Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Sipera Systems UC-Sec Secure Access Proxy with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to Support Core Enterprise Users - Issue 1.1

Abstract

These Application Notes describe the procedures for configuring Sipera Systems UC-Sec Secure Access Proxy with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to support core enterprise users.

The Sipera Systems UC-Sec Secure Access Proxy is a SIP security appliance that manages and protects the flow of SIP signaling and related media across trusted and un-trusted networks. Compliance testing focused on core enterprise Avaya SIP endpoints traversing the LAN network through the Sipera UC-Sec Secure Access Proxy to the Avaya SIP infrastructure while the Sipera UC-Sec enforced Denial of Service policies.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the procedures for configuring Sipera Systems UC-Sec Secure Access Proxy with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to support core enterprise users.

The Sipera Systems UC-Sec Secure Access Proxy is a SIP security appliance that manages and protects the flow of SIP signaling and related media across trusted and un-trusted networks. Compliance testing focused on core enterprise Avaya SIP endpoints traversing the LAN network through the Sipera UC-Sec Secure Access Proxy to the Avaya SIP infrastructure while the Sipera UC-Sec enforced Denial of Service policies.

For Compliance testing, Avaya Aura® Session Manager utilized the Sipera UC-Sec appliances for the role of Secure Access Proxy. The Sipera UC-Sec appliances solution offers comprehensive, real-time UC security (including threat mitigation, policy enforcement, access control, and encryption), while simplifying internal IP phone deployments by minimizing the impact to communications and security infrastructure.

UC-Sec performs the following functions to meet the security and deployment challenges within the core enterprise network:

• **Policy Control and Demarcation** – UC-Sec serves as the demarcation point for the enterprise VoIP/UC network and data networks and enforces fine-grained security policies on a per user, domain, network or device basis.

• **Threat Mitigation** – UC-Sec detects and mitigates thousands of attacks and security threats based on the most advanced library of vulnerabilities developed from years of primary research by Sipera's industry-leading VIPER Lab.

• **Access Control** – To ensure that VoIP services are used properly by only the users and devices for which they are intended, strong authentication and access control mechanisms must be enforced.

• **Core Protection** – The UC-Sec can provide essential security for core UC assets such as VoIP servers, enforcing VLAN separation for voice and data traffic and mitigating intrusion and unauthorized access threats.

2. General Test Approach and Test Results

The general test approach was to make calls through Sipera UC-Sec while DoS polices are in place using various codec settings and exercising common and advanced PBX features. Calls were made between the enterprise core Avaya SIP endpoints registered through the Sipera UC-Sec, the local SIP, H.323, Digital, Analog phones registered directly to Session Manager and Communication Manager and PSTN users.

2.1. Interoperability Compliance Testing

The compliance testing tested interoperability between the Sipera UC-Sec and Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Calls were made between core Avaya SIP endpoints registered through the Sipera UC-Sec and SIP, H.323, Digital, Analog phones registered directly to Session Manager and Communication Manager and PSTN users. The following specific SIP telephony functions were tested in the test environment set up for the compliance test:

- Successful registration of core enterprise Avaya SIP endpoints on Session Manager through Sipera UC-Sec.
- Calls to core enterprise Avaya SIP endpoints registered through the Sipera from Avaya SIP, H.323, Digital, Analog phones registered directly to Session Manager and Communication Manager and PSTN users.
- Calls from core enterprise Avaya SIP endpoints registered through the Sipera to Avaya SIP, H.323, Digital, Analog phones registered directly to Session Manager and Communication Manager and PSTN users.
- Calls to core enterprise Avaya SIP endpoints registered through the Sipera from core enterprise Avaya SIP endpoints registered through the Sipera.
- Basic call scenarios using G.711 and G.729 codecs
- SIPPING-19 supplementary call features (including Hold, Transfer, Conference, Bridged Calls, etc.)
- Advanced call features provided via Feature Name Extensions (FNE) on Communication Manager (such as Call Forwarding, Call Park, Call Pickup, Automatic Redial, Send All Calls, etc.)
- Verified Voicemail and Message Waiting Indicator (MWI) for both Communication Manager Messaging and Avaya Modular Messaging
- Validated that the Sipera UC-Sec preserves the Layer 2 & 3 QoS values marked by the Avaya IP Telephones.

2.2. Test Results

All feature functionality, serviceability, and performance passed all test cases described in **Section 2.1**. VoIP traffic and voice features worked properly while traversing the network through the Sipera UC-Sec Secure Access Proxy.

2.3. Support

Technical support for Sipera Systems UC-Sec Secure Access Proxy:

- Phone: (866) 861-3113
- Email: support@sipera.com
- Web: http://www.sipera.com

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows several Avaya SIP endpoints registered through the Sipera UC-Sec and a combination of Avaya SIP, H.323, Digital, Analog phones registered directly to Session Manager and Communication Manager.

The private side interface of the Sipera UC-Sec is connected to the trusted corporate LAN. The Sipera UC-Sec is assigned two IP addresses for the private interfaces.

All SIP traffic for the core enterprise Avaya SIP endpoints and the enterprise Avaya SIP, H.323, Digital, Analog phones registered directly to Session Manager and Communication Manager and PSTN users flows through the Sipera UC-Sec. In this manner, the Sipera UC-Sec can protect the main site's infrastructure from any SIP-based attacks. In addition, HTTP transfers required by the core enterprise Avaya SIP endpoints to gather licensing or configuration data, also passes through the Sipera UC-Sec.

The network diagram shown in **Figure 1** illustrates the network environment used for the compliance test. The network consists of an Avaya Aura® Telephony Infrastructure including Avaya Aura® Communication Manager running on an Avaya S8300 Server with an Avaya G450 Media Gateway, an Avaya S8800 server running Avaya Aura® Session Manager, an Avaya S8800 server running Avaya Aura® System Manager, Avaya Modular Messaging, multiple Avaya 9600 Series H.323 and SIP Telephones, one Avaya 2420 Digital Telephone, one Avaya Analog Telephone and one Sipera Systems UC-Sec Secure Access Proxy. An ISDN-PRI trunk connects the media gateway to the PSTN. One computer is present in the network providing network services such as Radius, DHCP, HTTP, and TFTP.

The non-core enterprise SIP endpoints located at the corporate site are registered to Avaya Aura® Session Manager. All calls originating from Communication Manager at the corporate site and destined for the core enterprise Avaya SIP endpoints will be routed through the Avaya Aura® Session Manager to the Sipera UC-Sec, and across the IP network.

The voice communication across the network for the Avaya 9600 IP Telephones use SIP over TLS.

The core enterprise Avaya SIP endpoints register with Avaya Aura® Session Manager through the Sipera UC-Sec. These telephones use the private IP address of Sipera UC-Sec as their configured server.

The Sipera UC-Sec will forward any registration messages it receives from the core enterprise Avaya SIP endpoints to Avaya Aura® Session Manager. Thus, the Sipera UC-Sec appears to the Avaya Aura® Session Manager as a set of SIP endpoints. All calls originating from the core enterprise Avaya SIP endpoints are routed across the IP network, Sipera UC-Sec and Avaya Aura® Session Manager to Avaya Aura® Communication Manager.

All SIP telephones use the HTTP server at the main site to obtain their configuration files. SIP endpoints that registered to SM via the Sipera UC-Sec were configured with a third party certificate via the 46xxsetiings file TRUSTCERTS parameter. SIP endpoints that registered directly to SM did not have the TRUSTCERTS parameter configured The Sipera UC-Sec will perform any address translation of private IP addresses in the configuration files before sending the files to the core enterprise Avaya SIP endpoints. All SIP endpoints both local and enterprise core use the same SIP domain: ***dev4.com***.

