER"



    {

/* The User portion of the URI in the Refer-To header is checked to see if it starts with the prefix 011.  If it does, then it is replaced with an empty string. If URI.USER does not match the regex, then the action is ignored and the message is left intact.*/


        %HEADERS["Refer-To"][1].URI.USER.regex_replace("^011","");


    }







}
```

Description

The messages which have the "**Refer-To**" method are checked if the URI contains a prefix. If so, it is stripped before sending it out.

Limitations

The regular expression in **regex_replace** can't have the $ symbol.

E-SBC GUI SigMa Editor

Figure 12-4, on the next page, shows the new Signaling Manipulation SigMa Editor screen, which is accessed by selecting the Signaling Manipulation function from the Global Profiles feature in the Task Pane. This screen contains a full set of controls for managing all of your Signaling Manipulation scripts, including the following:

- Signaling Manipulation Scripts Pane – Lists all of the scripts that are stored on the device. Clicking on a script name in the list, displays the script in the SigMa Editing window to the right, where the script can be modified.

Note:	By consecutively clicking on additional script names in the list, you can open up multiple SigMa Editor screens at one time.

- Edit Button – Inside each SigMa Editor window at the bottom is an Edit button. Clicking on this button allows you to make modifications to the existing script.
- Save Button (not shown) – Once the Edit button is clicked and modifications are made to an existing script, you can click on a Save button to save the changes to the script.

Note:	Once the **Save** button is clicked, the script will be transparently submitted to the backend and validated before it is saved to the disk. If it fails validation, error messages will be displayed to the user to help them correct any syntax errors in the script.

- Add Script Button – Located above the scripts pane, is an Add Script button which allows you to create a new script by opening up a blank SigMa Editing window to the right.
- Upload Script Button – Allows you to upload the selected script to a remote location.
- Download Script Button – Allows you to download a script to the device from a remote location.
- Clone Script Button – Allows you to copy the selected script to a new script name for the purposes of modifying the newly named script for different functionality.
- Delete Script Button – Allows you to delete the selected script

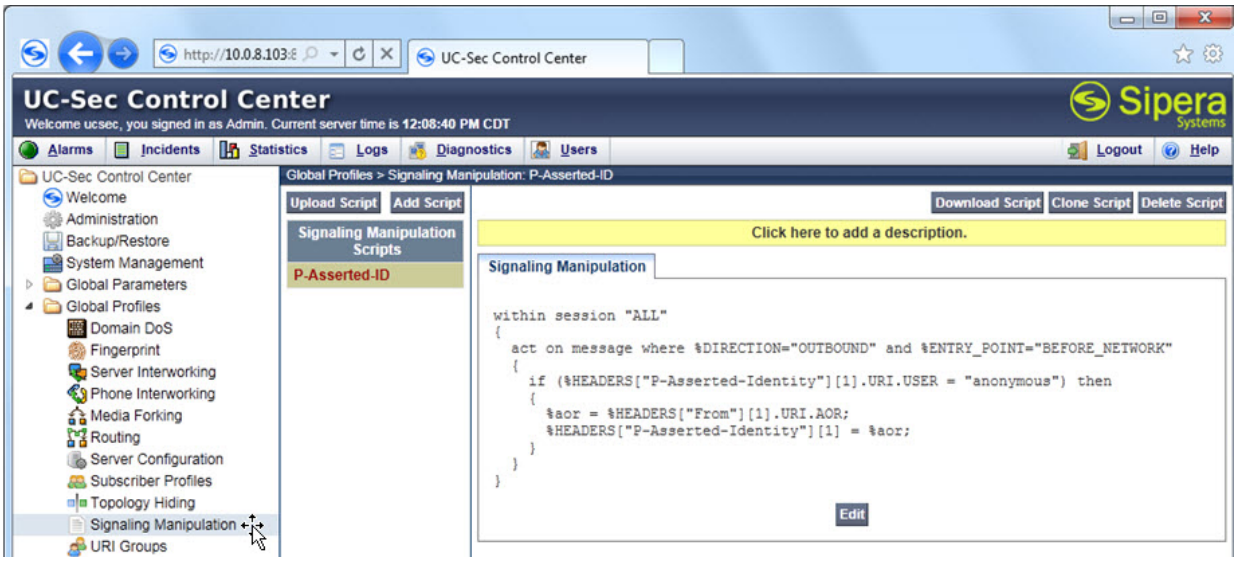


Figure 12-4 SigMa Editor Screen for Signaling Manipulation

Sigma Design Overview

A Sigma Process Flowchart is provided below in Figure 12-5.

Note:	Once you have created a SigMa script, you will have to specify it in a Server Configuration before you can execute it.

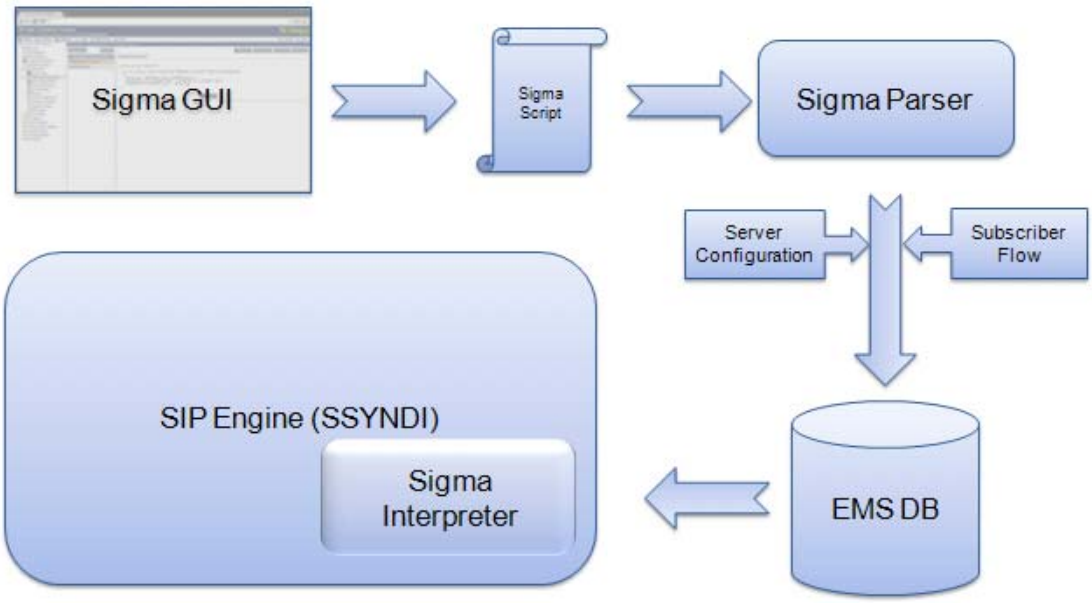


Figure 12-5 SigMa Process Flowchart

Specifying a SigMa Script in a Server Configuration

Use the following sample procedure to specify a SigMa script in a Server Configuration:

Note:	**The procedure below assumes that no Server Configurations have been created yet. If you are specifying a SigMa script in a Server Configuration that already exists, proceed to Step 9 of this procedure.**

1. Login to the E-SBC Control Center as the Admin.
2. Select the Server Configuration function from the Global Profiles feature from the Task Pane to display the Server Configuration screen (Figure 12-6).

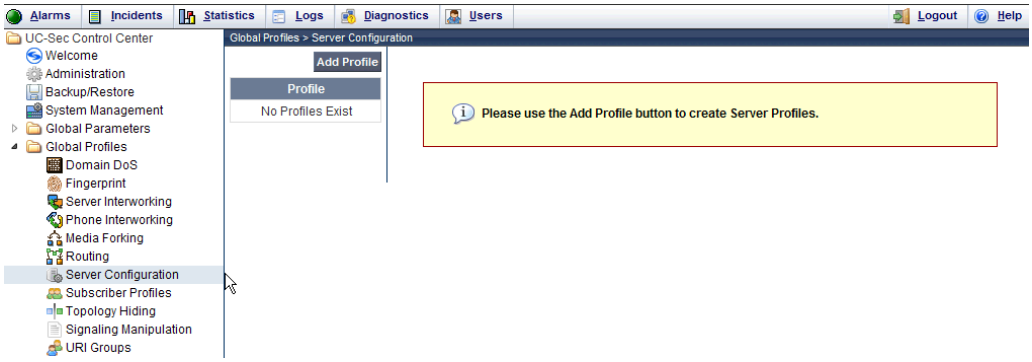


Figure 12-6 Server Configuration Screen

3. In the Server Configuration screen (Figure 12-6), select the **Add Profile** button to display the first Add Server Configuration screen (Figure 12-7).

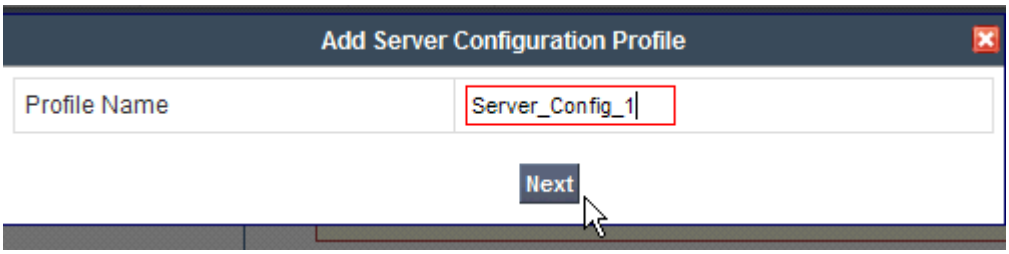


Figure 12-7 Add Server Configuration Profile Screen 1

4. In the first Add Server Configuration Profile screen (Figure 12-7), enter a name in the Profile Name field and select Next to display a second Add Server Configuration Profile General screen (Figure 12-8).

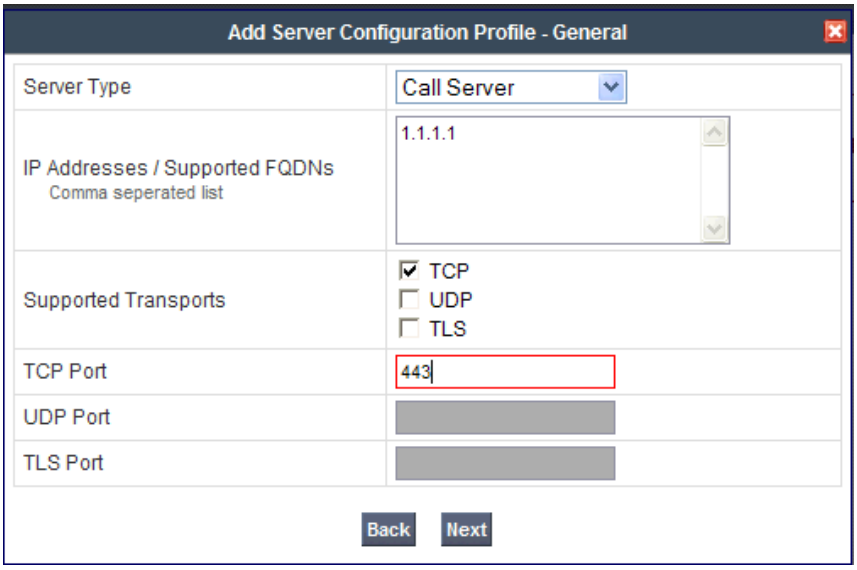


Figure 12-8 Add Server Configuration Profile General Screen 2

5. In the second Add Server Configuration General screen (Figure 12-8), enter the appropriate information, and then select **Next** to display a third Add Server Configuration Profile Authentication screen (Figure 12-9).

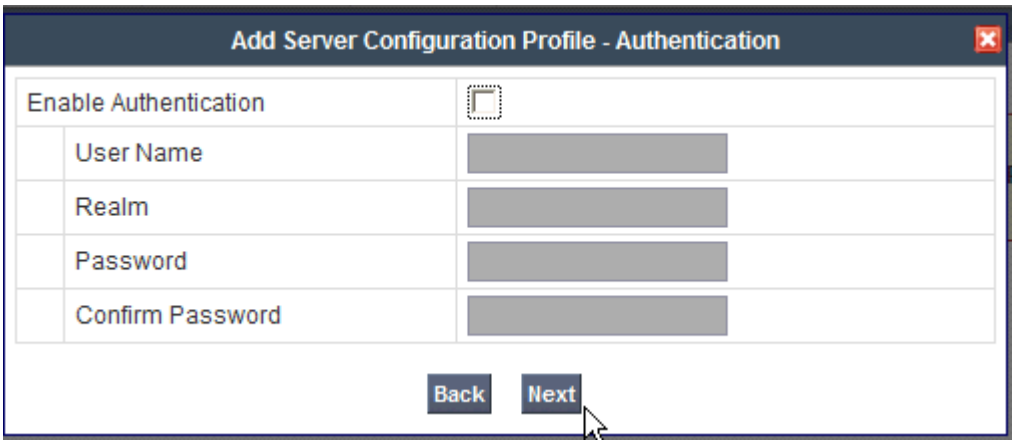


Figure 12-9 Add Server Configuration Profile Authentication Screen 3

6. In the third Add Server Configuration Authentication screen (Figure 12-9), enter the appropriate information, and then select **Next** to display a fourth Add Server Configuration Profile Heartbeat screen (Figure 12-10).

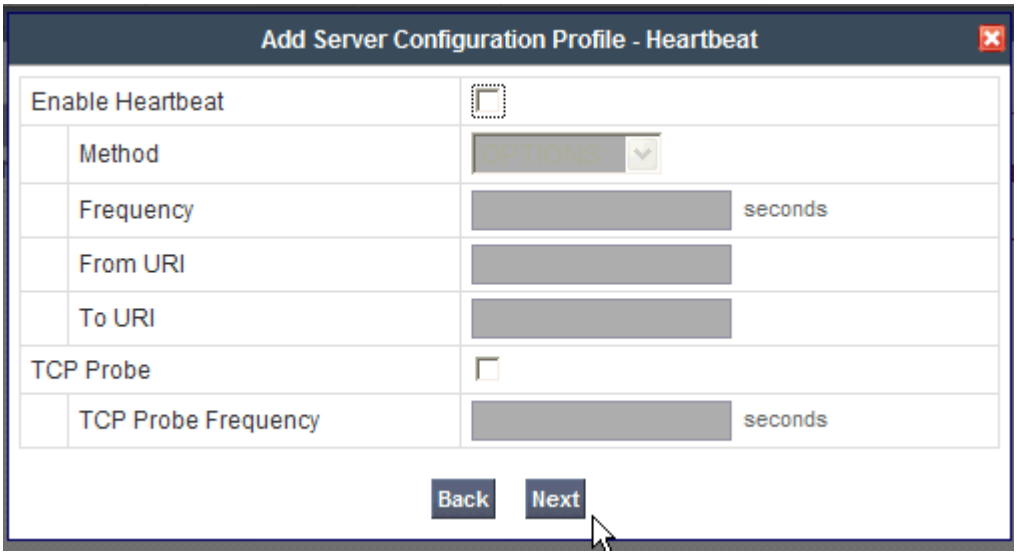


Figure 12-10 Add Server Configuration Profile Heartbeat Screen 4

7. In the fourth Add Server Configuration Heartbeat screen (Figure 12-10), enter the appropriate information, and then select **Next** to display a fifth Add Server Configuration Profile Advanced screen (Figure 12-11).

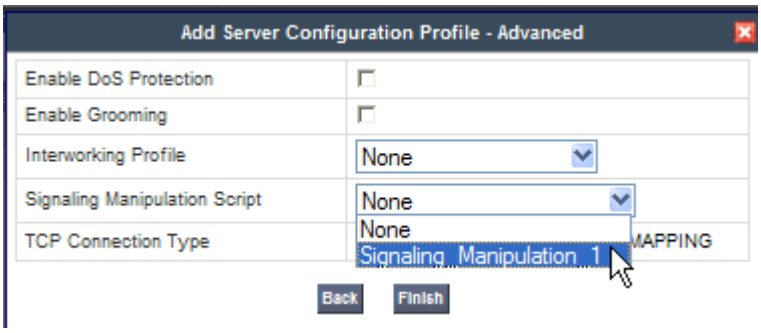


Figure 12-11 Add Server Configuration Profile Advanced Screen 5

8. In the fifth Add Server Configuration Advanced screen (Figure 12-11), enter the appropriate information, and then select **Finish** to submit, save, exit, and redisplay the updated Server Configuration screen (Figure 12-12) showing the newly-added profile (Config_Server_1 in the example).

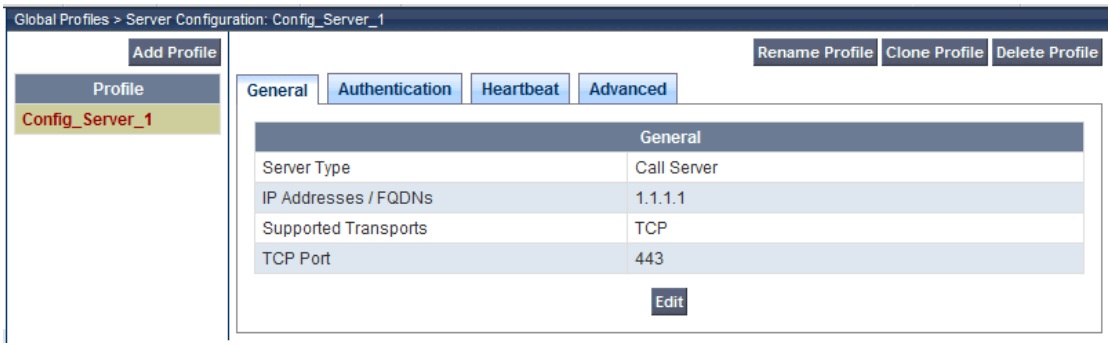


Figure 12-12 Updated Server Configuration Screen

9. Begin the procedure here at Step 9 if you are specifying a SigMa Script in a Server Configuration that has previously been created.

   In this procedure, beginning with Step 9, it is assumed in this example that the previously created Server Configuration is the one titled Config_Server_1 as shown in Figure 12-12.

10. In the Server Configuration screen, select the profile name (Config_Server_1 in the example) and then select the Advanced tab button (see Figure 12-13) to display the Sever Configuration Advanced tab screen (Figure 12-14).

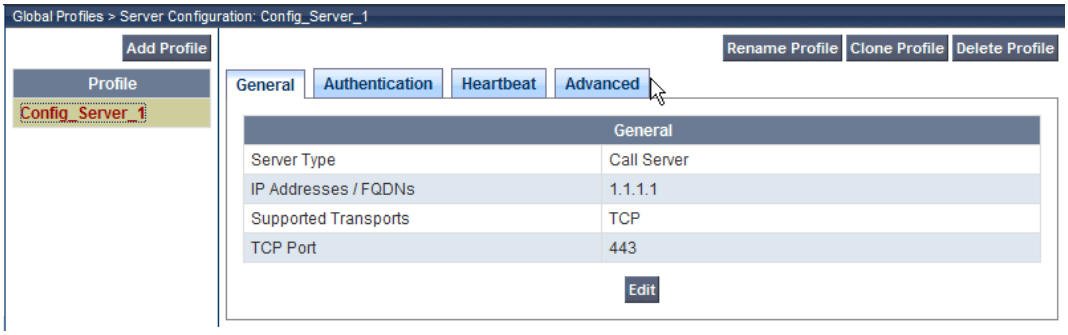


Figure 12-13 Sever Configuration Advanced Tab Button

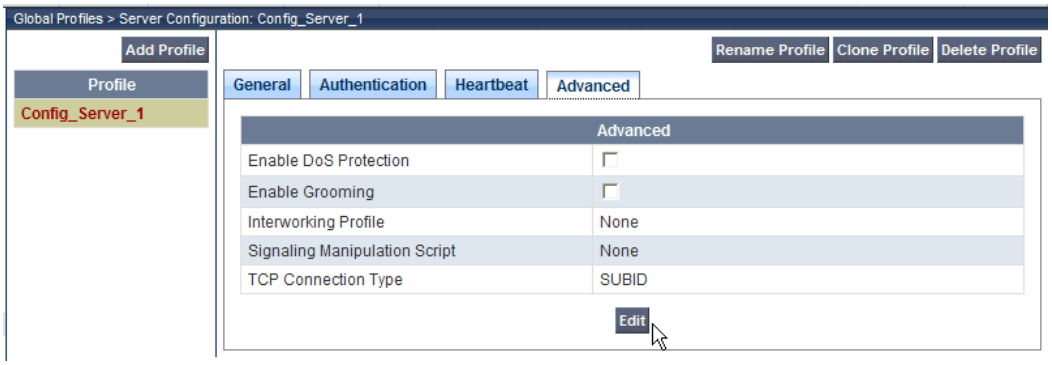


Figure 12-14 Server Configuration Advanced Tab Screen

11. In the Server Configuration Advanced Tab screen, select the **Edit** button to display the Edit Server Configuration Profile – Advanced screen (Figure 12-15).

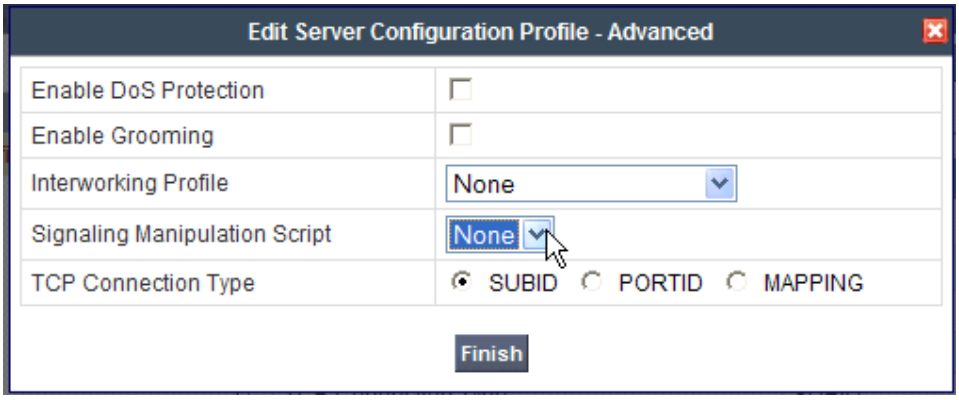


Figure 12-15 Server Configuration Advanced Tab Edit Screen

12. In the Edit Server Configuration Profile Advanced screen (Figure 12-15), select the name of the SigMa script that you want to specify from the drop-down list in the Signaling Manipulation Script field, as shown above.

13. Select **Finish** to submit, save, and exit.

This completes the procedure for specifying a SigMa Script in a Server Configuration.

This page intentionally left blank.

Acronyms and Abbreviations A

This appendix contains an alphabetical list of all the acronyms and abbreviations used throughout this manual.

Acronym	Definition
AAA	Authentication, Authorization, and Accounting
ACD	Automatic Call Distribution
ACL	Access Control List
ACS	Access Control Server
AD	Active Directory
AES	Advanced Encryption Standard *or* Access Edge Server
AH	Authentication Header
AKA	Authentication Key Agreement
ARP	Address Resolution Protocol
AT	Authentication Tag
AXL	Cisco AXL Application Programming Interface (API)
B2B	Back-to-Back (Agent)
CA	Certificate Authority
CALEA	Communications Assistance for Law Enforcement Act
CCM	Cisco Call Manager
CDR	Call Detail Record
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
CM	Call Manager
Codec	Coder/Decoder
CoS	Class-of-Service
CRL	Certificate Revocation List
CS	Call Server
CSR	Certificate Signing Request
CTI	Computer Telephony Integration or Computer-Telephone Integration
CTL	Certificate Trust List
CUCM	Cisco Unified Communication Manager
CUPC	Cisco Unified Presence Client

Acronym	Definition
CUPS	Cisco Unified Presence Server / Cisco Unified Personal Communicator
DA	Digest Authentication
DDoS	Distributed Denial-of-Service
DES	Data Encryption Standard
DH	Diffie-Hellman
DHA	Directory Harvest Attack
DHCP	Dynamic Host Control Protocol
DHE	Ephemeral Diffie-Hellman
DiffServ	Differentiated Services
DLR	Dialog-Level Router
DMZ	Demilitarized Zone
DoS	Denial-of-Service
DoW	Day-of-Week
DSCP	Differentiated Services Code Point
DSS	Digital Signature Standard
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EMS	Element Management System
ENUM	E Number Working Group *or* Electronic Numbering
ERTP	Encrypted Real-Time Transport Protocol
ESP	Encrypted Security Payload
FCAPS	Faults, Configuration, Accounting, Performance, and Security
FIPS	Federal Information Processing Standards
FPM	Federated Presence Management
FQDN	Fully-Qualified Domain Name
FW	Firewall
GARP	Gratuitous Address Resolution Protocol *or* Gratuitous ARP
GbE	Gigabit Ethernet
GUI	Graphical User Interface
HA	High-Availability *or* Harvest Attack
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IDP	Intrusion Detection and Prevention

Acronym	Definition
IDS	Intrusion Detection System
IM	Instant Messaging
IP	Internet Protocol
IPI	Intelligent Peripheral protocol
IPS	Intrusion Protection System
IPSec	Internet Protocol Security
ITSP	Internet Telephony Service Provider
LAN	Local Area Network
LB	Load Balancer
LCRV	Lightweight Certificate Revocation Verification
LCS	Live Communications Server (Microsoft™)
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MAD	Media Anomaly Detection
MAM	Media Anomaly Manager
MAP	Media Anomaly Protection
MCD	Machine Call Detection
MD5	Message Digest 5
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extension
MKI	Master Key Identifier
MMS	Multimedia Message Service
MPLS	Multiprotocol Label Switching
MSA	Message Sequence Analysis
MSD	Media Silence Detection
MTLS	Multiplexed Transport Layer Security
MWI	Message Waiting Indicator
NAPT	Network Address Port Translator
NAPTR	Naming Authority Pointer
NAT	Network Address Translation
NAT/T	Network Address Translation / Traversal
NIDS	Network Intrusion Detection System
NOC	Network Operations Center

Acronym	Definition
NSAP	Network Service Access Point
NTLM	NT LAN Manager (Microsoft™)
NTP	Network Time Protocol
OAM&P	Operations, Administration, Maintenance and Provisioning
OCS	Office Communications Server (Microsoft™)
PAP	Protected Authentication Protocol
PAT	Port Address Translator
PCMA	Pulse Code Modulation – A law
PCMU	Pulse Code Modulation – mu law
PKI	Public Key Infrastructure
POP	Point-of-Presence *or* Post Office Protocol
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PSOM	Persistent Shared Object Model
PSTN	Public Switched Telephony Network
QoP	Quality-of-Protection
QoS	Quality-of-Service
RADIUS	Remote Authentication Dial-in User Service
RAM	RTP Anomaly Manager
RC	Root Certificate
RED	Random Early Detection *or* Random Early Drop
RegEx	Regular Expression
RSA	Rivest, Shamir & Adleman
RTC	Real-Time Collaboration
RTCP	Real-Time Transport Control Protocol
RTCP XR	RTP Control Protocol Extended Reports
RTDB	Real-Time Database
RTP	Real-Time Transport Protocol
RTSP	Real-Time Streaming Protocol
SA	Security Association
SAP	Session Announcement Protocol
SAST	System Administrator Security Token
SBA	Secure Border Access

Acronym	Definition
SBC	Session Border Controller
SCTP	Stream Control Transmission Protocol
SD	Spoof Detection
SDK	Software Development Kit
SDP	Session Description Protocol
SFTP	Secure File Transfer Protocol
SHA-1	Secure Hash Algorithm-1
SIM	Security Information / Infrastructure Management
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
SIV	Sender Intention Verification / Validation
SLA	Service –Level Agreement
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOV	Session Origin Verification / Validation
SOX	Sarbanes-Oxley (Security Act of 2002)
SPI	Security Parameter Index
SPIM	SPAM-over-Instant Messaging (IM)
SPIT	SPAM-over-Internet Telephony
SRL	SIP Relay Layer
SRTP	Secure Real-Time Transport Protocol
SRV	Service Record
SSL	Secure Socket Layer
SSR	SIP Stateless Relay
SSRC	Synchronization Source
STUN	Simple Traversal of UDP through NAT
TA	Transport Agent
TAM	Traffic Acceleration Monitor
TAPI	Telephony Application Programming Interface
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol

Acronym	Definition
TCP/UDP	Transmission Control Protocol / User Datagram Protocol
TDES	Triple Data Encryption Standard
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
ToD	Time-of-Day
ToS	Type-of-Service *or* Terms-of-Service
TSAP	Transport Service Access Point
TURN	Traversal Using Relay NAT
TVM	Traffic Velocity Monitor
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VID	VLAN Identifier
VIPA	Virtual IP Addressing
VLAN	Virtual LAN
VLSM	Variable Length Subnet Mask
VM	Voice Mail
VoIP	Voice-over-Internet Protocol
VPA	Virtual Private Assistant
VPN	Virtual Private Network
VRU	Voice Response Unit
VSLAM	Variable Length Subnet Mask
WLF	White List Filter
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

Glossary B

This appendix contains a glossary of the definitions for the terms used in this manual.

Acronym	Definition
Access Control List (ACL)	A table listing which access rights or security attributes each user has to a particular system object or function. The most common privileges include the ability to read a file, to write to the file, and to execute the file (if it is an executable file, or program). These lists are implemented differently by each control platform.
Anti-tromboning	The capability of allowing media traffic to flow directly between two end-points that are located in the same private network, instead of having to traverse the access network before reaching its destination. Also referred to as *Media Release*. See *Tromboning*.
Authentication Tag (AT)	The Secure Real-Time Transport Protocol (SRTP) field that carries message authentication data.
Availability	The ability to make information or services available for use when needed.
AXL	The Cisco AXL Application Programming Interface (API) that provides a mechanism for inserting, retrieving, updating, and removing data from a Cisco CallManager database. AXL provides for the following: (1) Access to Cisco CallManager data using XML (2) Uses requests that are a combination of HTTP and SOAP (3) Is a provisioning and configuration API
Call	A voice or data connection made between two endpoints in a network.
Certificate (Digital)	A digital certificate is akin to an electronic "credit card" that establishes a client's credentials and authenticity when establishing a communication session and is issued by a certification authority (CA). It contains various information used for encrypting messages and digital signatures). In addition, the certificate contains the digital signature of the certificate-issuing authority so that it can be verified as being real. Some digital certificates conform to a standard, such X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys. See also *Certificate Authority (CA)*.