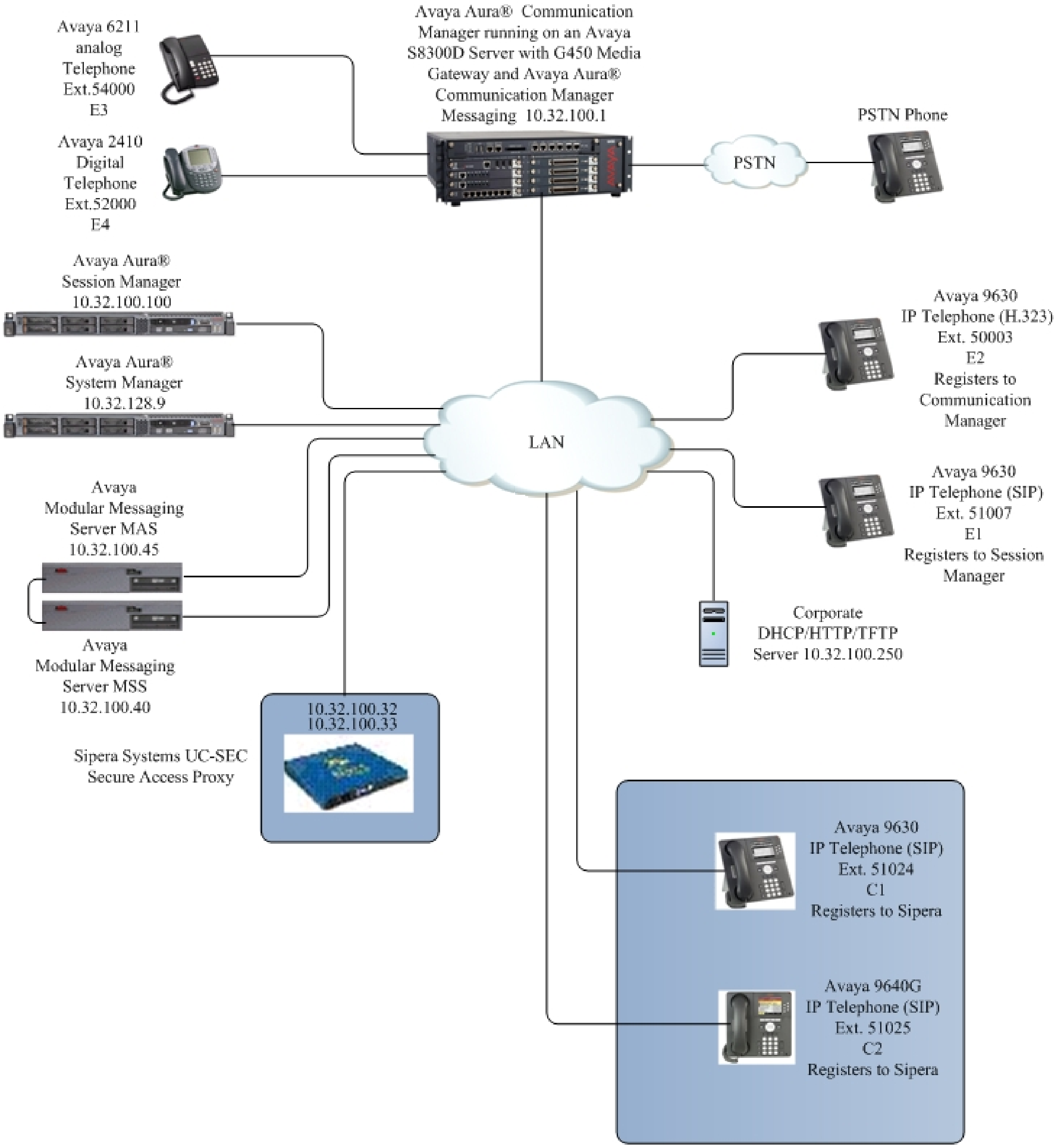

Avaya Aura® Communication Manager running on an Avaya S8300D Server with G450 Media Gateway and Avaya Aura® Communication Manager Messaging 10.32.100.1
Avaya 6211 analog Telephone Ext.54000 E3
Avaya 2410 Digital Telephone Ext.52000 E4
PSTN
PSTN Phone
Avaya Aura® Session Manager 10.32.100.100
Avaya Aura® System Manager 10.32.128.9
LAN
Avaya 9630 IP Telephone (H.323) Ext. 50003 E2 Registers to Communication Manager
Avaya 9630 IP Telephone (SIP) Ext. 51007 E1 Registers to Session Manager
Avaya Modular Messaging Server MAS 10.32.100.45
Avaya Modular Messaging Server MSS 10.32.100.40
Corporate DHCP/HTTP/TFTP Server 10.32.100.250
10.32.100.32
10.32.100.33
Sipera Systems UC-SEC Secure Access Proxy
Avaya 9630 IP Telephone (SIP) Ext. 51024 C1 Registers to Sipera
Avaya 9640G IP Telephone (SIP) Ext. 51025 C2 Registers to Sipera

Figure 1: Avaya and Sipera Enterprise Core User Solution

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

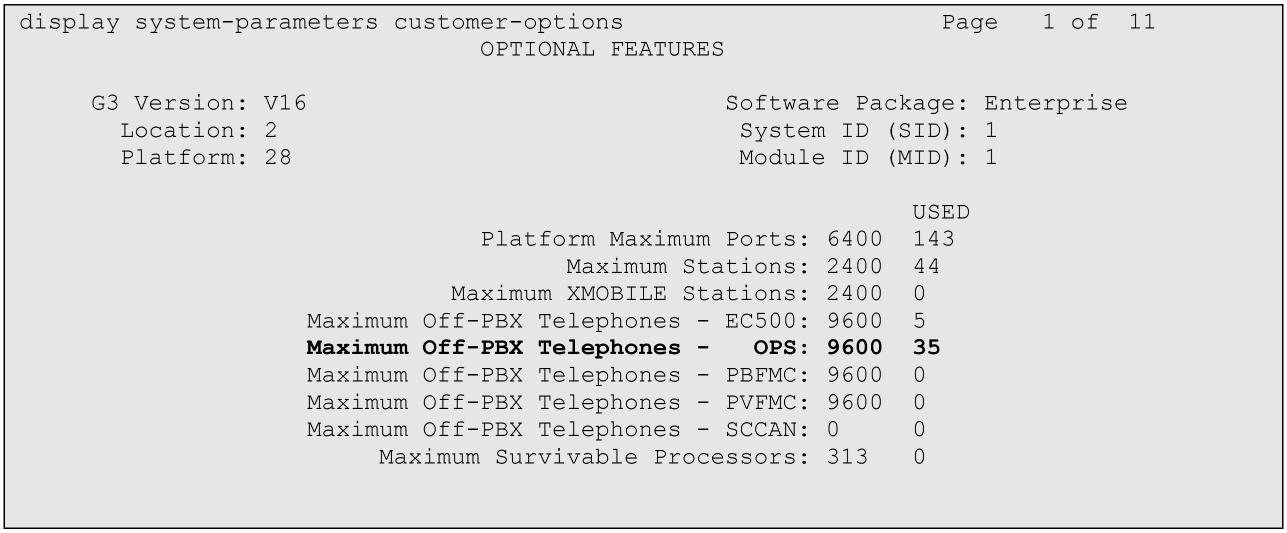
Equipment	Software/Firmware
Avaya PBX Products	
Avaya S8300 Server running Avaya Aura® Communication Manager	Avaya Aura® Communication Manager 6.0
Avaya G450 Media Gateway MGP MM712 DCP Media Module	 30 .13 .2 HW9
Avaya Aura® Session Manager	
Avaya Aura® Session Manager	6.0
Avaya Aura® System Manager	6.0
Avaya Messaging (Voice Mail) Products	
Avaya Modular Messaging - Messaging Application Server (MAS)	5.2
Avaya Modular Messaging - Message Storage Server (MSS)	5.2
Avaya Aura® Communication Manager Messaging (CMM)	6.0
Avaya Telephony Sets	
Avaya 9600 Series IP Telephones	(H.323 3.1.1) and (SIP 2.6)
Avaya 2410 Digital Telephone	5.0
Avaya Analog Telephone	NA
Sipera Systems Products	
Sipera Systems UC-Sec Secure Access Proxy	v4.0 v4.0.4 (TLS Certificate Testing)
Microsoft Products	
DHCP/HTTP/TFTP Server	Microsoft Windows 2003 Server

5. Avaya Aura® Communication Manager and Avaya Aura® Session Manager

There is no Sipera UC-Sec specific configuration required on Avaya Aura® Communication Manager and Avaya Aura® Session Manager to support this solution. It is assumed that all Aura® Telephony components, appropriate licenses and authentication files have been configured already. Trunks, dial plans, etc, will not be covered in this document. For detailed information on the installation, maintenance, and configuration of Communication Manager and Session Manager, please reference **Section 10, [1]** through **[3].** Sections 5.1 and 5.2 are supplied for reference, no configuration is required.

5.1. Verify OPS and SIP Trunk Capacity

Using the SAT, verify that the Off-PBX Telephones (OPS) and SIP Trunks features are enabled on the **Optional Features** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative. On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.



```
display system-parameters customer-options                    Page   1 of  11
                               OPTIONAL FEATURES

     G3 Version: V16                               Software Package: Enterprise
       Location: 2                                  System ID (SID): 1
       Platform: 28                                 Module ID (MID): 1

                                                                  USED
                               Platform Maximum Ports: 6400  143
                                     Maximum Stations: 2400  44
                             Maximum XMOBILE Stations: 2400  0
                   Maximum Off-PBX Telephones - EC500: 9600  5
                   Maximum Off-PBX Telephones -   OPS: 9600  35
                   Maximum Off-PBX Telephones - PBFMC: 9600  0
                   Maximum Off-PBX Telephones - PVFMC: 9600  0
                   Maximum Off-PBX Telephones - SCCAN: 0     0
                        Maximum Survivable Processors: 313   0
```

5.2. Verify QoS on Communication Manager

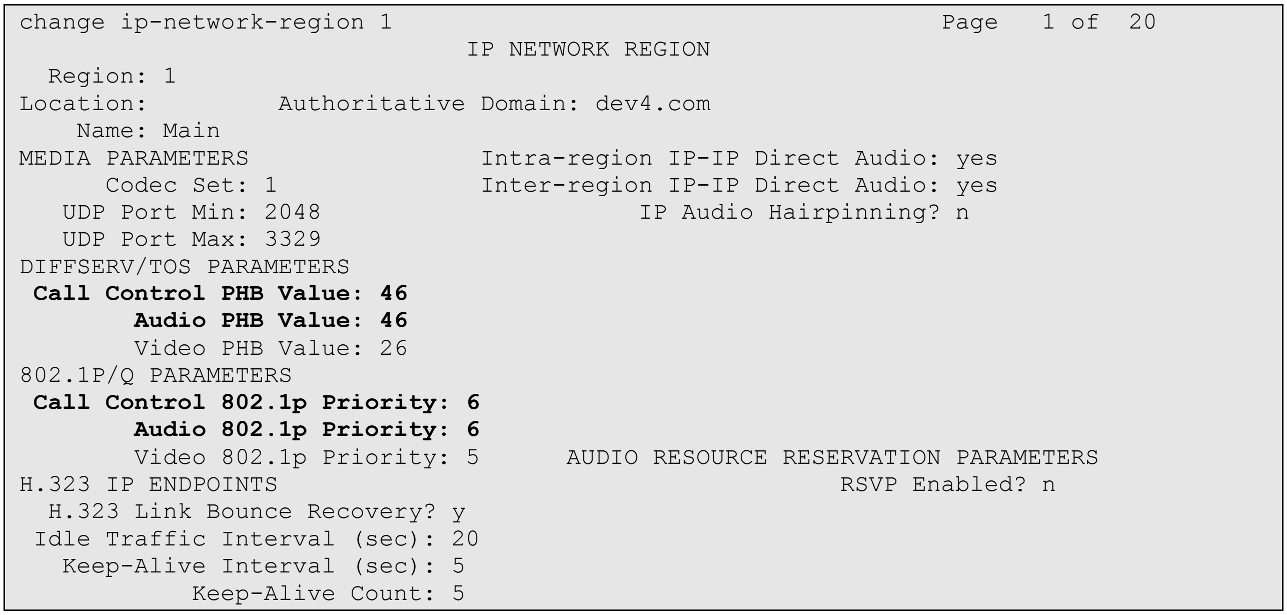
IP networks were originally designed to carry data on a best-effort delivery basis, which meant that all traffic had equal priority and an equal chance of being delivered in a timely manner. As a result, all traffic had an equal chance of being dropped when congestion occurred. QoS is now utilized to prioritize VoIP traffic and should be implemented throughout the entire network.

In order to achieve prioritization of VoIP traffic, the VoIP traffic must be classified. The Avaya Aura® telephony infrastructure supports both IEEE 802.1p and DiffServ.

The DiffServ and 802.1p/Q values configured here will be downloaded to the Avaya H.323 IP Telephones via Communication Manager. Avaya SIP IP Telephones will get QoS settings by downloading the 46xxsettings file from the HTTP server. For more information on QoS settings please refer to **Section 10.**

On **Page 1** of the **change ip-network-region** form, verify the Differentiated Services Code Points.

The Differentiated Services Code Point for **Call Control PHB Value** and **Audio PHB Value** are **46** and the **Call Control 802.1p Priority** and **Audio 802.1p Priority** are set to **6**.



```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: dev4.com
    Name: Main
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.3. Add SIP Users to Avaya Aura® Session Manager

Add SIP users corresponding to the core users shown in **Figure 1.**

This section provides the procedures for configuring SIP users on the Session Manager.

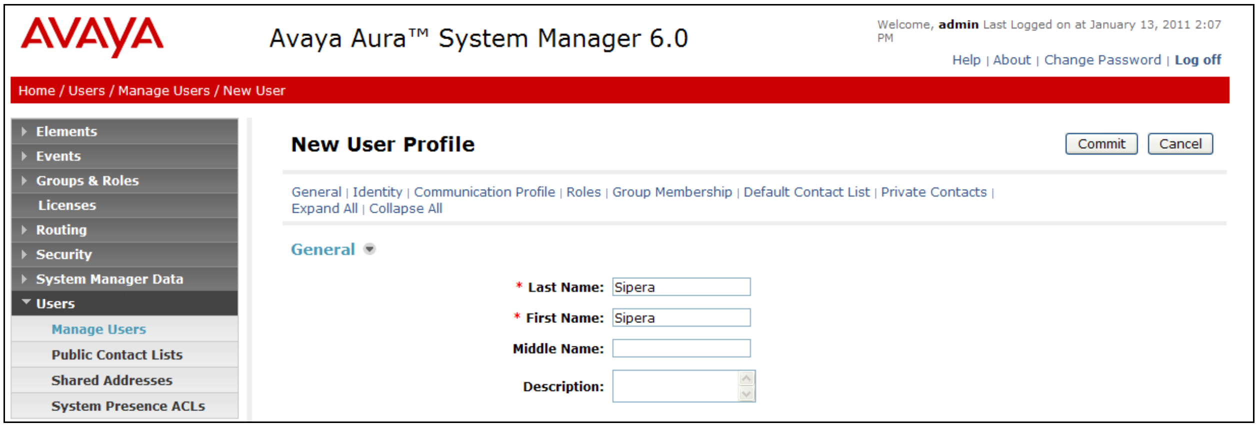
Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager using the URL "https://<*ip-address*>/SMGR", where <*ip-address*> is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.

To add new SIP users, expand **Users** and select **Manage Users** from left and select **New** button (not shown) on the right.

Enter values for the following required attributes for a new SIP user in the **General** section of the new user form.

▪ **Last Name:**	Enter the last name of the user.
▪ **First Name:**	Enter the first name of the user.

The screen below shows the information when adding a new SIP user to the sample configuration.


AVAYA
Avaya Aura™ System Manager 6.0
Welcome, admin Last Logged on at January 13, 2011 2:07 PM
Help | About | Change Password | Log off
Home / Users / Manage Users / New User
Elements
Events
Groups & Roles
Licenses
Routing
Security
System Manager Data
Users
Manage Users
Public Contact Lists
Shared Addresses
System Presence ACLs
New User Profile
Commit
Cancel
General | Identity | Communication Profile | Roles | Group Membership | Default Contact List | Private Contacts |
Expand All | Collapse All
General

* Last Name: Sipera

* First Name: Sipera

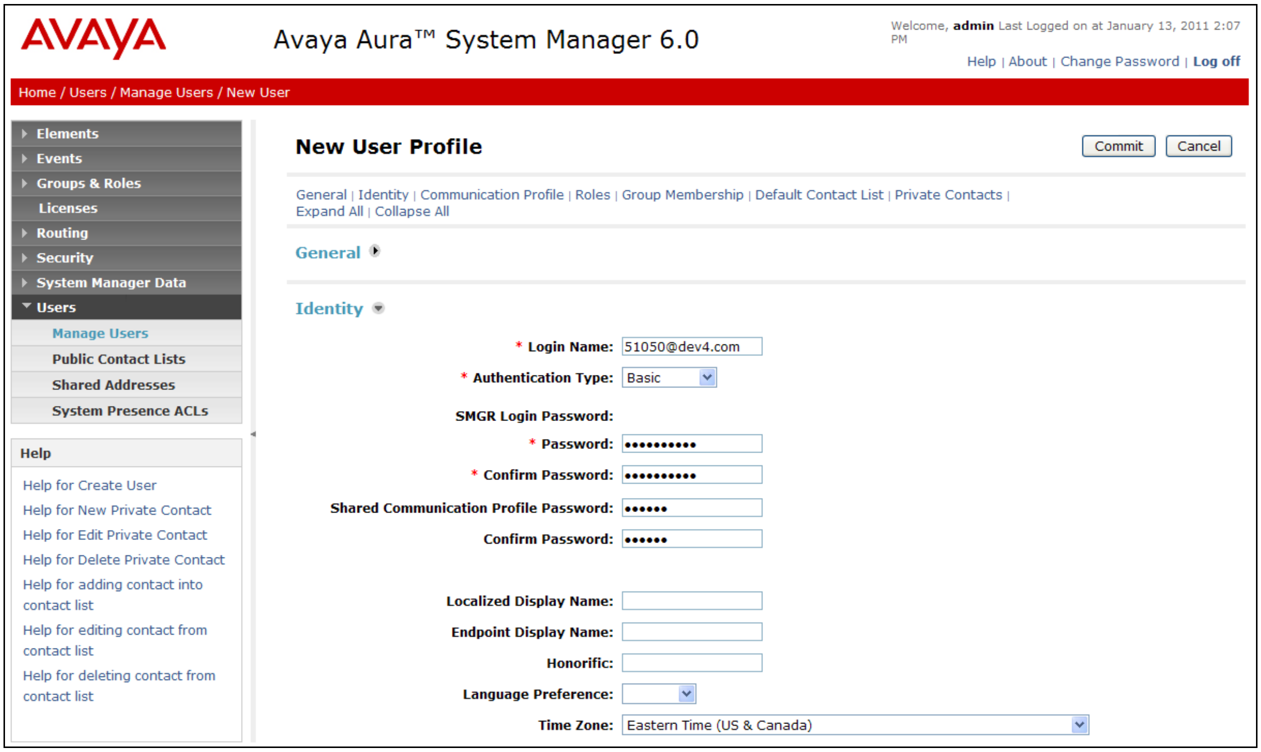
Middle Name:

Description:

Enter values for the following required attributes for a new SIP user in the **Identity** section of the new user form.

- **Login Name:** Enter <*extension*>@<*sip domain*> of the user (e.g., 51050@dev4.com).
- **Authentication Type:** Select *Basic*.
- **SMGR Login Password:** Enter the password which will be used to log into System Manager.
- **Confirm Password:** Re-enter the password from above.
- **Shared Communication Profile Password:** Enter the password that will be used by the SIP phone to log into Session Manager.