Certificate Authority (CA)	The CA is a trusted body that confirms the validity and identity of entities involved in public key exchange. As a user's digital certificate is the only means by which entities may trust each other, the CA must be a legitimate, regulated, and officially recognized entity. An example of a well known CA that is used by many commercial organizations, is Verisign.
Certificate Signing Request (CSR)	In a Public Key Infrastructure (PKI) systems, a CSR is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a directory name in the case of an X.509 certificate), and the public key chosen by the applicant. The corresponding private key is not included in the CSR, but is used to digitally sign the entire request. The CSR may be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate

Acronym	Definition
	authority may contact the applicant for further information. If the request is successful, the certificate authority will send back an identity certificate that has been digitally signed with the private key of the certificate authority.
Cisco Unified Communication Manager (CUCM)	Cisco Unified Communications Manager (CUCM), formerly Cisco Unified CallManager and Cisco CallManager (CCM), is a software-based call-processing system developed by Cisco Systems that tracks all VoIP network components.
Cisco Unified Presence Server (CUPS)	The Cisco® Unified Presence Server is a critical component for delivering the full value of a Cisco Unified Communications environment. It collects information about a user's availability status, such as whether or not you are using a communications device such as a phone at a particular time. It also collects information regarding a user's communications capabilities.
Cisco Unified Presence Client (CUPC)	Among Cisco's Unified Presence products, "Cisco Unified Presence Client" is another accepted name for the product's official name, "Cisco Unified Personal Communicator."
Cisco Unified Personal Communicator (CUPC)	An integral component of the Cisco Unified Communications family of products, Cisco Unified Personal Communicator is a powerful desktop computer application that integrates the most frequently used communications applications and services (e.g., VoIP, IM, audio, video, conferencing, etc.). Also know as Cisco Unified Presence Client, the client application is similar to the Microsoft™ Office Communications Server (OCS) client application called Microsoft Office Communicator.
Classless Inter-Domain Routing (CIDR)	A method used to help ease the load on Internet and large data network backbone routers by increasing the size of routing tables. Given the fact that large routing tables normally have several adverse effects, such as requiring extraordinary amounts of system memory to manipulate these large tables and increasing latency, CIDR alleviates these problems by efficiently aggregating IP addresses. This allows several networks to be spanned by a single routing entry. CIDR is also referred to as *Variable Length Subnet Mask (VLSM).*
Client	A device or application that initiates a request for a connection with a server.
Client Authentication	Refers to the process of authenticating a client identity by using the client certificate (in TLS).
Communications Assistance for Law Enforcement Act (CALEA)	A US wiretapping law passed in 1994 requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities. Common carriers, facilities-based broadband Internet access providers, and providers of interconnected Voice over Internet Protocol (VoIP) service – all three types of entities are defined to be "telecommunications carriers" for purposes of CALEA section 102. The driving force in adopting CALEA was the FBI's worry that increasing use of digital telephone exchange switches would make tapping phones at the phone company's central office harder and slower to execute, or in some cases impossible. Since the original requirement to add CALEA-compliant interfaces required phone companies to modify or replace hardware and software in their

Acronym	Definition
	systems, U.S. Congress included funding for a limited time period to cover such network upgrades. CALEA was passed on October 25, 1994 and came into force on January 1, 1995.
Computer Telephony Integration (CTI)	Also called computer-telephone Integration, CTI is technology that allows interactions on a telephone and a computer to be integrated or coordinated. As contact channels have expanded from voice to include email, web, and fax, the definition of CTI has expanded to include the integration of all customer contact channels (voice, email, web, fax, etc.) with computer systems.
Contributing Source (CSRC)	A Real-Time Protocol (RTP) variable that is used to indicate the sources behind a mixing function. This mixing function is used to combine streams before they are played to the end user.
Data Encryption Standard (DES)	An early method of encryption adopted as the Federal Information Processing Standard (FIPS) and used extensively by the US Government. Continual improvements in the method have been incorporated, to where it is now more commonly referred to as Triple DES (TDES). See *Triple DES (TDES)*.
Day Zero Attack	See *Zero-Day Attack*.
Demilitarized Zone (DMZ)	A computer network-related term that refers to the "neutral zone" between an enterprise's private network and outside public network. Typically, a computer host or small network is inserted into this neutral zone to prevent outside users from getting direct access to the internal network.
Denial-of-Service (DoS)	The objective or end-result of certain types of malicious attacks or other activities against a network, where access to network services, resources, or endpoints is prohibited.
Diffie-Hellman (D-H) Key Exchange	The process in which "session keys" are distributed between parties that have no prior knowledge of each other across an unsecure public network. This involves setting-up a secure tunnel using Public Key Encryption (PKE), through which session keys are passed.
Digest Authentication (DA)	A Hypertext Transport Protocol (HTTP) authentication scheme whereby user passwords are encrypted prior to being sent across the Internet, thus certifying the integrity of the Uniform Resource Locator (URL) data. The downside of DA is that although passwords are encrypted, the data being exchanged is not; it is sent in the clear.
Directory Access Protocol (DAP)	A software protocol for enabling anyone to locate resources in a network and is part of X.500.
Directory Harvest Attack (DHA)	DHA is an attempt to determine the valid e-mail addresses associated with an e-mail server so that they can be added to a SPAM database. A directory harvest attack can use either of two methods for harvesting valid e-mail addresses. The first method uses a *brute force* approach to send a message to all possible alphanumeric combinations that could be used for the username part of an e-mail address at the server. The second and more selective method involves sending a message to the most likely user names - for example, for all possible combinations of first initials followed by common surnames. In either case, the e-mail server generally returns a **Not found** reply message for all messages sent to a nonexistent address, but does not return a message for those sent to valid addresses. The DHA program creates a database of all the e-mail addresses at the server that were not returned during the

Acronym	Definition
	attack. This explains how a new e-mail address can start receiving spam within days or hours after its creation.
Distributed Denial-of-Service (DDoS)	A more sophisticated type of DoS attack where a common vulnerability is exploited to first penetrate widely dispersed systems or individual end-points, and then use those systems to launch a coordinated attack. Much more difficult to detect than simple DoS attacks.
Dynamic Host Protocol Control (DHCP)	A protocol used to dynamically allocate and assign IP addresses.
E Number Working Group (ENUM)	ENUM is a standard adopted by the Internet Engineering Task Force (IETF) that uses the Domain Name System (DNS) to map telephone numbers to Web addresses or Uniform Resource Locators (URL). The goal of the ENUM standard is to provide a single number to replace the multiple numbers and addresses for an individual's home phone, business phone, fax, cell phone, and e-mail. The Request for Comments (RFC) for the ENUM proposal is RFC 2916.
Eavesdropping	The unauthorized interception and monitoring of voice packets or media streams.
Encapsulating Security Payload (ESP)	The ESP header normally forms part of an extension to the IP header, and is denoted in the IP type field by the value 50. The header itself is used to indicate the SPI Security Parameter Index (SPI) value that has been employed which, in turn, is associated to the key and algorithm that has been used to encrypt the IP payload. Only those entities privy to the Security Association (SA) have the mapping between the SPI and the key, consequently they are the only users who can decrypt the data. The ESP protocol is defined in RFC 2406.
Encryption	A process that secures network traffic from unauthorized access. By using secure procedures or secure software keys that are known only to authorized users, the encrypted network traffic can be accessed.
Endpoint	A SIP or H.323 terminal gateway. An endpoint can call and be called; it generates and terminates the information stream.
False negative	A malicious message that is erroneously treated as a legitimate message.
False positive	A legitimate message that is erroneously treated as a malicious message.
Faults, Configuration, Accounting, Performance, and Security (FCAPS)	FCAPS is the current network management model, which is comprised of the functions indicated in its name. **Fault Management** — To recognize, isolate, correct, and log faults that occur in the network. Furthermore it uses trend analysis to predict errors so that the network always remains available. **Configuration Management** — Gathers and stores configurations from network devices, simplifies device configuration, tracks configuration changes, and configures (provisions) circuit paths through non-

Acronym	Definition
	switched networks. **Accounting** (for billed networks) **/ Administration** (for non-billed networks): Billing management. Gathers usage statistics and maintains usage quotas. Common protocols normally used for accounting are RADIUS, TACACAS, and DIAMETER. For non-billed networks, Accounting is replaced by Administration. This function administers authorized users by establishing users, passwords and permissions, and administers equipment operations such as back-ups, archives, and synchronization. **Performance**: Used to determine the efficiency of the network using performance metrics such as throughput, percent utilization, error rates, response times, etc. **Security**: The function of controlling access to assets in the network through the use of tools and technologies such as authentication and encryption.
Federation	A group of Voice-over-IP (VoIP) services providers and enterprises which have agreed to: • receive calls from each other via Session Initiation Protocol (SIP), • a set of administrative rules for exchanging SIP calls (settlement, abuse-handling, etc.), and • a specific rules for the technical details of the interconnections they maintain between each other. Federations have a unique identifier and provide a number of advantages. These include: • the ability to avoid transcoding and enable the use of wideband coders/decoders (codecs), as well as avoid the service limitations of presence, Instant Messaging (IM), and video applications; • avoiding the drawbacks inherent in SPAM/SPIT; • overcome the lack of trusted Caller IDs; and • the ability to provide selective and controlled associations. Federation examples: • Transport Level Security (TLS)-based. (SIP over TLS). Used on the public Internet where the federation acts as a Certificate Authority (CA). • Private Network. The case where a federation builds its own network where members connect directly over this network. • SIP hubs / Transit networks. The case where calls are routed via a central SIP proxy. See *Peering*.
Firewall (FW)	Software or hardware specifically configured to limit access to a data network.
Fully-Qualified Domain Name (FQDN)	An FQDN is that portion of an Internet Uniform Resource Locator (URL) that fully identifies the server program that an Internet request is addressed to. The FQDN includes the second-level domain name (such as "**sipera.com**") and any other levels (for

Acronym	Definition
	example, "**www.sipera.com**"). The prefix "**http://**" added to the fully-qualified domain name completes the URL.
Gateway (GW)	A routing device within an IP network that connects a VoIP network with PBXs and PSTN devices by converting application-layer information from one protocol to another.
Global Cluster	Two or more nodes of a UC-Sec functional element, such as Signaling or Intelligence.
Global Node	One logical E-SBC functional entity (Signaling or Intelligence) that is deployed in a network.
H.323	ITU Recommendation that defines "packet-based multimedia communications systems." It defines a distributed architecture for creating multimedia applications, including VoIP.
Hashing	The process of transforming a string of characters into a usually shorter fixed-length value or key that uniquely represents the original string. Hashing is oftentimes used to index and retrieve items in a database because it is faster to find them using the shorter hashed key than to find it using the original value. Hashing is also used in many encryption algorithms.
High-Availability	The E-SBC feature which allows two E-SBC security devices to be deployed as an integral pair, wherein one of the devices functions as the **Primary** and the other as an **Alternate** or **Stand-by**. Connected by a heartbeat signal and shared database, the two E-SBC security devices provide fail-over protection in the event one of the devices malfunctions.
Hypertext Transfer Protocol (HTTP)	The protocol used by web browsers and web servers to transfer text, graphics, and multimedia files.
IM Logging	Any method used to log and archive instant messages; usually required as a result of a company's internal IT policies, but more often now required and enforced by federal regulations such as SOX to ensure the integrity and validity of financial reports (*see SOX*).
Integrity	The ability to keep information unaltered / uncorrupted by unauthorized users or events.
Internet Protocol (IP)	A network-layer (OSI Layer 3) protocol in the TCP/IP stack that offers a connectionless internetwork service. IP provides features for addressing, type-of-service (ToS) specifications, fragmentation and reassembly, and security.
Internet Protocol Security (IPSec)	IPSec is a general framework of open standards which provide for the integrity, confidentiality, and authentication of data exchanged between two peers.
Intrusion	A malicious user or process deliberately masquerading as a legitimate user or process.
IP Softphone	A special software client that enables a computer to function as a VoIP telephone, including an on-screen dialing pad for point-and-click dialing.
Key Agreement Protocol	A type of cryptographic protocol whereby two or more parties to a communications exchange agree on a key in such a way that both influence the outcome. If properly done, this precludes undesired third-parties from forcing a key choice on the agreeing parties. Protocols which are useful in practice also do not reveal to any eavesdropping party what key has been agreed upon.

Acronym	Definition
Key Establishment	The process of establishing a shared secret key to be used for encrypting data exchanged between a client and a server over a Transport Layer Security (TLS) connection. Key establishment is also referred to as “key exchange”. In some key exchanges (e.g., RSA), the client generates a random key and sends it to the server. In other schemes (e.g., Diffie-Hellman, or DH) the server generates some random data, sends it to the client, the client generates additional random data, combines it with the server’s random data, and the resulting “key” is sent to the server to be used as a secret key. This latter scheme is an example of a “key agreement” type of key establishment because the two sides together agree on the key. See also *Diffie-Hellman (D-H) Key Exchange* and *Rivest, Shamir, & Adleman (RSA)*.
Latency	The amount of time it takes for a packet to cross a network connection, from sender to receiver. Also, the amount of time a packet is held by a network device (firewall, router, etc.) before it is forwarded to its next destination.
Location Directory Access Protocol (LDAP)	A Software protocol for enabling anyone to locate resources in a network. LDAP is a less robust version of the more commonly found Directory Access Protocol (DAP).
Location Server (LS)	An LS is used by a SIP redirect or proxy server to obtain information about a called party's possible locations. It contains a list of bindings of address-of-record keys to zero or more contact addresses. Bindings can be created and removed in many ways; the SIP specification defines a REGISTER method for updating these bindings. Location servers are often collocated with redirect servers.
Management Information Base (MIB)	An MIB is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of the SNMP. (All other MIBs are extensions of this basic management information base.) MIB-I refers to the initial MIB definition; MIB-II refers to the current definition. SNMP v2 includes MIB-II and adds some new objects. There are MIBs (or more accurately, MIB extensions) for each set of related network entities that can be managed. For example, there are MIB definitions specified in the form of Requests for Comments (RFCs) for Domain Name System (DNS), Fiber Distributed-Data Interface, and RS-232C network objects. Product developers can create and register new MIB extensions.
Man-in-the-Middle Attack (MIM)	A type of network security attack wherein an attacker takes control of an established communications session and masquerades as one of the participating end points. In this type of attack, the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other directly. The attacker uses a program that appears to be the server to the client and appears to be the client to the server. This attack may be used simply to gain access to the messages, or to enable the attacker to modify them before retransmitting them. (See also *public key infrastructure*).
Master Key Identifier (MKI)	That field of the Secure Real-Time Transport Protocol (SRTP) that identifies the master key from which the session keys were derived that authenticate and / or encrypt a particular packet. The MKI can also be used by key management to re-key and to identify a particular master key with the cryptographic text.

Acronym	Definition
Media Access Control (MAC)	The part of the network interface that controls physical access to the LAN through the MAC address.
Media Access Control (MAC) Address	An address that uniquely identifies a network device or endpoint in a Local Area Network (LAN). The MAC address is typically represented in hexadecimal notation (00-04-24-58-90-6E). On an Ethernet LAN, the Mac address is the same as the Ethernet address. When a computer or other MAC addressed device is connected to an Internet Protocol (IP) host, a table translates the physical MAC address to a corresponding IP address that can be accessed by other devices on the LAN. The MAC address is used by the Media Access Control sublayer of the Data Link Layer (DLL) of telecommunication protocols. There is a different MAC sublayer for each physical device type.
Media Gateway Server (MGC)	A device within an IP network which controls media and signaling gateways.
Media Release	See *Anti-tromboning.* See also *Tromboning*.
Message Integrity	The ability to ensure that the message that was received is same as the message that was sent.
Multimedia Session	A set of media streams that exist for a certain duration of time.
Multiprotocol Label Switching (MPLS)	MPLS essentially integrates Layer 2 (Data Link Layer) information about network links such as bandwidth, latency and utilization into Layer 3 (IP Layer) to improve IP packet exchange. MPLS gives network operators more flexibility to divert and route traffic around link failures, congestion and bottlenecks, allowing converged networks to operate more fluidly. In an MPLS network, incoming data packets are assigned a "label" by a Label Edge Router (LER). Packets are then forwarded along a Label Switch Path (LSP) where each LSR makes forwarding decisions based solely on the contents of the label. At each hop, the LSR strips off the existing label and applies a new label which tells the next hop how to forward the packet. LSPs are established by network operators for a variety of purposes, such as to guarantee a certain level of performance, to route data around network congestion, or to create IP tunnels for network-based Virtual Private Networks (VPNs). In many ways, LSPs are no different than circuit-switched paths in Asynchronous Transfer Mode (ATM)or Frame Relay networks, except that they are not dependent on a particular Layer 2 (Data Link Layer) technology. An LSP can be established that crosses multiple Layer 2 transports such as ATM, Frame Relay or Ethernet. Thus, one of the unique abilities of MPLS is to create end-to-end circuits, with specific performance characteristics, across any type of transport medium, eliminating the need for overlay networks or Layer 2-only control mechanisms.
Multipurpose Internet Mail Extension (MIME)	A technical standard that describes the transmission of non-text data (or data that cannot be represented in plain ASCII code). It is often used in email to deal with foreign language text as well as for audio and video data. MIME is defined in Request For Comments (RFC) 2045.
Naming Authority Pointer (NAPTR)	A TYPE OF Domain Name Service (DNS) record that supports

Acronym	Definition
	regular expression (regex)-based rewriting. See *Regular Expression (Regex)*.
Network Address Translation (NAT) Device	A "barrier" device placed between two networks that translates an IP address used in one network to a different address known within the other network. One of these networks is designated the *inside* network (for example, an enterprise LAN) and the other is the *outside* network (for example, the Internet). Users on the inside network can "see" the outside network, but the outside can't see the inside users, as all communication with the outside network is through the NAT device. (*See also PAT*).
Network Service Access Point (NSAP)	The part of the network address that identifies which application on the host system in sending or receiving a packet. See *Transport Service Access Point (TSAP)*.
Network Time Protocol (NTP)	One of three TCP/IP Application Layer protocols (see also *RTCP* and *RTP*). NTP enables and synchronizes system timing to ensure that signals are received and transmitted within the proper timeframe to assure call quality.
Nonce	A parameter that varies with time. A nonce can be a time stamp, a visit counter on a web page, or a special marker intended to limit or prevent the unauthorized replay or reproduction of a file. Because a nonce changes with time, it is easy to tell whether or not an attempt at replay or reproduction of a file is legitimate; the current time can be compared with the nonce. If it does not exceed it or if no nonce exists, then the attempt is authorized. Otherwise, the attempt is not authorized. In SSL / TLS, a nonce is a 32-bit timestamp and a 28-byte random field that is used during key exchange to prevent replay attacks.
NT LAN Manager (Microsoft™)	A Microsoft authentication protocol used with the Server Message Block (SMB) protocol. See *Server Message Block (SMB)*.
Office Communications Server (Microsoft™)	Microsoft Office Communications Server 2007, OCS 2007, is an enterprise real-time communications server, providing the infrastructure for enterprise instant messaging, presence, file transfer, Peer to peer and multiparty Voice and Video calling, ad hoc and structured conferences (audio, video and web) and PSTN connectivity.
Packet Spoofing	Impersonating a legitimate user transmitting data.
P-Asserted-ID	A private extension used in the Session Initiation Protocol (SIP). The P-asserted-id is a Sip header field that contains a SIP Uniform resource Identifier (URI) and an optional display name such as: `"Joe Brown" <sip:topengr@sipera.com>` A SIP proxy server can insert a P-asserted-id header into a message and forward it to another trusted proxy. However, if the user requests that this information be kept private, then the SIP proxy must remove this field prior to forwarding it to an *un*trusted proxy.
Passphrase	A sequence of words or other text used to control access to a protected network or system, program, or data. A passphrase is similar to a password, but generally longer and with more restrictions for added security. Passphrases are often used to control both access to and operation of cryptographic programs and systems. Passphrases are particularly application to systems that use the passphrase as an encryption key.

Acronym	Definition
Peering (Direct)	An alternative to a Federation (see *Federation*). Peering is a mode of SIP-to-SIP communications where two or more SIP-based enterprises get together, exchange directory and routing information between them, and set-up policies and procedures for communicating amongst themselves. Not as scalable as the federation model.
Persistent Shared Object Model (PSOM)	Persistent Shared Object Model (often referred to as PSOM), is a Microsoft Protocol used in Web Conferencing with Microsoft's OCS 2007 and Live Meeting Console products. PSOM is used to download content for a web conferencing client (i.e. Live Meeting Console). PSOM uses port 8057 (over TLS) to listen for PSOM connections from Live Meeting console web conferencing client.
Port	A special number present in the header of a data packet (such as those used by TCP and UDP) used to "map" data to a particular process running on a computer/server/host. As an example, a server used for sending and receiving e-mail may provide both a Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) 3 service; each of which will be handled by different processes on the server. The port number, then, will be used to determine which data is associated with which process; SMTP or POP3.
Port Scanning	A method used by individuals to break into a network to see which assets or services they can hi-jack for their own use or sabotage to limit their use by someone else. A port scan essentially consists of sending a message to each port, one at a time, and monitoring what kind of response, if any, is received. The type of response indicates whether the port is used and can therefore be exploited further. Since network services are normally associated with a "well-known" port number which provides access to it, a port scan can effectively identify which network resources can be exploited further.
Proxy Server	The server on which a given resource or application neither resides nor is to be created. To complete a client request, the proxy server must get the requested resource or application from the original host server.
Proxy Server	The proxy server is an intermediary SIP network entity that acts as both a server and a client for the purpose of making requests on behalf of other clients.
Public Key Infrastructure (PKI)	PKI is a digital certificate that enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and other information through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.
Real-Time Transfer Protocol (RTP)	A commonly used Internet protocol which enables the transport of real-time data over packet-oriented networks.
Real-Time Transport Control Protocol (RTCP)	A companion protocol to RTP that is used for gathering statistics on the performance of the RTP connection. These statistics are used to dynamically adjust and optimize the connection for current network conditions. *See RTP*.
Redirect Server (RD)	The RD is a server that accepts a SIP request form a client initiating a call and checks the address of the endpoint being called against an address table for any additional addresses which can

Acronym	Definition
	be mapped to the one in the request. The results are returned to the client. Unlike proxy servers, redirect servers do not pass the request to other servers.
Regular Expression (RegEx)	'RegEx' or 'regex' is a way for a user to define how an application should search for a specific pattern in text strings and then what the application should do when a pattern match is found. For example, a regular expression could tell a program to search for all text lines that contain the word "SPAM" and then implement a security filter to block all calls from the offending source.
Remote Authentication Dial-in User Service (RADIUS)	A popular authentication, authorization, and accounting (AAA) protocol for network access or IP mobility applications which can be used in both local and roaming situations.
Rivest, Shamir, & Adleman (RSA)	RSA describes a public key encryption algorithm and certification process to protect user data over networks. The system was designed by three individuals whose last names now designate the process.
Root Certificate (RC)	In cryptography and computer security, a root certificate is an unsigned public key certificate, or a self-signed certificate, and is part of a Public Key Infrastructure (PKI) scheme. The most common commercial variety is based on the ITU-T X.509 standard. Normally an X.509 certificate includes a digital signature from a Certificate Authority (CA) which vouches for correctness of the data contained in a certificate. The authenticity of the CA's signature, and whether the CA can be trusted, can be determined by examining its certificate in turn. This chain must however end somewhere, and it does so at the **root certificate**, so called as it is at the root of a tree structure. (A CA can issue multiple certificates, which can be used to issue multiple certificates in turn, thus creating a tree). Root certificates are implicitly trusted. They are included with many software applications. The best known is Web browsers; they are used for SSL/TLS secure connections. However this implies that you trust your browser's publisher to include correct root certificates, and in turn the certificate authorities it trusts, and anyone to whom the CA may have issued a certificate-issuing-certificate, to faithfully authenticate the users of all their certificates. This (transitive) trust in a root certificate is merely assumed in the usual case, there being no way in practice to better ground it, but is integral to the X.509 certificate chain model.