- **Confirm Password:** Re-enter the password from above.

The screen below shows the information when adding a new SIP user to the sample configuration.


AVAYA
Avaya Aura™ System Manager 6.0
Welcome, admin Last Logged on at January 13, 2011 2:07 PM
Help | About | Change Password | Log off
Home / Users / Manage Users / New User
Elements
Events
Groups & Roles
Licenses
Routing
Security
System Manager Data
Users
Manage Users
Public Contact Lists
Shared Addresses
System Presence ACLs
Help
Help for Create User
Help for New Private Contact
Help for Edit Private Contact
Help for Delete Private Contact
Help for adding contact into contact list
Help for editing contact from contact list
Help for deleting contact from contact list
Commit
Cancel
General | Identity | Communication Profile | Roles | Group Membership | Default Contact List | Private Contacts |
Expand All | Collapse All

New User Profile

General

Identity

* Login Name:	51050@dev4.com
* Authentication Type:	Basic
SMGR Login Password:	
* Password:	••••••••••
* Confirm Password:	••••••••••
Shared Communication Profile Password:	••••••
Confirm Password:	••••••
Localized Display Name:	
Endpoint Display Name:	
Honorific:	
Language Preference:	
Time Zone:	Eastern Time (US & Canada)

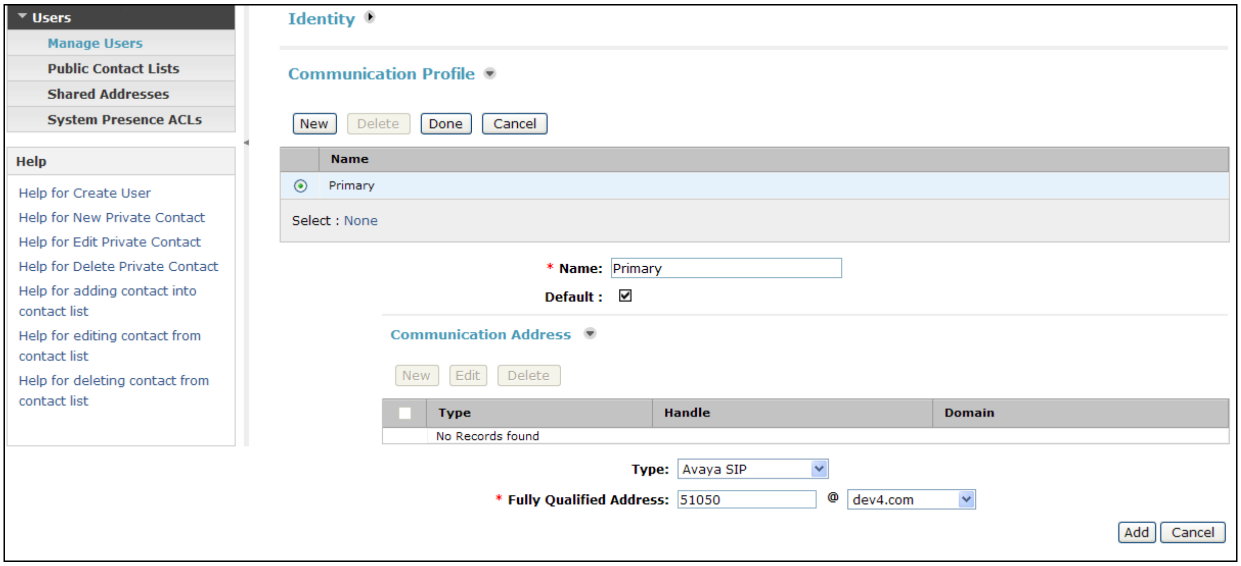
Scroll down to the **Communication Profile** section and select **New** to define a **Communication Profile** for the new SIP user. Enter values for the following required fields:

- **Name:** Enter name of communication profile.
- **Default:** Select field to indicate that this is the default profile.

Click **New** to define a **Communication Address** for the new SIP user. Enter values for the following required fields:

- **Type:** Select *Avaya SIP*.
- **Fully Qualified Address:** Enter extension number and select SIP domain.

The screen below shows the information when adding a new SIP user to the sample configuration. Click **Add**.


Users
Manage Users
Public Contact Lists
Shared Addresses
System Presence ACLs
Help
Help for Create User
Help for New Private Contact
Help for Edit Private Contact
Help for Delete Private Contact
Help for adding contact into contact list
Help for editing contact from contact list
Help for deleting contact from contact list
Identity
Communication Profile
New
Delete
Done
Cancel

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

Communication Address
New
Edit
Delete

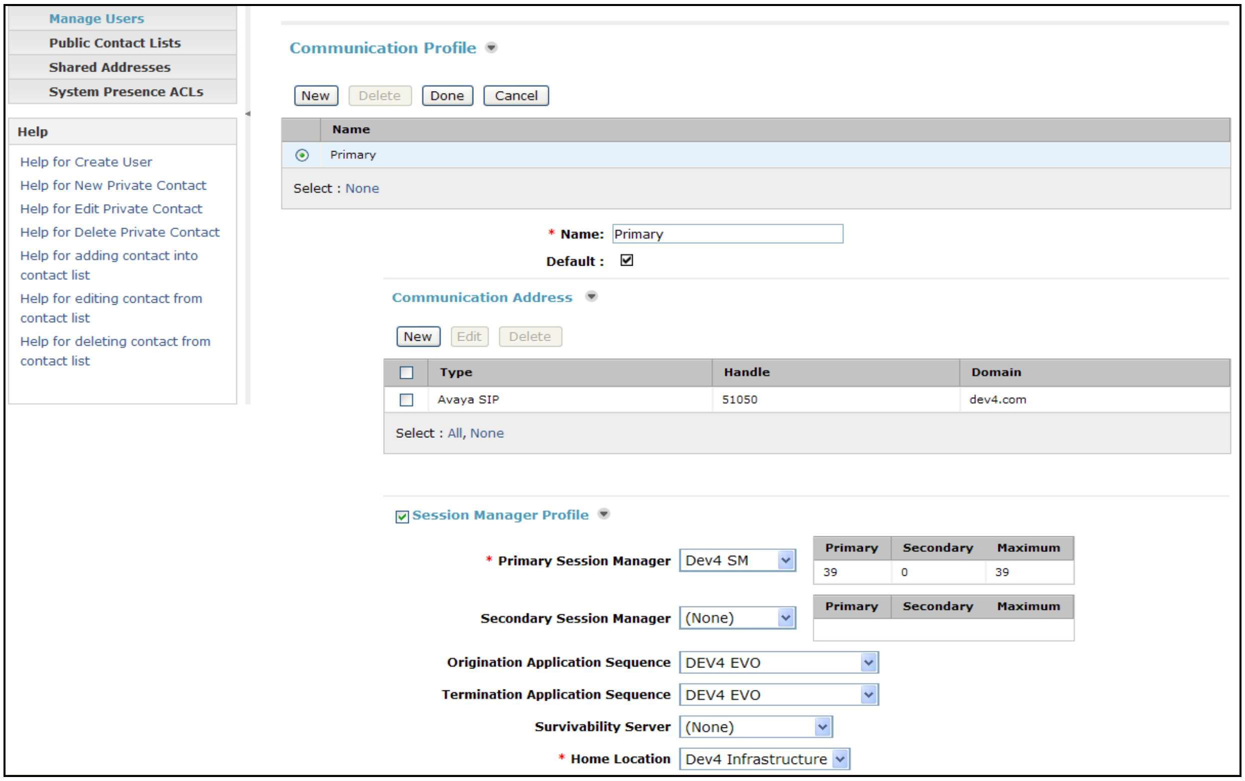
□	Type	Handle	Domain
	No Records found		

Type: Avaya SIP

* Fully Qualified Address: 51050 @ dev4.com

In the *Session Manager* section, configure the following:

- **Primary Session Manager:** Dev4 SM was used for testing
- **Origination Application Sequence:** DEV4 EVO was used for testing
- **Termination Application Sequence:** DEV4 EVO was used for testing
- **Home Location:** Dev4 Infrastructure was used for testing


Manage Users
Public Contact Lists
Shared Addresses
System Presence ACLs
Help
Help for Create User