Sarbanes-Oxley Act of 2002 (SOX)	A group of federal regulations which very strictly defines and enforces how businesses safeguard, disseminate, store, track, and report financial transaction-related information.
Secure Sockets Layer (SSL)	SSL is a commonly-used method for managing the security of a message transmitted via the Internet and is included as part of most browsers and Web server products. Originally developed by Netscape, SSL gained the support of various influential Internet client/server developers and became the de facto standard until evolving into Transport Layer Security (TLS). The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer (where a "socket" is an endpoint in a connection). SSL uses the Rivest, Shamir, and Adleman (RSA) public-and-private key encryption system, which also includes the use of a digital certificate.

Acronym	Definition
	If a Web site is hosted on a server that supports SSL, SSL can be enabled and specific Web pages can be identified as requiring SSL access. TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.
Security Association (SA)	An SA is the process by which "secret words" or "keys" are exchanged between communicating parties in order to establish a secure connection. SA also entails the management, life, and rotation of keys during the communication session.
Server	A device or application that passively waits for connection requests from one or more clients. A server may accept or reject a connection request from a client.
Server Authentication	The process of authenticating the server's identity by using the server certificate (in TLS).
Server Message Block (SMB)	The Server Message Block (SMB) operates as an application-level network protocol mainly used to provide shared access to files, printers, serial ports, and miscellaneous communications between nodes in a network.
Service Record (SRV)	A category of data in the Domain Name Server (DNS) that specifies information on available services. Required in Session Initiation Protocol (SIP).
Session	A series of interactions between two end points that occur during the span of a single communications connection. Typically, one end point requests a connection with another specific end point and if that end point replies agreeing to the connection, the end points take turns exchanging commands and data ("talking to each other"). The session begins when the connection is established at both ends and terminates when the connection is ended.
Session Description Protocol (SDP)	SDP is the protocol used to describe multimedia session announcement, multimedia session invitation and other forms of multimedia session initiation. SDP determines the highest level of common services between two endpoints.
Session Hijack	A type of network security attack wherein the attacker takes control of a communication session between two end points and masquerades as one of them (see *Man-in-the-Middle Attack*).
Session Initiation Protocol (SIP)	SIP is a peer-to-peer (request-response) signaling protocol for initiating, managing and terminating voice and video sessions across packet networks. SIP permits peers (also known as user agents) to effectively operate as a single, coherent communications system.
Session Initiation Protocol (SIP) for Instant Messaging and Presence Leveraging Extensions (SIMPLE)	SIMPLE is an open standard Instant Messaging (IM) and presence protocol that applies SIP to the problems of: (1) registering for presence information and receiving notifications when such events occur; (2) sending short messages, analogous to SMS or two-way paging; and (3) managing a session of real-time messages between two or more participants.
Simple Object Access Protocol (SOAP)	SOAP is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on Extensible Markup Language (XML) as its message format, and usually relies on other Application Layer protocols (most notably Remote Procedure Call (RPC) and HTTP) for message negotiation and transmission. SOAP can form the foundation layer of a web services protocol stack, providing a basic

Acronym	Definition
	messaging framework upon which web services can be built.
SIP Entities	A SIP network is composed of four types of logical SIP entities, each of which has a specific function and participates in SIP communications either as a client (initiating requests), a server (responds to requests), or both. The four entities are: *user agent*, *proxy server*, *redirect server*, and *registration server*.
SIP Trunk	A VoIP trunk from a service provider that uses SIP for call control and routing, enabling an enterprise to create a single, pure connection to carrier clouds. A SIP proxy in the enterprise peers with a carrier SIP proxy, with the appropriate federations and security protections between them. Voice is simply layered on top of the network as another IP application, traversing routers, switches, and border elements.
SNMP Traps	Unsolicited SNMP messages used to notify the management node of significant system events (alarms).
Socket	A method of communication between a client and a server in a network. Specifically, a socket is defined as "the endpoint in a connection" and is created and used with a set of programming requests or "function calls" sometimes called the socket's Application Programming Interface (API).
SPAM	A common term used to describe the deliberate flooding of Internet addresses or voice mail boxes with multiple copies of the same digital or voice message in an attempt to force it on users who would not otherwise choose to receive it. SPAM can be either malicious or simply annoying, but in either case the cost of sending those messages are for the most part borne by the recipient or the carriers rather than by the sender (SPAMMER).
SPAM-over-Instant Messaging (SPIM)	SPIM is a term used to designate unsolicited bulk messages that target Instant Messaging (IM) services. SPIM is perpetuated by bots (short for "robot", a computer program that runs automatically) that harvest IM screen names off of the Internet and simulate a human user by sending SPAM to the screen names via an IM. The SPIM typically contains a message or link to a Web site that the 'Spimmer' (the individual or organization responsible for sending the SPIM) is trying to market.
SPAM-over-Internet Telephony (SPIT)	SPIT is a term used to designate unsolicited bulk messages broadcast over VoIP to phones connected to the Internet. Although marketers already use voice mail for commercial messages, SPIT makes a more effective channel because the sender can send messages in bulk instead of dialing each number separately. Internet phones are often mapped to telephone numbers, in the interests of computer-telephony integration (CTI) but each has an IP address as well. Malicious users can harvest VoIP addresses or may hack into a computer used to route VoIP calls. Furthermore, because calls routed over IP are much more difficult to trace, the potential for fraud is significantly greater. (See also *SPAM*).
Spoof	A prevalent method of deceiving VoIP endpoints to gain access to and manipulate its resources (for example, faking an Internet address so that a malicious user looks like a known or otherwise harmless and trusted Internet user).
Subscriber	A subscriber is a user (SIP endpoint) that has static subscriber information such as user ID, password, and call-forwarding settings. Subscribers generally register dynamically with the SIP network by means of a periodic REGISTER request from their SIP

Acronym	Definition
	endpoint (see *User Agent*). User agents can include cell phones, desk phones, PC clients, and personal digital assistants (PDAs).
Synchronization Source (SSRC)	A Real-Time Protocol (RTP) variable that is used to indicate the source that is responsible for setting the sequence number and the timestamp value in the RTP message.
Syslog	The standard for forwarding log messages in an IP network. The term “Syslog” is often used for both the actual Syslog protocol, as well as the application or library sending the Syslog messages.
Transmission Control Protocol (TCP)	One of two major control protocols in the TCP/IP family of protocols. In VoIP calls, the TCP protocol is replaced by the other major control protocol, UDP. *See User Datagram Protocol*.
Transport Layer Security (TLS)	A popular security protocol that ensures privacy between servers (applications) and clients (users) communicating on the IP network. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL). TLS is composed of two layers: the *TLS Record Protocol* and the *TLS Handshake Protocol*. The TLS Record Protocol provides connection security using some encryption method such as the Data Encryption Standard (DES), but can also be used without encryption. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged. Although TLS is based on Netscape's SSL 3.0 protocol, the two are not interoperable. See *Secure Sockets Layer (SSL)*.
Transport Service Access Point (TSAP)	That part of the OSI IP addressing scheme that identifies the Network Service Access Point (NSAP) between the Session Layer and the Network Layer. See *Network Service Access Point (NSAP)*.
Triple DES (TDES)	See *Data Encryption Standard (DES)*.
Tromboning	The situation where RTP media traffic originates at a certain point within a network and follows a path out of that network into another network (the access network, for example) and back again to a destination close to where it originated. See *Anti-Tromboning*.
Tunneling	A security method used to ensure that data packets traversing an unsecure public network do so in a secure manner that prevents disruption or tampering.
Unified Communications (UC)	An evolving communications technology architecture which automates and unifies all forms of human and device communications in context, and with a common experience. Its purpose is to optimize business processes and enhance human communications by reducing latency, managing flows, and eliminating device and media dependencies.
Uniform Resource Locator (URL)	A subset of the Uniform Resource Identifier (URI) and is the Web page address of a specific point of content on the Internet. URLs typically describe (1) the mechanism used to access the requested resource, (2) the specific computer that the resource is housed on, and (3) the specific name of the resource (normally a file name) on the computer.

Acronym	Definition
User Agent (UA)	The user agent (UA) is the endpoint entity (see *Subscriber*) which initiates and terminates sessions by exchanging requests and responses. RFC 2543 defines the UA as an application which contains both a UA client (UAC) and a UA server (UAS).
User Agent Client (UAC)	The UAC is a client application that initiates a SIP request.
User Agent Server (UAS)	The UAS is a server application that contacts the user when a SIP request is received and returns a response (ACCEPT, REJECT, or REDIRECT) on behalf of the user.
User Datagram Protocol (UDP)	As an alternative to TCP, UDP is a control protocol used to process VoIP calls with an IP network. Implemented at the transport layer, UDP uses IP to transport a data unit (called a *datagram*) from one point to another. UDP is normally preferred by IP applications that want to save processing time because the datagrams exchanged are normally very small and no packet processing is done.
Variable Length Subnet Mask (VLSM)	See *Classless Inter-Domain Routing (CIDR)*.
Virtual IP Addressing (VIPA)	VIPA is an internet addressing scheme which eliminates a host system's dependency upon individual, physical network interfaces. This means that although incoming packets are sent to a system's VIPA address, they actually travel through the an actual, physical interface. Previously, if an interface failed, any connections to that interface were immediately lost. With VIPA implemented on the system and routing protocols within the network providing automatic rerouting, recovery from the failure occurs without disrupting existing user connections that are using the interface as long as packets can continue to arrive through another physical interface.
Virtual LAN (VLAN)	A manner of segmenting a switched network according to a logical topology. For example, a VLAN can be used to group or restrict data traffic in a domain to a logical entity such as a workgroup. VLANs enhance network performance and security.
Virus	A program that replicates itself by being copied or initiating its copying to another program, operating system, or document. Viruses are transmitted in many ways, such as in attachments to e-mails, as part of downloadable files, or be present on diskettes or CDs. Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances or events cause their code to be executed by the unsuspecting host.
VLAN Tag	A four-byte tag that contains a VLAN Identifier (VID) and certain user priority information to identify which VLAN that data packet is assigned.
Voice-over-Internet Protocol (VoIP)	Voice-over-Internet Protocol (VoIP) is a reliable technology that enables routing of typical voice conversations over the Internet or any other IP network. Voice data (e.g. telephone calls and faxes) is transmitted with POTS-like functionality and audio quality over a general-purpose, packet-switched network instead of the more traditional and expensive dedicated, circuit-switched voice transmission lines.

Acronym	Definition
Zero-Day Attack	A particular type of exploit that takes advantage of a security vulnerability in a network on the same day that the vulnerability itself becomes generally known. Ordinarily, since the vulnerability isn't known in advance, there is oftentimes no way to guard against an exploit or attack until it happens.
Zombie	A IP network element that has been surreptitiously 'taken-over' by an attacker, usually without the user's knowledge.

System Alarm List C

This appendix contains a description of the *E-SBC* system-generated alarms.

CPU Alarms

Alarm: CPU

Message: `CPU utilization is over 80%`
Condition: CPU utilization is between 80%-89%.
Service Affecting: No.
Type: Alarm.
Severity: Minor.
Description: CPU utilization is between 80% - 89%.
Clearing Event: CPU utilization goes below 80% or above 89%.
Manual Intervention: No.

Alarm: CPU

Message: `CPU utilization is over 90%`
Condition: CPU utilization is between 90%-99%.
Service Affecting: No.
Type: Alarm.
Severity: Major.
Description: CPU utilization is between 90% - 99%.
Clearing Event: CPU utilization goes below 90% or becomes 100%.
Manual Intervention: No.

Alarm: CPU

Message: `CPU utilization is 100%`
Condition: CPU utilization is 100%.
Service Affecting: Yes.
Type: Alarm.
Severity: Critical.