Help for New Private Contact
Help for Edit Private Contact
Help for Delete Private Contact
Help for adding contact into contact list
Help for editing contact from contact list
Help for deleting contact from contact list
Communication Profile
New
Delete
Done
Cancel

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

Communication Address
New
Edit
Delete

□	Type	Handle	Domain
□	Avaya SIP	51050	dev4.com

Select : All, None

☑ Session Manager Profile

* Primary Session Manager: Dev4 SM

Primary	Secondary	Maximum
39	0	39

Secondary Session Manager: (None)

Primary	Secondary	Maximum

Origination Application Sequence: DEV4 EVO

Termination Application Sequence: DEV4 EVO

Survivability Server: (None)

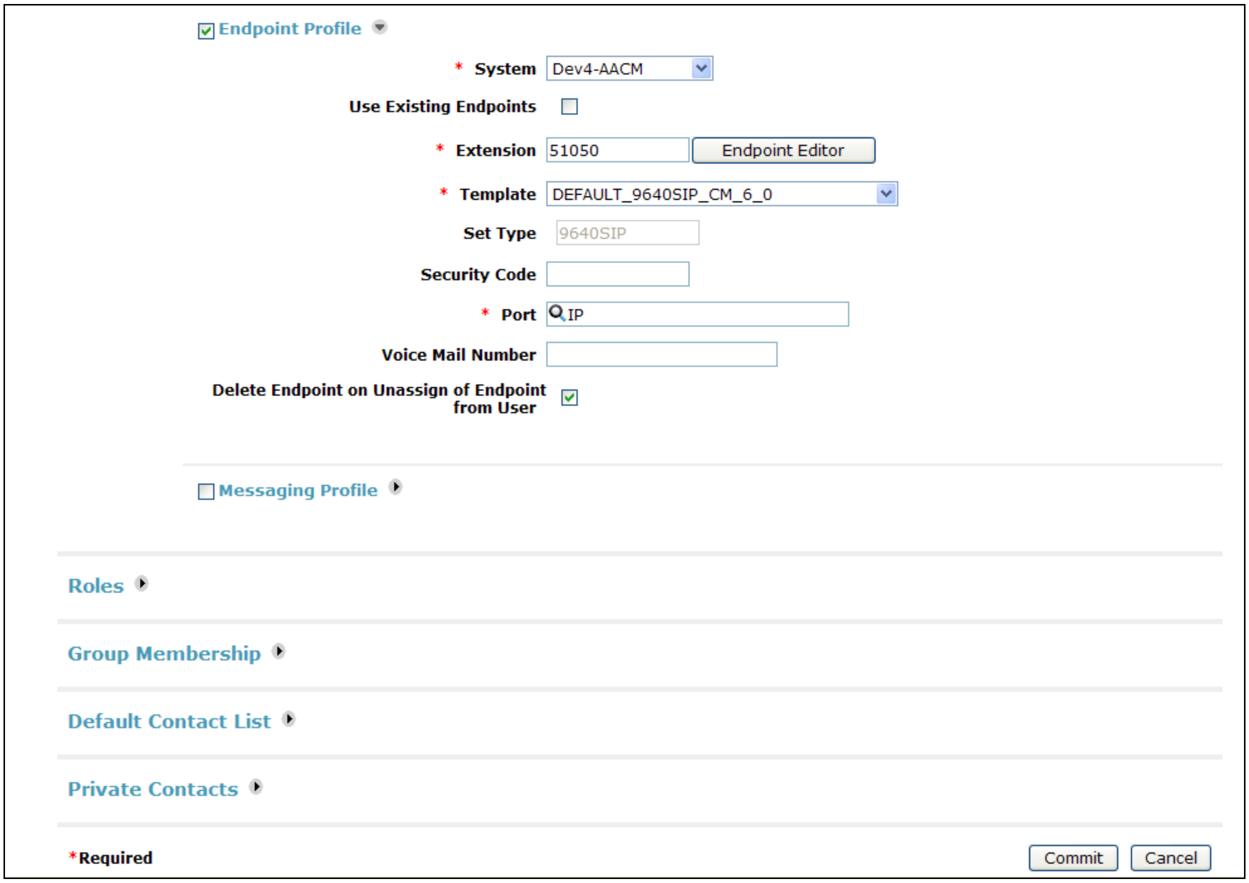
* Home Location: Dev4 Infrastructure

In the **Endpoint Profile** section, fill in the following fields:

- **System:** Select the managed element corresponding to Communication Manager.
- **Use Existing Endpoints:** If field is not selected, the station will automatically be added in Communication Manager.
- **Extension:** Enter extension number of SIP user.
- **Template:** Select template for type of SIP phone.
- **Port:** Enter *IP*.
- **Delete Endpoint on Unassign of Endpoint:** Enable field to automatically delete station when **Station Profile** is un-assigned from user.

Select **Commit** to complete the SIP user configuration. Repeat **Section 5.3** for each desired SIP user.

The screen below shows the information when adding a new SIP user to the sample configuration.



☑ Endpoint Profile

* System Dev4-AACM

Use Existing Endpoints □

* Extension 51050

* Template DEFAULT_9640SIP_CM_6_0

Set Type 9640SIP

Security Code

* Port IP

Voice Mail Number

Delete Endpoint on Unassign of Endpoint from User ☑

□ Messaging Profile

6. Configure the Avaya SIP Telephones

The Avaya IP SIP telephones at the main site will register to Avaya Aura® Session Manager. The Avaya IP SIP telephones of the enterprise core users will use the IP address of Sipera UC-Sec as the SIP server.

The tables below shows an example of the SIP telephone network settings for both the main site and the core users. For complete details on configuring a specific endpoint type, refer to **Section 10**. The Avaya SIP endpoints that directly register to the Avaya SM and to Avaya SM via the Sipera UC-Sec use different 46xxsetiings files. The 46xxsetiings file used for SIP endpoints registered to Avaya SM via the Sipera UC-Sec use the TRUSTCERTS parameter to download the third party certificate to the Avaya SIP endpoints.

Avaya IP Telephones at Main Sit

	Main Site (9600 SIP)	**Main Site (9600 H.323)**
Extension	51007	50003
IP Address	10.32.75.100	10.32.75.101
Subnet Mask	255.255.255.0	255.255.255.0
SIP/H.323 Server	10.32.100.100	10.32.100.1
Router	10.32.75.254	10.32.75.254
File Server	10.32.100.250	10.32.100.250

Enterprise Core Avaya IP Telephones

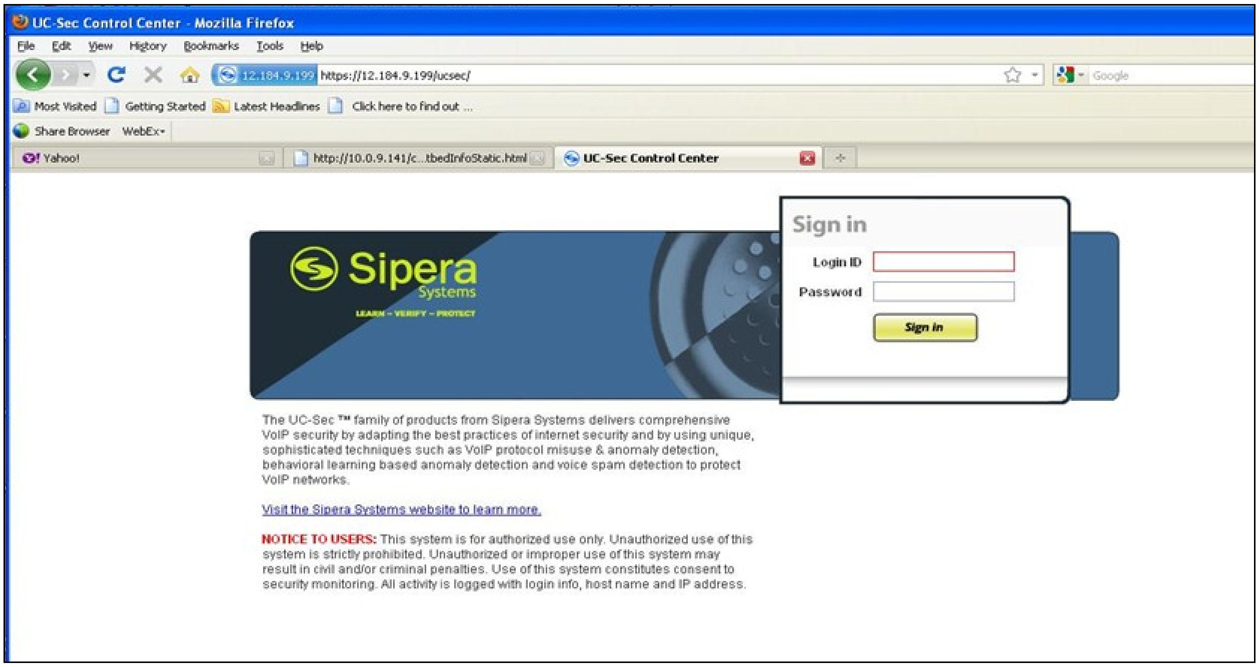
	Enterprise Core C1 (9600 SIP)	**Enterprise Core C2 (9600 SIP)**