Description: CPU utilization is 100%.
Clearing Event: CPU utilization goes below 100%.
Manual Intervention: No.

Memory (including Swap Space) Alarms

Alarm: MEMORY

Message:	`Memory utilization is over 80%`
Condition:	Memory utilization is between 80%-89%.
Service Affecting:	No.
Type:	Alarm.
Severity:	Minor.
Description:	Memory utilization is between 80% - 89%.
Clearing Event:	Memory utilization goes below 80% or above 89%.
Manual Intervention:	No.

Alarm: MEMORY

Message:	`Memory utilization is over 90%`
Condition:	Memory utilization is between 90%-99%.
Service Affecting:	Yes.
Type:	Alarm.
Severity:	Major.
Description:	Memory utilization is between 90% - 90%.
Clearing Event:	Memory utilization goes below 90% becomes 100%.
Manual Intervention:	No.

Alarm: MEMORY

Message:	`Memory utilization is 100%`
Condition:	Memory utilization is 100%.
Service Affecting:	Yes.
Type:	Alarm.
Severity:	Critical.
Description:	Memory utilization is 100%.
Clearing Event:	Memory utilization goes below 100%.
Manual Intervention:	No.

Disk Partition Space Alarms

Alarm: DISK PARTITION SPACE

Message:	`Disk partition <partition_name> utilization is over 80%`
Condition:	Disk partition utilization is between 80% - 89%.
Service Affecting:	No.
Type:	Alarm.
Severity:	Minor.
Description:	Disk utilization is between 80% - 89% for a given partition.
Clearing Event:	Disk utilization goes below 80% or above 89%.
Manual Intervention:	No.

Alarm: DISK PARTITION SPACE

Message:	Disk partition <*partition_name*> utilization is over 90%
Condition:	Disk partition utilization is between 90% - 99%.
Service Affecting:	Yes.
Type:	Alarm.
Severity:	Major.
Description:	Disk utilization is between 90% - 99% for a given partition.
Clearing Event:	Disk utilization goes below 90% becomes 100%.
Manual Intervention:	No.

Alarm: DISK PARTITION SPACE

Message:	Disk partition <*partition_name*> utilization is 100%
Condition:	Disk partition utilization is 100%.
Service Affecting:	Yes.
Type:	Alarm.
Severity:	Critical.
Description:	Disk utilization is 100% for a given partition.
Clearing Event:	Disk utilization goes below 100%.
Manual Intervention:	No.

Disk Failure Alarms

Alarm: HARD DISK FAILURE

Message:	Hard disk <*disk_ID*> failure
Condition:	Hard disk failure.
Service Affecting:	Yes.
Type:	Alarm.
Severity:	Critical.
Description:	The hard disk drive has failed and cannot be used.
Clearing Event:	The alarm is cleared only when the kernel detects no failures when testing the hard disk drive. This will only happen when the hard disk drive is replaced.
Manual Intervention:	Yes. Hard disk drive must be replaced.

Link Failure Alarms

Alarm: LINK FAILURE

Message:	`Network link failure <interface>`
Condition:	Network link goes down on the given interface.
Service Affecting:	Yes. No traffic can be sent or received on the failed link.
Type:	Alarm.
Severity:	Critical.
Description:	A link on a particular interface in down and cannot be used.
Clearing Event:	Network connection is restored and alarm manually cleared by user.
Manual Intervention:	Yes. User needs to manually restore the link.

Process Failure Alarms

Alarm: PROCESS FAILURE

Message:	`Application failure`
Condition:	One or more system processes failed to send a heartbeat ping.
Service Affecting:	Yes. Port By-pass is automatically enabled.
Type:	Alarm.
Severity:	Critical.
Description:	One or more system processes is malfunctioning
Clearing Event:	Malfunctioning process is restarted either automatically by the system or manually by the Security Administrator and the alarm cleared.
Manual Intervention:	Yes. Required if automatic self-start is not successful.

Database Failure Alarms

Alarm: DATABASE FAILURE

Message:	`Database failure`
Condition:	Connectivity to the database has been lost.
Service Affecting:	Yes. Port By-pass is automatically enabled after multiple failed restarts.
Type:	Alarm.
Severity:	Critical.
Description:	Either the database is down or connectivity to the database has been lost.
Clearing Event:	The database failure being cleared either automatically by the system or manually by the Security Administrator.
Manual Intervention:	Yes. Required if automatic self-start is not successful.

Component Failure Alarms

Alarm: COMPONENT FAILURE

Message:	Component failure
Condition:	One or more elements (signaling, media, intelligence, or EMS) in a multi-component configuration has failed to send a heartbeat ping.
Service Affecting:	Yes
Type:	Alarm
Severity:	Critical
Description:	One or more E-SBC server elements (signaling, media, intelligence, or EMS) is malfunctioning.
Clearing Event:	The malfunctioning elements could be restarted manually and the alarm cleared manually.
Manual Intervention:	Required if self restart in not successful.

This page left intentionally blank

GUI and Console Alarm List D

This appendix contains a description of the E-SBC GUI and Console-generated alarms.

New User Added Alarms

Alarm: NEW USER ADDED

Message: New User Added: <*username*>

Condition: A new GUI / System user was added.

Service Affecting: No.

Type: Alarm.

Severity: Informational.

Description: A new user was added to the system.

Clearing Event: Alarm either cleared by the administrator or it times-out.

Manual Intervention: No.

New Administrator Added Alarms

Alarm: NEW ADMIN ADDED

Message: Admin User Added: <*username*>

Condition: A new GUI / System admin user was added.

Service Affecting: No.

Type: Alarm.

Severity: Informational.

Description: A new admin user was added to the system.

Clearing Event: Alarm either cleared by the administrator or it times-out.

Manual Intervention: No.

User Privilege Change Alarms

Alarm: USER PRIVILEGE CHANGE

Message: User Privilege Changed: <*username*>

Condition: A user's access privilege was changed (either from admin to normal or from normal to admin).

Service Affecting: No.

Type: Alarm.

Severity: Informational.

Description: A user's access privilege was changed (either from admin to normal or from normal to admin).

Clearing Event: Alarm either cleared by the administrator or it times-out.

Manual Intervention: No.

User Deleted Alarms

Alarm: USER DELETED

Message:	User Deleted: <*username*>
Condition:	A new GUI / System admin user was deleted.
Service Affecting:	No.
Type:	Alarm.
Severity:	Informational.
Description:	A user was deleted from the system.
Clearing Event:	Alarm either cleared by the administrator or it times-out.
Manual Intervention:	No.

Login Failure Alarms

Alarm: LOGIN FAILURE

Message:	User Login Failure: <*username*>
Condition:	A user had multiple consecutive login failures.
Service Affecting:	No.
Type:	Alarm.
Severity:	Warning.
Description:	A user had more than a certain number of consecutive login failures.
Clearing Event:	Alarm either cleared by the administrator or it times-out.
Manual Intervention:	No.

E-SBC SNMP Details E

This appendix provides SNMP details on Sipera's E-SBC appliance. Standard Management Information Bases (MIBs) are defined in RFC-1213. Sipera E-SBC supports rfc1213.mib on E-SBC 200/300/500.

MIB-II Support

With E-SBC Product Release 4.0.4.Q28, support was added for MIB-II (RFC1213) for the E-SBC data interfaces. UDP port 8001 is used for MIB-II support.

- E-SBC listens on Port 161for sipera-mib
- Port 8001 is used for MIB-II

E-SBC OID Descriptions

This section contains a description of the key Object Identifiers (OIDs).

Private Enterprise OIDS supported on Sipera E-SBC Appliance

ipcs stats sip calls: .1.3.6.1.4.1.25257.1.4.1

.iso.org.dod.internet.private.enterprises.sipera.ipcsstatisticsinfo.ipcsstatssip.ipcsstatssipcalls

ipcs stats sip protocol: .1.3.6.1.4.1.25257.1.4.3

.iso.org.dod.internet.private.enterprises.sipera.ipcsstatisticsinfo.ipcsstatssip.ipcsstatssipprotocol

Ipcsincidenceinfo: .1.3.6.1.4.1.25257.2

.iso.org.dod.internet.private.enterprises.sipera.ipcsincidencesinfo

Ipcsalarmainfo: .1.3.6.1.4.1.25257.4

.iso.org.dod.internet.private.enterprises.sipera.ipcsalarmsinfo

MIB Tree Structure

An MIB tree structure diagram for the OIDs listed above is provided in Figure E - 1 on the next page.

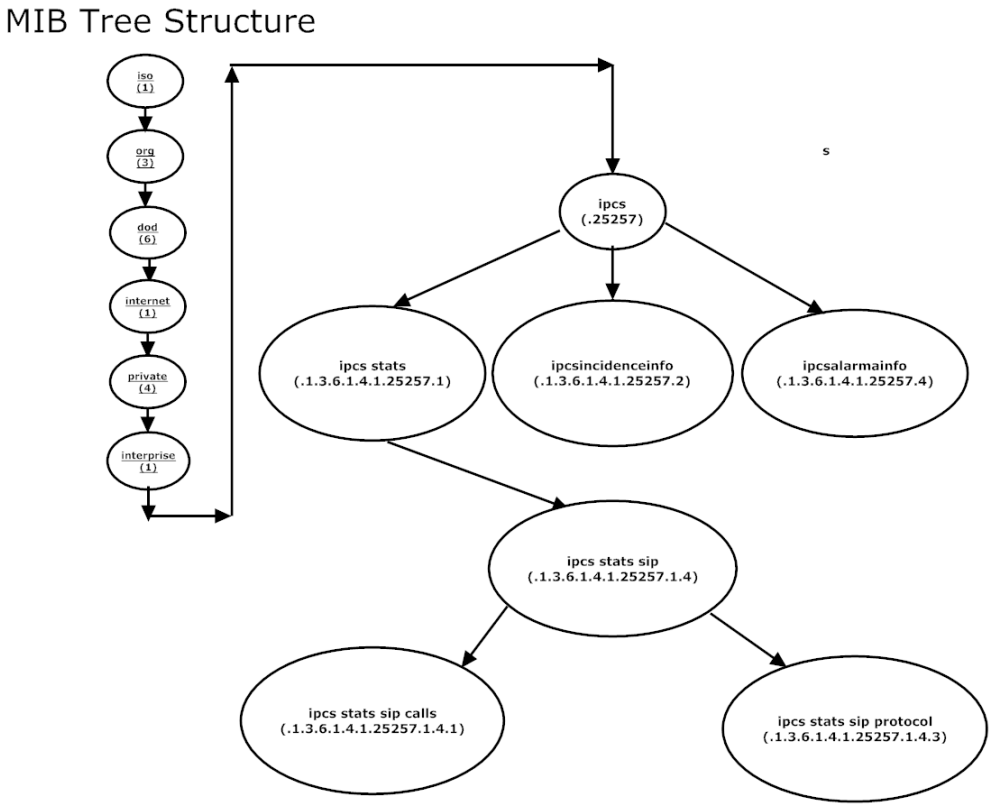


Figure E - 1 MIB Tree Structure

Key OIDS

Ipcsstatssipcalls

ipcssipcTotalRegistrationRequests

Number of Registration Requests received at node. This does not include the registration triggered by node for keeping the pinhole open.

ipcssipcTotalRegistrationsChallenged

Number of Registrations Challenged by node and also includes the number of challenges from the Call Server. The number of registrations challenged by IPCS node includes the SIP 401/407 based Radius Authentication Responses (AAA feature) and SIP 407 based SIV Authentication Responses (DOS feature).

ipcssipcTotalRegistrationsRejected

Number of Registrations Rejected by the node and also includes the failed registration responses observed from the call server at the node. Failed registration responses include the SIP 4xx-7xx class responses excluding SIP 400, SIP 401/407 Responses. The registrations are rejected by node due to failed registration challenges, failed registration processing and registrations blocked due to security features.

ipcssipcTotalCallsReceived

Total Number of SIP Calls received at the node. This one equals Calls Blocked + Calls Allowed.

ipcssipcTotalCallsBlocked.

Number of SIP calls Blocked by the node due to SIP Parse errors, failed AAA challenges and calls blocked due to security features.

ipcssipcTotalCallsAllowed

Number of SIP calls classified by the node as Legitimate.

Classification of Requests/Responses matching a particular Domain Policy Group at the node

ipcsTotalINVITES

Number of SIP INVITE messages

ipcsTotalINVITERetransmits

Number of SIP INVITE Retransmits

ipcsTotalINVITE100Responses

Number of SIP INVITE 100 Responses

ipcsTotalINVITE1XXResponses

Number of SIP INVITE 1XX class Responses excluding SIP 100 Response.

ipcsTotalINVITE200Responses

Number of SIP INVITE 200 Responses

ipcsTotalINVITE200ResponseRetransmits

Number of SIP INVITE 200 Response Retransmits

ipcsTotalINVITE4XX6XXResponses

Number of SIP INVITE 4XX 6XX Responses

ipcsTotalINVITE4XX6XXResponseRetransmits

Number of SIP INVITE 4XX 6XX Response Retransmits

ipcsTotalBYESent

Number of SIP BYE requests

ipcsTotalBYERetransmits

Number of SIP BYE Retransmits

ipcsTotalBYE200Responses

Number of SIP BYE 200 Responses

ipcsTotalCANCELSent

Number of SIP CANCEL requests

ipcsTotalCANCEL200Responses

Number of SIP CANCEL 200 Responses

ipcsTotalACK200Responses

Number of SIP ACK requests for INVITE 200 OK Response

ipcsTotalACK4XX6XXResponses

Number of SIP ACK requests for INVITE 4xx-6xx class Responses

ipcsTotalACKTimeOuts

Number of SIP ACK timeouts ie. Number of ACK requests missing for the INVITE 200 OK/4xx-6xx class responses.

ipcsTotalNonInviteRequests

Number of NonInvite Requests

ipcsTotalNonInvite1xxResponses

Number of NonInvite 1xx Responses

ipcsTotalNonInvite2xxResponses

Number of NonInvite 2xx Responses. Also includes the 200 OK responses for BYE and CANCEL requests.

Out of Dialog Requests Dropped

ipcsTotalOutOfDialogReferMesFromNW.

Number of Out of Dialog REFER requests dropped at the node.

IpcsTotalAckMessageOutOfDialogue.

Number of Out of Dialog ACK requests dropped at the node.

IpcsTotalByeMessageOutOfDialogue.

Number of Out of Dialog BYE requests dropped at the node.

IpcsTotalCancelMessageOutOfDialogue.

Number of Out of Dialog CANCEL requests dropped at the node.

IpcsTotalNotifyMessageOutOfDialogue.

Number of Out of Dialog NOTIFY requests dropped at the node.

ipcsTotalReinviteMessageOutOfDialogue.

Number of Out of Dialog RE-INVITE requests dropped at the node.

Out of Dialog Responses Dropped

ipcsTotal1XXMessageOutOfDialogue.

Number of Out of Dialog 1XX class responses dropped by the node.

ipcsTotal2XXMessageOutOfDialogue.

Number of Out of Dialog 2XX class responses dropped by the node.

ipcsTotal3XXMessageOutOfDialogue.

Number of Out of Dialog 3XX class responses dropped by the node.

ipcsTotal4XXMessageOutOfDialogue.

Number of Out of Dialog 4XX class responses dropped by the node.

ipcsTotal5XXMessageOutOfDialogue.

Number of Out of Dialog 5XX class responses dropped by the node.

ipcsTotal6XXMessageOutOfDialogue.

Number of Out of Dialog 6XX class responses dropped by the node.

Out of Transaction Responses Dropped

ipcsTotal1XXMessageOutOfTransaction.

Number of 1XX Messages received out of transaction dropped by the node.

ipcsTotal2XXMessageOutOfTransaction.

Number of 2XX Messages received out of transaction dropped by the node.

ipcsTotal3XXMessageOutOfTransaction.

Number of 3XX Messages received out of transaction dropped by the node.

ipcsTotal4XXMessageOutOfTransaction.

Number of 4XX Messages received out of transaction dropped by the node.

ipcsTotal5XXMessageOutOfTransaction.

Number of 5XX Messages received out of transaction dropped by the node.

ipcsTotal6XXMessageOutOfTransaction.

Number of 6XX Messages received out of transaction dropped by the node.

ipcsTotalCancelMessageOutOfTransaction.

Number of CANCEL requests received out of transaction dropped by the node.

Statistics Details With Examples

For One External-External Call Through IPCS Between the Two External Phones A and B

In the below scenarios a call is made from A to B

1. No of Registrations in Statistics: Counter increments by 2

   One registration per phone, so in total 2 registrations from both A and B .

2. No of Invites in Statistics: Counter increments by 2

   The counter increments whenever IPCS receives an INVITE
   First INVITE from phone A towards IPCS which is sent to call server.
   Second INVITE from Call Server towards IPCS which is sent to phone B

3. No of Invites 200 Responses in Statistics: Counter increments by 2

   The counter increments whenever IPCS receives a 200 Ok for INVITE sent
   First 200 ok response from phone B towards IPCS which is sent to call server.
   Second 200 ok response from Call Server towards IPCS which is sent to phone A

4. No of Bye in Statistics: Counter increments by 2

   The counter increments whenever IPCS receives a Bye
   First Bye from phone A towards IPCS which is sent to call server.
   Second Bye from Call Server towards IPCS which is sent to phone B

For One External-Internal Call Through IPCS Between the External Phone A and Internal Phone C

In the below scenarios a call is made from A to C and call is disconnected at A

1 . No of Registrations in Statistics: Counter increments by 1

   One registration per phone, so in total 1 registration.
   Phone C registration will not be seen by IPCS as it is internal phone

2 . No of Invites in Statistics: Counter increments by 1

   The counter increments whenever IPCS receives an INVITE
   INVITE from phone A towards IPCS which is sent to call server.

3. No of Invites 200 Responses in Statistics: Counter increments by 1

   The counter increments whenever IPCS receives a 200 Ok for INVITE sent
   200 ok response from phone C towards IPCS which is sent to phone A

4. No of Bye in Statistics: Counter increments by 1

   The counter increments whenever IPCS receives a Bye
   Bye from phone A towards IPCS which is sent to call server.

E-SBC MIB

This section contains the Sipera E-SBC MIB.

```
-- File Name : SIPERA_IPCS_MIB(4).mib
-- Date      : Mon Dec 09 10:16:55 IST 2009
-- Author    : AdventNet Agent Toolkit C Edition - MibEditor 6


SIPERA-IPCS-MIB    DEFINITIONS ::= BEGIN
        IMPORTS
                DisplayString, RowStatus, DateAndTime
                        FROM SNMPv2-TC
                DisplayString
                        FROM RFC1213-MIB
                enterprises, MODULE-IDENTITY, OBJECT-TYPE, Integer32, Gauge32,
Counter32, NOTIFICATION-TYPE, Counter64, IpAddress
                        FROM SNMPv2-SMI;

        moduleIdentity          MODULE-IDENTITY
                LAST-UPDATED    "200610030823Z"
                ORGANIZATION    "Sipera "
                CONTACT-INFO    ""
                DESCRIPTION             ""
                REVISION                "200610030823Z"
                DESCRIPTION             ""
                ::= { enterprises 1 }

        org     OBJECT IDENTIFIER
                ::= { iso 3 }

        dod     OBJECT IDENTIFIER
                ::= { org 6 }

        internet        OBJECT IDENTIFIER
                ::= { dod 1 }

        private OBJECT IDENTIFIER
                ::= { internet 4 }

        enterprises     OBJECT IDENTIFIER
                ::= { private 1 }

        sipera  OBJECT IDENTIFIER
                ::= { enterprises 25257 }

        ipcsstatisticsinfo      OBJECT IDENTIFIER
                ::= { sipera 1 }
```

```
    ipcsincidencesinfo      OBJECT IDENTIFIER
            ::=  {  sipera  2  }

notifications  OBJECT IDENTIFIER
    ::=  { sipera 3}

    ipcsalarmsinfo OBJECT IDENTIFIER
            ::=  {  sipera  4  }


    ipcsstatssip      OBJECT IDENTIFIER
            ::=  {  ipcsstatisticsinfo  4  }

    ipcsincidencesTable    OBJECT-TYPE
            SYNTAX              SEQUENCE  OF  IpcsincidencesEntry
            MAX-ACCESS          not-accessible
            STATUS              current
            DESCRIPTION         "Table for Incidences."
            ::=  { ipcsincidencesinfo  1 }

    ipcsincidencesEntry    OBJECT-TYPE
            SYNTAX              IpcsincidencesEntry
            MAX-ACCESS          not-accessible
            STATUS              current
            DESCRIPTION         "Row for each incidence entry."
            INDEX               {  ipcsincidenceId  }
            ::=  { ipcsincidencesTable 1 }

    IpcsincidencesEntry  ::=  SEQUENCE {
            ipcsincidenceName  OCTET STRING,
            ipcsincidenceId  Integer32,
            ipcsincidenceCategory  OCTET STRING,
            ipcsincidenceCause  OCTET STRING,
            ipcsincidenceTimeStamp  DateAndTime,
            ipcsincidenceIpcsId  OCTET STRING,
            ipcsincidencesRowStatus  RowStatus
            }


    ipcsincidenceName     OBJECT-TYPE
            SYNTAX                  OCTET STRING
            MAX-ACCESS              read-write
            STATUS                  current
            DESCRIPTION             "Name of the incidence raised."
            ::=  {  ipcsincidencesEntry  1  }
```