Extension	51024	51025
IP Address	10.32.75.105	10.32.75.106
Subnet Mask	255.255.255.0	255.255.255.0
Call Server	10.32.100.32	10.32.100.32
Router	10.32.75.254	10.32.75.254
File Server	10.32.100.32	10.32.100.32

7. Configure Sipera UC-Sec Secure Access Proxy

This section covers the configuration of the Sipera UC-Sec. It is assumed that the UC-Sec software has already been installed. For additional information on these configuration tasks, refer to **Section 10, [9]** and **[10].**

Step 1: Use a WEB browser to access the UC-Sec web interface, enter https://<ip-addr>/ucsec in the address field of the web browser, where <ip-addr> is the management LAN IP address of UC-Sec.

Log in with the appropriate credentials. Click **Sign In.**

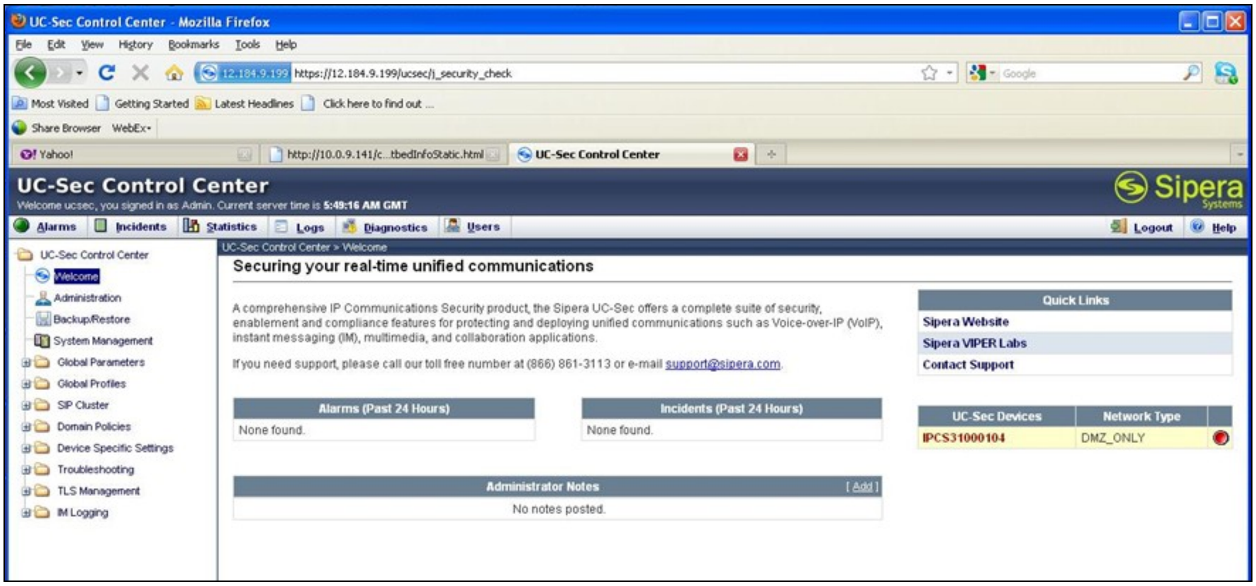

UC-Sec Control Center - Mozilla Firefox
File Edit View History Bookmarks Tools Help
12.184.9.199 https://12.184.9.199/ucsec/
Google
Most Visited Getting Started Latest Headlines Click here to find out ...
Share Browser WebEx
Yahoo!
http://10.0.9.141/c...tbedInfoStatic.html
UC-Sec Control Center
Sipera Systems
LEARN – VERIFY – PROTECT
Sign in
Login ID
Password
Sign in

The UC-Sec ™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

Visit the Sipera Systems website to learn more.

NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

Step 2: The main page of the UC-Sec Control Center will appear.


UC-Sec Control Center - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://12.184.9.199/ucsec/j_security_check
Most Visited Getting Started Latest Headlines Click here to find out ...
Share Browser WebEx
Yahoo!
http://10.0.9.141/c...tbedInfoStatic.html
UC-Sec Control Center
Alarms Incidents Statistics Logs Diagnostics Users
Logout Help
UC-Sec Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
Device Specific Settings
Troubleshooting
TLS Management
IM Logging
Sipera Systems

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 5:49:16 AM GMT

UC-Sec Control Center > Welcome

Securing your real-time unified communications

A comprehensive IP Communications Security product, the Sipera UC-Sec offers a complete suite of security, enablement and compliance features for protecting and deploying unified communications such as Voice-over-IP (VoIP), instant messaging (IM), multimedia, and collaboration applications.

If you need support, please call our toll free number at (866) 861-3113 or e-mail support@sipera.com.

Quick Links
Sipera Website
Sipera VIPER Labs
Contact Support

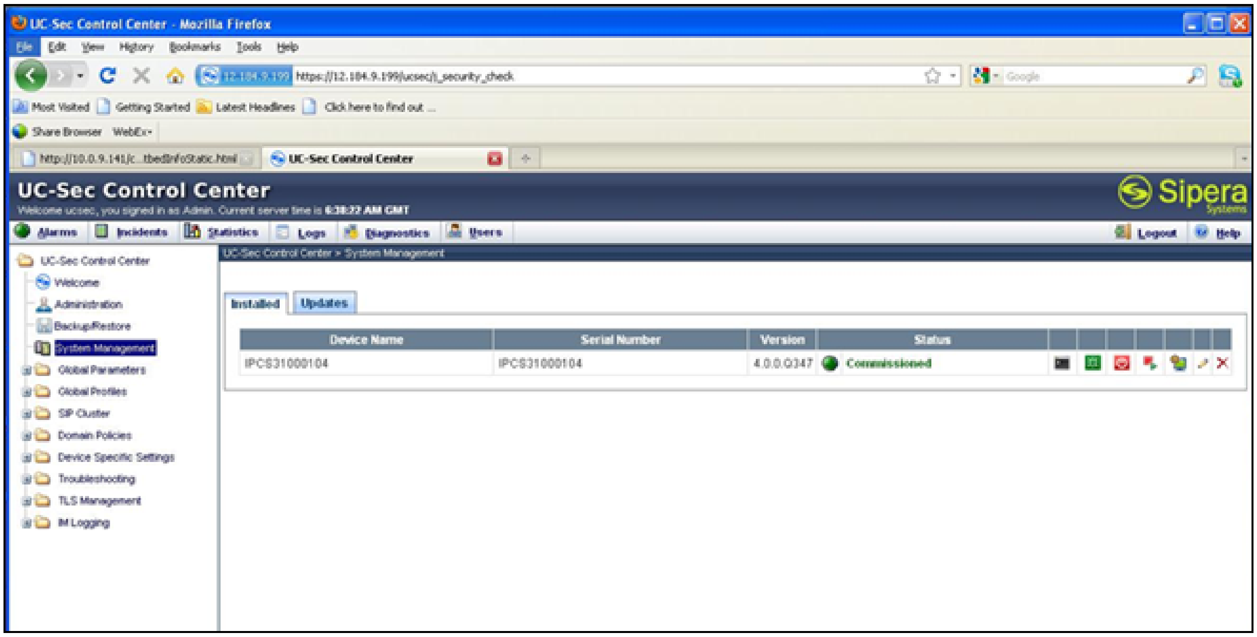
Alarms (Past 24 Hours)
None found.

Incidents (Past 24 Hours)
None found.

UC-Sec Devices	Network Type	
IPCS31000104	DMZ_ONLY	●

Administrator Notes [Add]
No notes posted.

Step 3: To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the compliance test, a single device named **IPCS310** is shown. To view the configuration of this device, click the monitor icon (the third icon from the right for the **IPCS310** device entry).