```
        ipcsincidenceId         OBJECT-TYPE
                SYNTAX                  Integer32
                MAX-ACCESS              not-accessible
                STATUS                  current
                DESCRIPTION             "Unique incidence Identity."
                ::= { ipcsincidencesEntry 2 }


        ipcsincidenceCategory       OBJECT-TYPE
                SYNTAX                  OCTET STRING
                MAX-ACCESS              read-write
                STATUS                  current
                DESCRIPTION             "Catagory of the incidence raised.
                                        Different categories include DOS,
                                        FINGER_PRINT, POLICY, ROUTE,
                                        MEDIA_ANOMALY, SIP_2FA."
                ::= { ipcsincidencesEntry 3 }


        ipcsincidenceCause    OBJECT-TYPE
                SYNTAX                  OCTET STRING
                MAX-ACCESS              read-write
                STATUS                  current
                DESCRIPTION             "Cause for the incidence raised."
                ::= { ipcsincidencesEntry 4 }


        ipcsincidenceTimeStamp      OBJECT-TYPE
                SYNTAX                  DateAndTime
                MAX-ACCESS              read-write
                STATUS                  current
                DESCRIPTION             "Time stamp when the incidence was
raised."
                ::= { ipcsincidencesEntry 5 }


        ipcsincidenceIpcsId    OBJECT-TYPE
                SYNTAX                  OCTET STRING
                MAX-ACCESS              read-write
                STATUS                  current
                DESCRIPTION             "ID of the UCSec on which this incidence
was raised."
                ::= { ipcsincidencesEntry 6 }
```

```
ipcsincidencesRowStatus      OBJECT-TYPE
        SYNTAX                  RowStatus
        MAX-ACCESS              read-create
        STATUS                  current
        DESCRIPTION             "RowStatus of this incidence entry."
        ::= { ipcsincidencesEntry 7 }

ipcsalarmsTable      OBJECT-TYPE
        SYNTAX          SEQUENCE OF IpcsalarmsEntry
        MAX-ACCESS      not-accessible
        STATUS          current
        DESCRIPTION     "Table for Alarms."
        ::= { ipcsalarmsinfo 1 }

ipcsalarmsEntry      OBJECT-TYPE
        SYNTAX          IpcsalarmsEntry
        MAX-ACCESS      not-accessible
        STATUS          current
        DESCRIPTION     "Row for each Alarm entry."
        INDEX           { ipcsalarmsId }
        ::= { ipcsalarmsTable 1 }

IpcsalarmsEntry ::= SEQUENCE {
        ipcsalarmsName DisplayString,
        ipcsalarmsId Integer32,
        ipcsalarmsMessage DisplayString,
        ipcsalarmsSequenceNumber Counter64,
        ipcsalarmsTimestamp DateAndTime,
        ipcsalarmsSystemType DisplayString,
        ipcsalarmsRowStatus RowStatus
        }


ipcsalarmsName      OBJECT-TYPE
        SYNTAX                  DisplayString
        MAX-ACCESS              read-write
        STATUS                  current
        DESCRIPTION             "Name of the alarm raised (Refer to the
UCSec manual for the different alarms)."
        ::= { ipcsalarmsEntry 1 }


ipcsalarmsId   OBJECT-TYPE
        SYNTAX                  Integer32
        MAX-ACCESS              not-accessible
        STATUS                  current
```

```
                DESCRIPTION             "ID of the alarm raised. Each alarm
type/alarm name will have a unique id."
                ::= { ipcsalarmsEntry 2 }


        ipcsalarmsMessage    OBJECT-TYPE
                SYNTAX                  DisplayString
                MAX-ACCESS              read-write
                STATUS                  current
                DESCRIPTION             "Detailed message relating to the alarm
raised."
                ::= { ipcsalarmsEntry 3 }


        ipcsalarmsSequenceNumber  OBJECT-TYPE
                SYNTAX                  Counter64
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Sequence number of the alarm raised. This
is the unique id for each alarm."
                ::= { ipcsalarmsEntry 4 }


        ipcsalarmsTimestamp OBJECT-TYPE
                SYNTAX                  DateAndTime
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Time stamp when the alarm was raised."
                ::= { ipcsalarmsEntry 5 }


        ipcsalarmsSystemType        OBJECT-TYPE
                SYNTAX                  DisplayString
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "ID of the UCSec on which this alarm was
raised."
                ::= { ipcsalarmsEntry 6 }


        ipcsalarmsRowStatus OBJECT-TYPE
                SYNTAX                  RowStatus
                MAX-ACCESS              read-create
                STATUS                  current
                DESCRIPTION             "RowStatus of the alarm raised."
                ::= { ipcsalarmsEntry 7 }
```

```
        ipcsincidenceNotification       NOTIFICATION-TYPE
                OBJECTS                 { ipcsincidenceCategory,
ipcsincidenceCause, ipcsincidenceId, ipcsincidenceIpcsId, ipcsincidenceName,
ipcsincidenceTimeStamp }
                STATUS                  current
                DESCRIPTION             "Notification for the incidence."
                ::= { notifications 1 }

        ipcsalarmsNotification          NOTIFICATION-TYPE
                OBJECTS                 { ipcsalarmsId, ipcsalarmsMessage,
ipcsalarmsName, ipcsalarmsSequenceNumber, ipcsalarmsSystemType,
ipcsalarmsTimestamp }
                STATUS                  current
                DESCRIPTION             "Notification for the alarm."
                ::= { notifications 2 }

        ipcsstatssipcalls       OBJECT IDENTIFIER
                ::= { ipcsstatssip 1 }

        ipcsstatssipprotocol    OBJECT IDENTIFIER
                ::= { ipcsstatssip 3 }

        ipcssipcTotalRegistrationRequests   OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Registration Requests
received.This does not include the registration triggered by IPCS for keeping the pinhole
open."
                ::= { ipcsstatssipcalls 1 }

        ipcssipcTotalRegistrationsChallenged        OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Registrations Challanged by the
node"
                ::= { ipcsstatssipcalls 2 }

        ipcssipcTotalRegistrationsRejected  OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Registrations Rejected by the
node due to failed registration challenges."
```

```
                ::= { ipcsstatssipcalls 3 }

        ipcssipcTotalCallsReceived   OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Total Number of SIP Calls received at the
node. This one equals .Calls Blocked + Calls Allowed.."
                ::= { ipcsstatssipcalls 4 }

        ipcssipcTotalCallsWithAnomalyDetected    OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Total Number of SIP Calls detected with
anomaly at the node. "
                ::= { ipcsstatssipcalls 5 }

        ipcssipcTotalCallsBlocked    OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP calls Blocked by the node.
This one is Less than or equal to Calls With Anomaly Detected.."
                ::= { ipcsstatssipcalls 6 }

        ipcssipcTotalCallsAllowed    OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP calls classified by the node
as Legitimate."
                ::= { ipcsstatssipcalls 7 }

        ipcssipcTotalMessagesExchanged    OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP messages exchanged
between the node and the network."
                ::= { ipcsstatssipcalls 8 }

        ipcssipcTotalActiveRegistrations     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
```

```
        DESCRIPTION             "Number of SIP active registrations."
        ::= { ipcsstatssipcalls 9 }

ipcssipcTotalActiveCalls    OBJECT-TYPE
        SYNTAX                  Gauge32
        MAX-ACCESS              read-only
        STATUS                  current
        DESCRIPTION             "Number of SIP active calls."
        ::= { ipcsstatssipcalls 10 }

ipcssipcTotalActiveTCPRegistrations     OBJECT-TYPE
        SYNTAX                  Gauge32
        MAX-ACCESS              read-only
        STATUS                  current
        DESCRIPTION             "Number of SIP active TCP registrations."
        ::= { ipcsstatssipcalls 11 }

ipcssipcTotalActiveUDPRegistrations     OBJECT-TYPE
        SYNTAX                  Gauge32
        MAX-ACCESS              read-only
        STATUS                  current
        DESCRIPTION             "Number of SIP active UDP registrations."
        ::= { ipcsstatssipcalls 12 }

ipcssipcTotalActiveTLSRegistrations     OBJECT-TYPE
        SYNTAX                  Gauge32
        MAX-ACCESS              read-only
        STATUS                  current
        DESCRIPTION             "Number of SIP active TLS registrations."
        ::= { ipcsstatssipcalls 13 }

ipcssipcTotalActiveSRTPCalls    OBJECT-TYPE
        SYNTAX                  Gauge32
        MAX-ACCESS              read-only
        STATUS                  current
        DESCRIPTION             "Number of SIP active SRTP calls."
        ::= { ipcsstatssipcalls 14 }

ipcssipcTotalRegistrations  OBJECT-TYPE
        SYNTAX                  Gauge32
        MAX-ACCESS              read-only
        STATUS                  current
        DESCRIPTION             "Number of SIP total registrations."
        ::= { ipcsstatssipcalls 15 }

ipcssipcTotalTCPRegistrations       OBJECT-TYPE
```

```
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP total TCP registrations."
                ::= { ipcsstatssipcalls 16 }

        ipcssipcTotalUDPRegistrations   OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP total UDP registrations."
                ::= { ipcsstatssipcalls 17 }

        ipcssipcTotalTLSRegistrations   OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP total TLS registrations."
                ::= { ipcsstatssipcalls 18 }

        ipcssipcTotalCalls      OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP total calls."
                ::= { ipcsstatssipcalls 19 }

        ipcssipcTotalCallsFailed        OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP total calls failed."
                ::= { ipcsstatssipcalls 20 }

        ipcssipcTotalRegistrationsDroppedByMissingPolicy        OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP total registrations dropped
by missing policy."
                ::= { ipcsstatssipcalls 21 }

        ipcssipcTotalInvitesDroppedByMissingPolicy      OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
```

```
                DESCRIPTION             "Number of SIP total invites dropped by
missing policy."
                ::= { ipcsstatssipcalls 22 }


        ipcssipTtlCallsDeniedDueToPolicy OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP total calls rejected due to
Policy Voilation."
                ::= { ipcsstatssipcalls 23 }


        ipcssipTtlSessDroppedDueToMaxNumofConcSessExc OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP sessions dropped due to
Max no of concurrent sessions exceed."
                ::= { ipcsstatssipcalls 24 }

        ipcsTotalINVITES    OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP INVITE messages"
                ::= { ipcsstatssipprotocol 1 }

        ipcsTotalINVITERetransmits OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP INVITE Retransmits"
                ::= { ipcsstatssipprotocol 2 }

        ipcsTotalINVITE100Responses     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP INVITE 100 Responses"
                ::= { ipcsstatssipprotocol 3 }

        ipcsTotalINVITE1XXResponses     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
```

```
                STATUS                  current
                DESCRIPTION             "Number of SIP INVITE 1XX Responses"
                ::= { ipcsstatssipprotocol 4 }

        ipcsTotalINVITE200Responses     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP INVITE 200 Responses"
                ::= { ipcsstatssipprotocol 5 }

        ipcsTotalINVITE200ResponseRetransmits   OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP INVITE 200 Response
Retransmits"
                ::= { ipcsstatssipprotocol 6 }

        ipcsTotalINVITE4XX6XXResponses          OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP INVITE 4XX 6XX
Responses"
                ::= { ipcsstatssipprotocol 7 }

        ipcsTotalINVITE4XX6XXResponseRetransmits     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP INVITE 4XX 6XX
Response Retransmits"
                ::= { ipcsstatssipprotocol 8 }

        ipcsTotalBYESent     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of SIP BYE"
                ::= { ipcsstatssipprotocol 9 }

        ipcsTotalBYERetransmits     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
```

```
            DESCRIPTION             "Number of SIP BYE Retransmits"
            ::= { ipcsstatssipprotocol 10 }

        ipcsTotalBYE200Responses  OBJECT-TYPE
            SYNTAX                  Gauge32
            MAX-ACCESS              read-only
            STATUS                  current
            DESCRIPTION             "Number of SIP BYE 200 Responses"
            ::= { ipcsstatssipprotocol 11 }

        ipcsTotalCANCELSent       OBJECT-TYPE
            SYNTAX                  Gauge32
            MAX-ACCESS              read-only
            STATUS                  current
            DESCRIPTION             "Number of SIP CANCEL"
            ::= { ipcsstatssipprotocol 12 }

        ipcsTotalCANCEL200Responses     OBJECT-TYPE
            SYNTAX                  Gauge32
            MAX-ACCESS              read-only
            STATUS                  current
            DESCRIPTION             "Number of SIP CANCEL 200 Responses"
            ::= { ipcsstatssipprotocol 13 }

        ipcsTotalCANCELRetransmits      OBJECT-TYPE
            SYNTAX                  Gauge32
            MAX-ACCESS              read-only
            STATUS                  current
            DESCRIPTION             "Number of SIP CANCEL Retransmits"
            ::= { ipcsstatssipprotocol 14 }

        ipcsTotalACK200Responses  OBJECT-TYPE
            SYNTAX                  Gauge32
            MAX-ACCESS              read-only
            STATUS                  current
            DESCRIPTION             "Number of SIP ACK 200 Responses"
            ::= { ipcsstatssipprotocol 15 }

        ipcsTotalACK4XX6XXResponses   OBJECT-TYPE
            SYNTAX                  Gauge32
            MAX-ACCESS              read-only
            STATUS                  current
            DESCRIPTION             "Number of SIP ACK 4XX 6XX
Responses"
            ::= { ipcsstatssipprotocol 16 }
```

```
        ipcsTotalACKTimeOuts        OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of ACK Time outs"
                ::= { ipcsstatssipprotocol 17 }

        ipcsTotalNonInviteRequests  OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of NonInvite Requests"
                ::= { ipcsstatssipprotocol 18 }

        ipcsTotalNonInvite1xxResponses      OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of NonInvite 1xx Responses"
                ::= { ipcsstatssipprotocol 19 }

        ipcsTotalNonInvite2xxResponses      OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of NonInvite 2xx Responses"
                ::= { ipcsstatssipprotocol 20 }

        ipcsTotalFromAndToHeaderMatchFailure    OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of From And To Header Match
Failure"
                ::= { ipcsstatssipprotocol 21 }

        ipcsTotalRegMesWithMoreContacts OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Registration Message With
More Contacts"
                ::= { ipcsstatssipprotocol 22 }

        ipcsTotalMesWithAddrIncomplete    OBJECT-TYPE
                SYNTAX                  Gauge32
```

```
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Message With Address
Incomplete"
                ::= { ipcsstatssipprotocol 23 }

        ipcsTotalAuthHeaderMatchFailure OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Auth Header Match Failure"
                ::= { ipcsstatssipprotocol 24 }

        ipcsTotalContactSrcAddrMatchFailure     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Contact Srource Addr Match
Failure"
                ::= { ipcsstatssipprotocol 25 }

        ipcsTotalViaMatchFailure    OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Via Match Failure"
                ::= { ipcsstatssipprotocol 26 }

        ipcsTotal3XXMesFromNW   OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of 3XX Message From Network"
                ::= { ipcsstatssipprotocol 27 }

        ipcsTotalOutOfDialogReferMesFromNW    OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Out Of Dialog Refer Message
From Network"
                ::= { ipcsstatssipprotocol 28 }

        ipcsTotalRegistrationMatchFailure   OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
```