UC-Sec Control Center - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://12.184.9.199/ucsec/j_security_check
Most Visited Getting Started Latest Headlines Click here to find out ...
Share Browser WebEx
http://10.0.9.141/c...tbedInfoStatic.html
UC-Sec Control Center
Alarms Incidents Statistics Logs Diagnostics Users
Logout Help
UC-Sec Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
Device Specific Settings
Troubleshooting
TLS Management
IM Logging
Sipera Systems
Installed
Updates

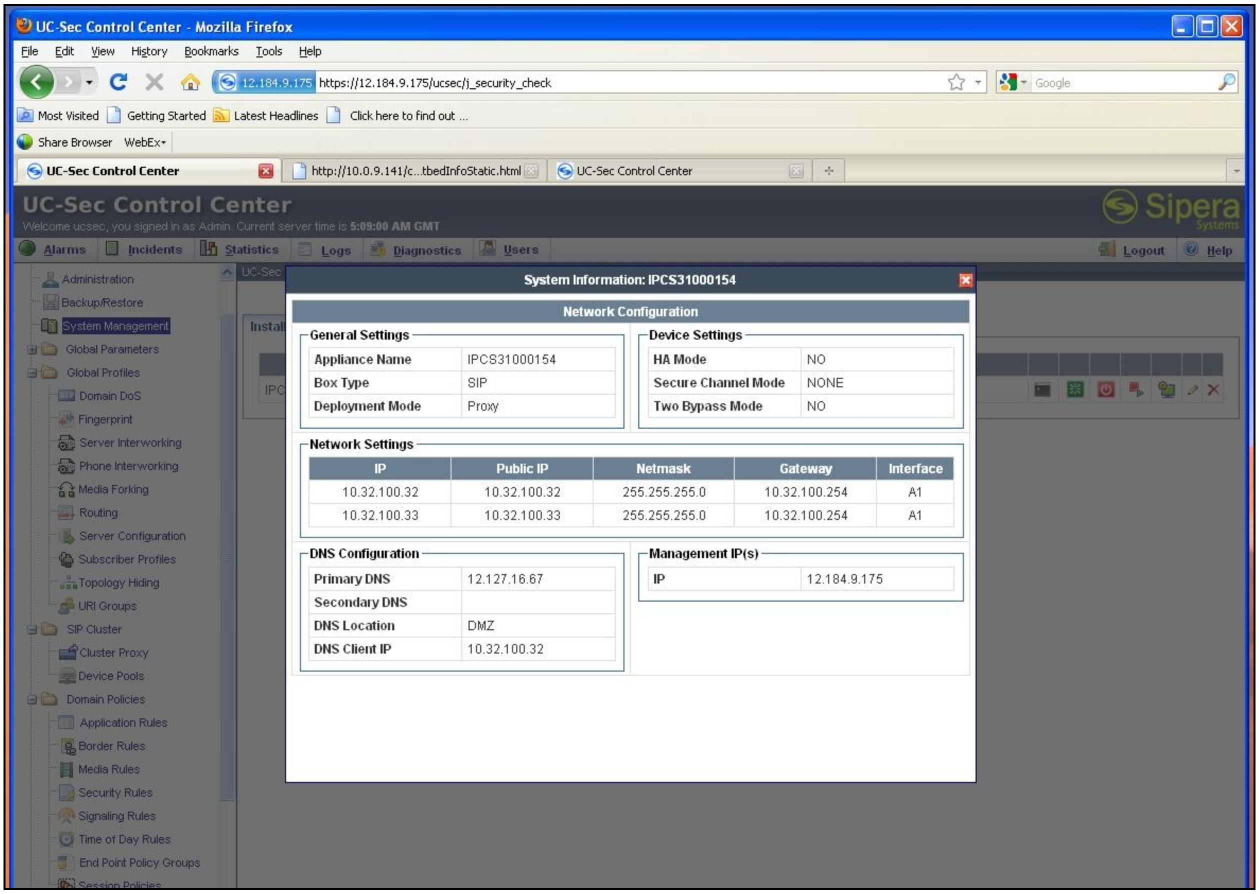
UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 6:38:22 AM GMT

UC-Sec Control Center > System Management

Device Name	Serial Number	Version	Status
IPCS31000104	IPCS31000104	4.0.0.Q347	● Commissioned

Step 4: The **System Information** screen shows the **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The compliance test did not use a DNS server, but an entry was required by UC-Sec. An arbitrary IP address was used for the **Primary DNS** field. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.



System Information: IPCS31000154

Network Configuration

General Settings

Appliance Name	IPCS31000154
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	NO
Secure Channel Mode	NONE
Two Bypass Mode	NO

Network Settings

IP	Public IP	Netmask	Gateway	Interface
10.32.100.32	10.32.100.32	255.255.255.0	10.32.100.254	A1
10.32.100.33	10.32.100.33	255.255.255.0	10.32.100.254	A1

DNS Configuration

Primary DNS	12.127.16.67
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.32.100.32

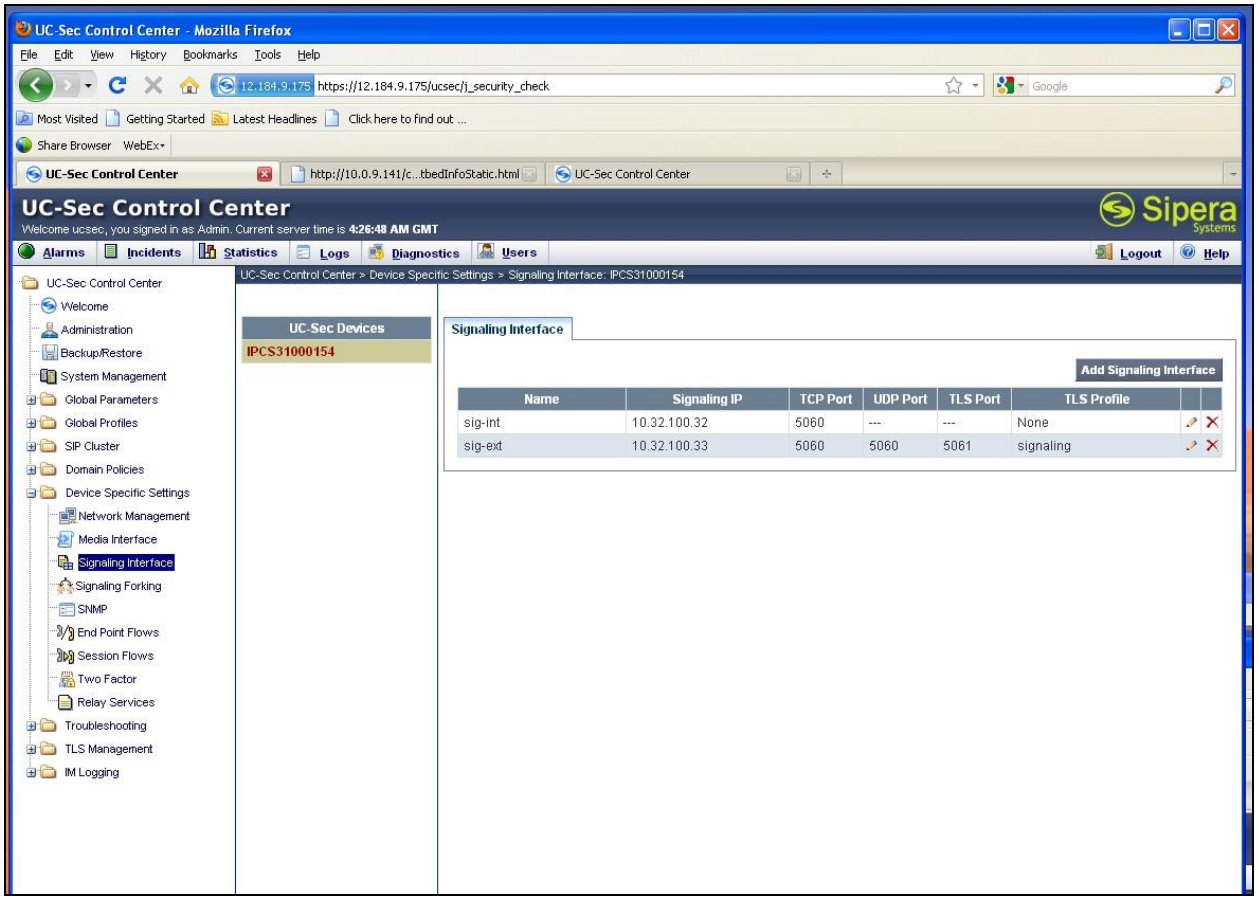
Management IP(s)

IP	12.184.9.175

Step 5: Signaling Interface
A signaling interface is created that maps a signaling interface name to an IP address and a set of ports and transport protocols that can be used on that interface.

To define a new signaling interface, navigate to **UC-Sec Control Center → Device Specific Settings → Signaling Interface**. Select the UC-Sec device name from the middle pane. Select the **Add Signaling Interface** button in the right pane. A new page is opened (not shown) where the new information can be entered and submitted.

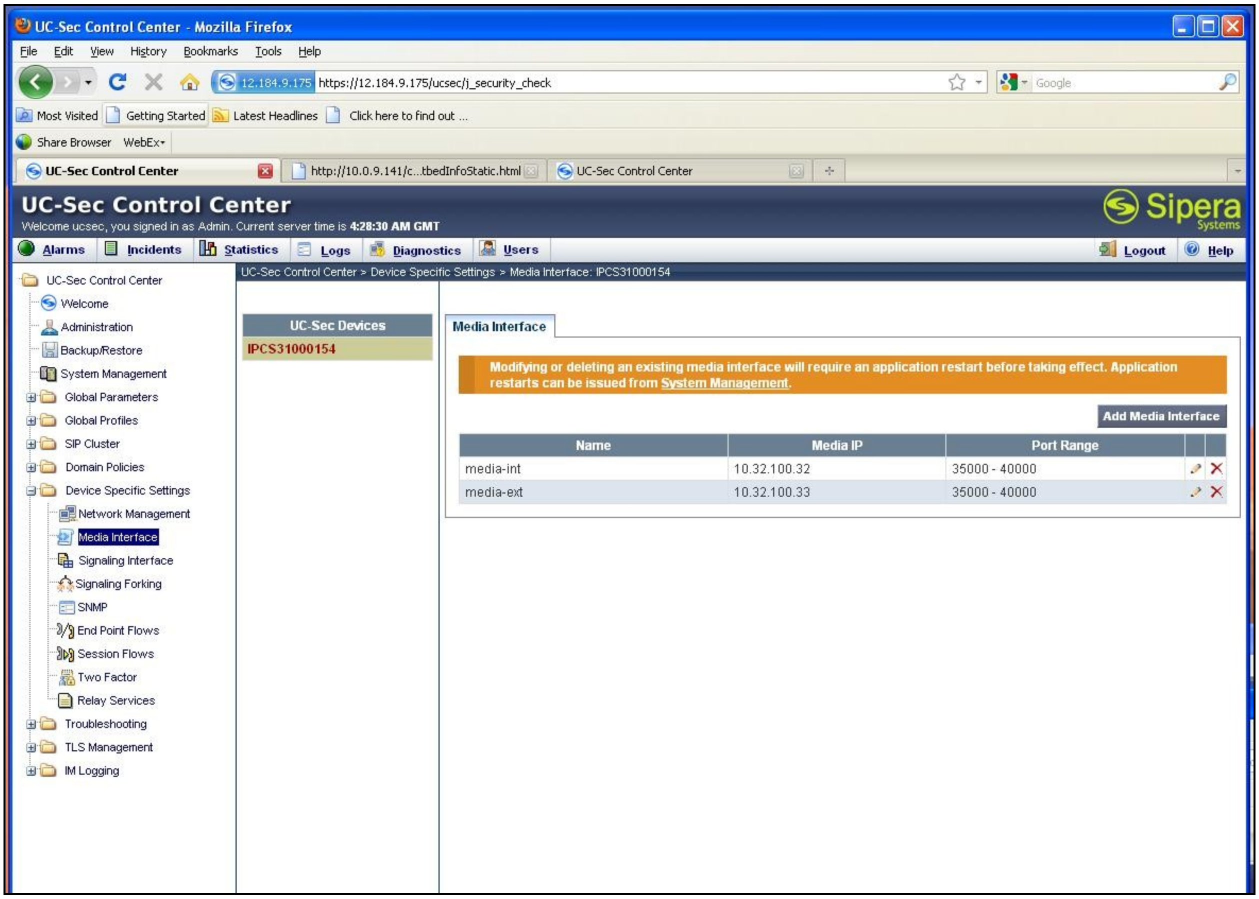
The example below shows the two interfaces created for the compliance test, one for each of the IP addresses assigned to UC-Sec. The interface named **sig-ext** supports TLS, which was used with the Avaya telephones. **Sig-int** interface supports TCP, which was used for Session Manager.



Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
sig-int	10.32.100.32	5060	---	---	None
sig-ext	10.32.100.33	5060	5060	5061	signaling

Step 6: Media Interface

A media interface maps a media interface name to an IP address and a range of ports that can be used on that interface. Navigate to **UC-Sec Control Center → Device Specific Settings → Media Interface**. The settings used by the compliance test are shown below.



Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