```
        STATUS                  current
        DESCRIPTION             "Number of Registration Match Failure"
        ::= { ipcsstatssipprotocol 29 }

ipcsTotalContactSDPConnMatchFailure     OBJECT-TYPE
        SYNTAX                  Gauge32
        MAX-ACCESS              read-only
        STATUS                  current
        DESCRIPTION             "Number of Contact SDP Match Failure"
        ::= { ipcsstatssipprotocol 30 }

ipcsTotalSpoofedSipBye      OBJECT-TYPE
        SYNTAX                  Gauge32
        MAX-ACCESS              read-only
        STATUS                  current
        DESCRIPTION             "Number of Spoofed Sip Bye"
        ::= { ipcsstatssipprotocol 31 }

ipcsTotalSpoofedReinvite    OBJECT-TYPE
        SYNTAX                  Gauge32
        MAX-ACCESS              read-only
        STATUS                  current
        DESCRIPTION             "Number of Spoofed Reinvite"
        ::= { ipcsstatssipprotocol 32 }

ipcsTotalSpoofedCancel      OBJECT-TYPE
        SYNTAX                  Gauge32
        MAX-ACCESS              read-only
        STATUS                  current
        DESCRIPTION             "Number of Spoofed Cancel"
        ::= { ipcsstatssipprotocol 33 }

ipcsTotalSpoofedCancelToRemote  OBJECT-TYPE
        SYNTAX                  Gauge32
        MAX-ACCESS              read-only
        STATUS                  current
        DESCRIPTION             "Number of Spoofed Cancel To Remote"
        ::= { ipcsstatssipprotocol 34 }

ipcsTotalSpoofed200 OBJECT-TYPE
        SYNTAX                  Gauge32
        MAX-ACCESS              read-only
        STATUS                  current
        DESCRIPTION             "Number of Spoofed 200"
        ::= { ipcsstatssipprotocol 35 }
```

```
        ipcsTotalSpoofedErrorResp   OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Spoofed Error Response"
                ::= { ipcsstatssipprotocol 36 }

        ipcsTotalRegistrationFailed   OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Registration Failed"
                ::= { ipcsstatssipprotocol 37 }

        ipcsTotalAckMessageOutOfDialogue        OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Ack Message received out of
Dialogue"
                ::= { ipcsstatssipprotocol 38 }

        ipcsTotalByeMessageOutOfDialogue        OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Bye Message out of Dialogue"
                ::= { ipcsstatssipprotocol 39 }

        ipcsTotalCancelMessageOutOfDialogue     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Cancel Message out of
Dialogue"
                ::= { ipcsstatssipprotocol 40 }

        ipcsTotalNotifyMessageOutOfDialogue     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Notify Message received out of
Dialogue"
                ::= { ipcsstatssipprotocol 41 }

        ipcsTotal1XXMessageOutOfDialogue        OBJECT-TYPE
```

```
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of 1XX Message received out of
Dialogue"
                ::= { ipcsstatssipprotocol 42 }

        ipcsTotal2XXMessageOutOfDialogue        OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of 2XX Message received out of
Dialogue"
                ::= { ipcsstatssipprotocol 43 }

        ipcsTotal3XXMessageOutOfDialogue        OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of 3XX Message received out of
Dialogue"
                ::= { ipcsstatssipprotocol 44 }

        ipcsTotal4XXMessageOutOfDialogue        OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of 4XX Message received out of
Dialogue"
                ::= { ipcsstatssipprotocol 45 }

        ipcsTotal5XXMessageOutOfDialogue        OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of 5XX Message received out of
Dialogue"
                ::= { ipcsstatssipprotocol 46 }

        ipcsTotal6XXMessageOutOfDialogue        OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of 6XX Message received out of
Dialogue"
                ::= { ipcsstatssipprotocol 47 }
```

```
        ipcsTotalReinviteMessageOutOfDialogue    OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Reinvite Message received out
of Dialogue"
                ::= { ipcsstatssipprotocol 48 }

        ipcsTotal1XXMessageOutOfTransaction     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of 1XX Message received out of
Transaction"
                ::= { ipcsstatssipprotocol 49 }

        ipcsTotal2XXMessageOutOfTransaction     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of 2XX Message received out of
Transaction"
                ::= { ipcsstatssipprotocol 50 }

        ipcsTotal3XXMessageOutOfTransaction     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of 3XX Message received out of
Transaction"
                ::= { ipcsstatssipprotocol 51 }

        ipcsTotal4XXMessageOutOfTransaction     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of 4XX Message received out of
Transaction"
                ::= { ipcsstatssipprotocol 52 }

        ipcsTotal5XXMessageOutOfTransaction     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
```

```
                DESCRIPTION             "Number of 5XX Message received out of
Transaction"
                ::= { ipcsstatssipprotocol 53 }

        ipcsTotal6XXMessageOutOfTransaction     OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of 6XX Message received out of
Transaction"
                ::= { ipcsstatssipprotocol 54 }

        ipcsTotalCancelMessageOutOfTransaction  OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Cancel Message received out of
transaction"
                ::= { ipcsstatssipprotocol 55 }

        ipcsTotalContactMismatchBetweenRegistrationAndInviteMessage OBJECT-
TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of Contact Mismatch Between
Registration And Invite Message"
                ::= { ipcsstatssipprotocol 56 }

        ipcsTotalFailureToRoute      OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Total Number of times Failure to Route has
occurred."
                ::= { ipcsstatssipprotocol 57 }

        ipcsTotalFailureToRouteCauseDNS  OBJECT-TYPE
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of times Failure to Route has
occurred due to DNS look-up failure."
                ::= { ipcsstatssipprotocol 58 }

        ipcsTotalFailureToRouteCauseENUM        OBJECT-TYPE
```

```
                SYNTAX                  Gauge32
                MAX-ACCESS              read-only
                STATUS                  current
                DESCRIPTION             "Number of times Failure to Route has
occurred due to ENUM look-up failure."
                ::= { ipcsstatssipprotocol 59 }

END
```

This page intentionally left blank.

Error Messages F

This appendix contains a list of the E-SBC error messages.

General

Table F-1. Error Messages.

General
'The <field name> field cannot be empty.'
'Only letters, numbers, and spaces are allowed in the <field name> field.'
'Please provide a valid IP address in the <field name> field.'
'Please provide a valid IP address (with a valid port) in the <field name> field.'
'Loopback address (<ip>) is not allowed in the <field name> field.'
'Class D (multicast) and E (reserved) IP addresses are not allowed in the <field name> field.'
'Broadcast address (<ip>) is not allowed in the <field name> field.'
'Network address (<ip>) is not allowed in the <field name> field.'
'Invalid subnet provided in the <field name> field. Please correct your input.'
'Only positive integer numbers are allowed in the <field name> field.'
'Only positive real numbers are allowed in the <field name> field.'
'Only letters and numbers are allowed in the <field name> field.'
'Only letters, numbers, and underscores are allowed in the <field name> field.'
'Invalid domain name provided in the <field name> field. Please correct your input.'
'Invalid URI provided in the <field name> field. Please correct your input.'
'Only letters, numbers, and dashes are allowed in the <field name> field.'
'Please select a <radio button name>'
'Value out of range for the <field name> field.'
'Invalid time provided in the <field name> field. Proper format is hh:mm [am|pm].'
'Invalid time provided in the <field name> field. Proper format is hh:mm.'
'Invalid date provided in the <field name> field. Proper format is mm/dd/yyyy.'
'Special characters, "'*%$+<>\&, are not allowed in the <field name> field.'
'Spaces are not allowed in the <field name> field.'
'<field value> is not a valid linux filename. Please correct your input.'
'<field value> is not a valid bitfield. Please correct your input.'
'<field value> is not a valid URL. Please correct your input.'
'The provided password does not meet requirements. Please enter a password of mixed case which is eight or more characters long and contains at least one special character and one number.'
'An invalid mask has been specified in the <field name> field.'
'<field value> must be less than <field maximum>.'
'<field value> must be less than or equal to <field maximum>.'
'<field value> must be greater than <field minimum>.'
'<field value> must be greater than or equal to <field minimum>.'

'<field value> must contain a valid MAC address.'
'<field value> should start with 'SEP' followed by a 12 character MAC address or start with 'UPC' followed by 1 to 29 alphanumeric characters."
'<field value> should be 15 characters, beginning with 'SEP' or 'ATA' followed by a valid MAC address."
'Only even numbers are allowed in the <field name> field.'
'Only odd numbers are allowed in the <field name> field.'
'The <field name> field must be unique.'
'The <field name> field must be equal to the <second field name> field.'
'<field name> must be greater than or equal to the highest <second field name> in this profile.'
'Duplicate <field name> are not allowed. Please choose a new <field name>.'
'Please provide a valid domain name or subnet (in CIDR format) in the <field name> field.'
'Only letters, numbers, dashes, slashes, and spaces are allowed in the <field name> field.'
'The <field name> field must not contain the same IP as the <second field name> field.'
'<field name> and <second field name> cannot be the same."
'<field name> and <second field name> must both be empty or both must be filled in. Please correct your input.'
'Duplicate entries are not allowed. Please enter a different <field name>.'
Network Management
'All IPs on the same interface must be in the same subnet. Please correct your input.'
'<ip ##> is not in this interface's subnet. Please correct your input.'
'Duplicate Public IPs are not allowed.'
'A Public IP cannot match an IP Address if the IP Address has no associated Public IP.'
'Only up to 2 interfaces may be active at one time.'
'Interface pairs A1 & A2 or B1 & B2 may not be used.'
'Only up to 2 interfaces can be monitored at one time. Please correct your input.'
'The internal and external interfaces are the same, but the subnets are not. Please correct your input.'
'The internal and external subnets are the same, but the interfaces are not. Please correct your input.'
'<ip ##> must be unique. Please note that you will not be able to re-use an IP address until after it has been deleted or changed (and committed).'
'At least one address must be configured on both the internal and external side. You cannot delete the only <internal|external> address!'
'This address is currently being used in a Cluster Proxy. You must remove this association before deletion is allowed.'
'This IP Address is in use and can not be deleted.'
'Public IP "<value>" is already in use. Please enter another Public IP.'

Administration
'Error on Requesting Passphrase Validation'
Application Rules
'IM Log Archival must be enabled before IM Logging can be enabled. IM Log Archival can be configured via Archival Settings.'
Security Rules
'The provided URI/Domain already exists in the white list. Duplicates are not allowed.'
'One of the provided URIs/Domains is too long, please correct "<value>".'
'One of the provided URIs/Domains is invalid, please correct "<value>".'
'One of the provided URIs/Domains is a duplicate. Duplicates are not allowed, please correct "<value>".'
'Please select at least one option from the Scrubber Packages field.'
Signaling Rules
'Configuring a standard header as a proprietary header is not allowed.'
'Configuring a standard method name as a proprietary method name is not allowed.'
Time of Day Rules
'At least one <field name> must be selected for recurrence.'
'The end date cannot be before the start date. Please correct the date and/or time.'
'The start date cannot be before the current time on the server. Please correct the date and/or time.'
URI Groups
'The URI provided already exists in this group. Duplicates are not allowed.'
'One of the provided <field name> is too long, please correct "<value>".
'One of the provided <field name> is invalid, please correct "<value>".'
'One of the provided <field name> is a duplicate. Duplicates are not allowed, please correct "<value>".'
'Invalid <value> provided in the <field name> field. Please correct your input.'
SNMP Configuration
'<field name> can only contain 4 or less IPs. Please correct your input.'
'An invalid IP:Port combination has been specified. Please correct: <value>'
Secure Channel
'The Secure Channel Mapping must be unique. Please select a different combination.'
Server Config
'An invalid ip or domain has been specified. Please correct: <value>'
'At least one transport type must be supported.'
'The following IP Address / FQDN is already configured in another server profile. Please change or remove: <values>'
'<field name> must be a well formed URI or domain. No wildcards are allowed. Please check your input.'
Installer
'The last port must be greater than the first port for the <field name> field'
'Incomplete addresses are not allowed. Please correct address #<field name>.'
'Each address much be in the same subnet as the gateway. Please correct address #<field name>.'
'Duplicate addresses are not allowed. Please correct address #<field name>.'

'The DNS client must be associated with a valid address.'
'All addresses on an interface must share the same subnet. Please correct address #<field name>'
'Only two interfaces may be configured at any given time.'
'A1 + A2 is an invalid interface combination. Please use A1 + B1 or B2.'
'B1 + B2 is an invalid interface combination. Please use B1 + A1 or A2.'
'The internal and external side subnets must be the same for single wire networks.'
'The internal and external side subnets must be different for two wire networks.'
'The <field name> must be in the same subnet as the <internal|external> Gateway. Please correct: <value>'
'Addresses must be unique across the internal and external side networks. Please correct <field name> and <second field name>'
'Duplicate public IP addresses are not allowed. Please correct <field name> and <second field name>'
'An external and public IP are required to create an address. Please fill in the <field name> field.'
Interworking
'At least one regular expression must be provided for either the URI or domain.'
'At least a User or Domain action must be taken. None may not be chosen for both portions.'
Syslog Management
'Duplicate profiles are not allowed; this profile already exists for this device.'
'The EMS management IP may not be used here.'
Media Forking
'<field name> can not be a broadcast MAC address.'
'<field name> must be unique across all UC-Sec devices. This currently conflicts with <feature name>. Please correct your input.'
Media Interface
'The specified port range overlaps with an existing <feature name>. Please choose a different range.'
System Management
'The serial number you've entered is invalid.'
'The appliance name you've chosen is already in use. Please chose another name.'
'At least one device must be selected for <rollback|upgrade>.'
Relay Services
'<field name> is required if TLS is selected as a Transport. Please correct your input.'
Backup/Restore
'This SFTP Host Address is already used on another snapshot server. Please correct your input.'
' field must be a valid IP, IP:Port, or domain name.'
Routing Rules
'<field name> field must be a valid IP, IP:Port, or domain name.'
Signaling Interface
'TLS cannot be disabled while associated with a secure SIP cluster.'
'At least one TCP, UDP, or TLS port must be configured.'

'TCP Port and TLS Port must be different.'
'The specified <field name> port is already in use by an existing <feature name>. Please choose a different port.'
Packet Capture
'<value> is not a valid MAC Address.'
IM Log Config
'Please choose a Frequency.'
'Please select at least one day.'
'One or more Application Rules have IM Logging enabled. Click here to disable IM Logging in all Application Rules.'
Advanced Options
'Please enable SIV before trying to enable FINGERPRINT.'
'Please enable SIV before trying to enable DOS.'
'Please disable FINGERPRINT before trying to disable SIV.'
'Please disable DOS before trying to disable SIV.'
'This port range overlaps a <feature name>. Please correct your input.'
'One or more port ranges overlap. All port ranges must be mutually exclusive. Please correct your input.'
Touring Test
FAILURE timeout
FAILURE incorrect digits
FAILURE call disconnected by the called party
FAILURE call disconnected by calling party

This page intentionally left blank.