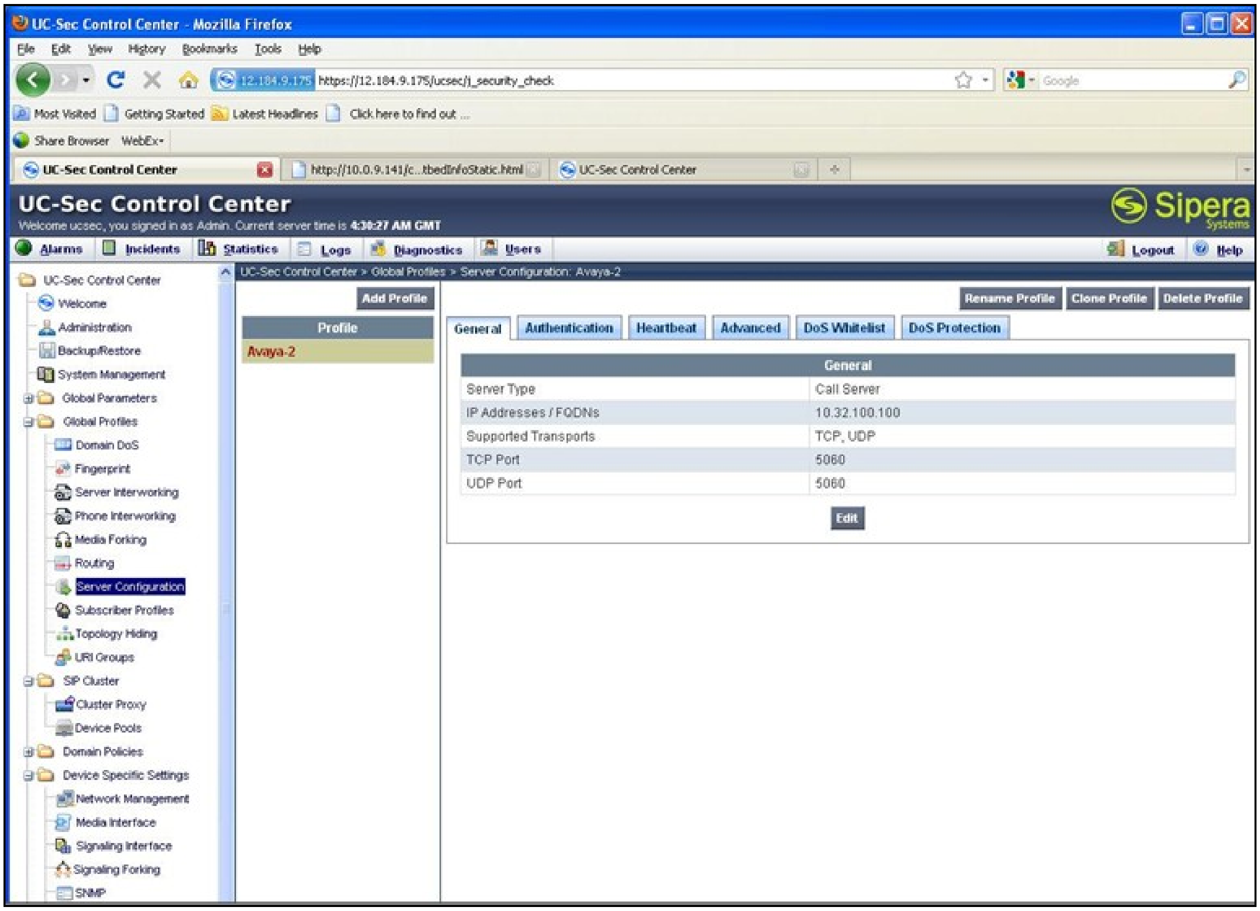
Name	Media IP	Port Range
media-int	10.32.100.32	35000 - 40000
media-ext	10.32.100.33	35000 - 40000

Step 7: Server Definition – General

A server configuration profile is created to define the characteristics of the Session Manager 6.0 to which the UC-Sec will communicate.

To define a new server configuration profile, navigate to **UC-Sec Control Center → Global Profiles → Server Configuration**. Select the **Add Profile** button in the middle pane to enter and submit the new information.

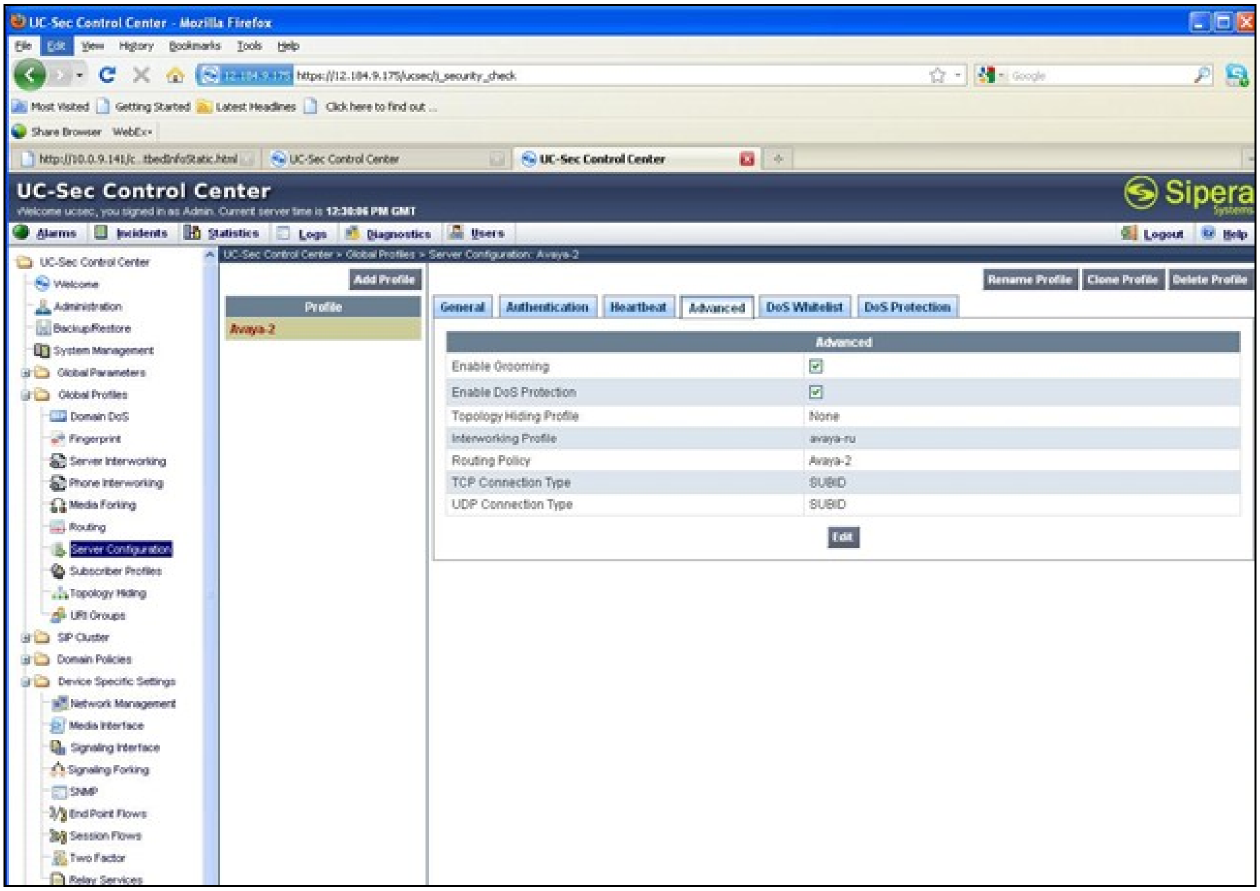
The example below shows the server configuration profile named A**vaya-2,** which was used for the compliance test. The General tab shows the **Server Type** as **Call Server** and the IP of the Session Manager SIP signaling interface (**10.32.100.100**) in the **IP Addresses/FQDNs** field. The remaining fields show the transport protocols and ports supported for traffic between UC-Sec and Session Manager.



General	
Server Type	Call Server
IP Addresses / FQDNs	10.32.100.100
Supported Transports	TCP, UDP
TCP Port	5060
UDP Port	5060

Step 8: Server Definition – Advanced

On the **Advanced** tab, profiles are specified that will be applied to traffic between the UC-Sec and this server (Session Manager). The **Interworking** profiles are applied to traffic from the UC-Sec ***to*** the server and the **Routing** profile is applied to traffic to the UC-Sec ***from*** the server. These profiles: **Interworking** and **Routing** are described in **Steps 9-10**. Grooming is also activated since Session Manager only supports up to 6 TCP connections from different ports from the same IP address.



UC-Sec Control Center > Global Profiles > Server Configuration: Avaya-2

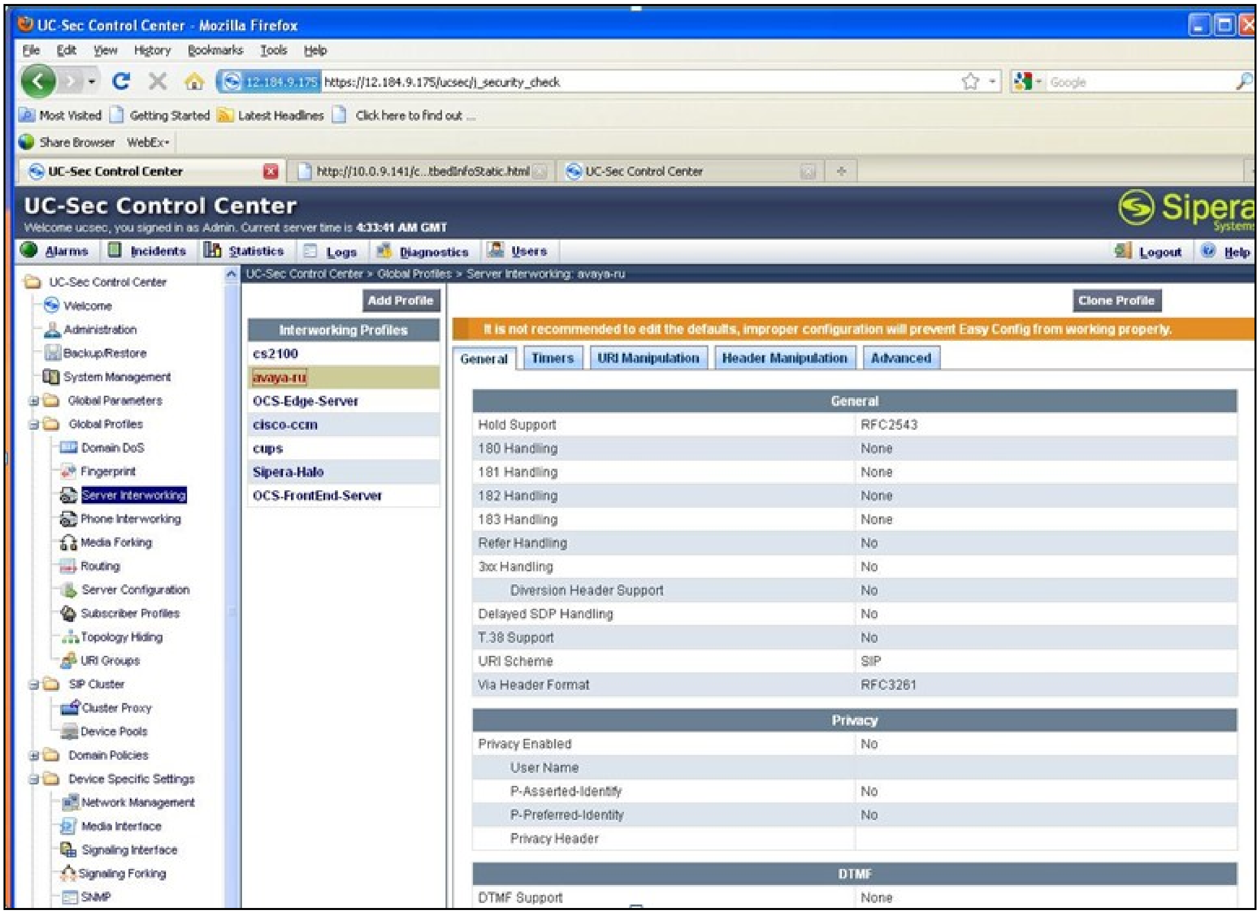
Advanced	
Enable Grooming	☑
Enable DoS Protection	☑
Topology Hiding Profile	None
Interworking Profile	avaya-ru
Routing Policy	Avaya-2
TCP Connection Type	SUBID
UDP Connection Type	SUBID

Step 9: Server – Interworking Profile

Server Interworking profile defines how SIP message headers and content (other than the IP addresses) may be manipulated for interoperability with different call servers.

To define a new interworking profile, navigate to **UC-Sec Control Center → Global Profiles → Server Interworking**. Select the **Add Profile** button in the middle pane to enter and submit the new information.

In the example below, multiple profiles are shown in the middle pane. Only the profile named **avaya-ru** was used for the compliance test. By highlighting this profile in the middle pane, its details are shown in the right pane. On the **Advanced** tab, **Hold Support** was changed to RFC2543 for interworking with the gateway used for testing with Analog and Digital phone. Default values were used for all other fields.



It is not recommended to edit the defaults, improper configuration will prevent Easy Config from working properly.

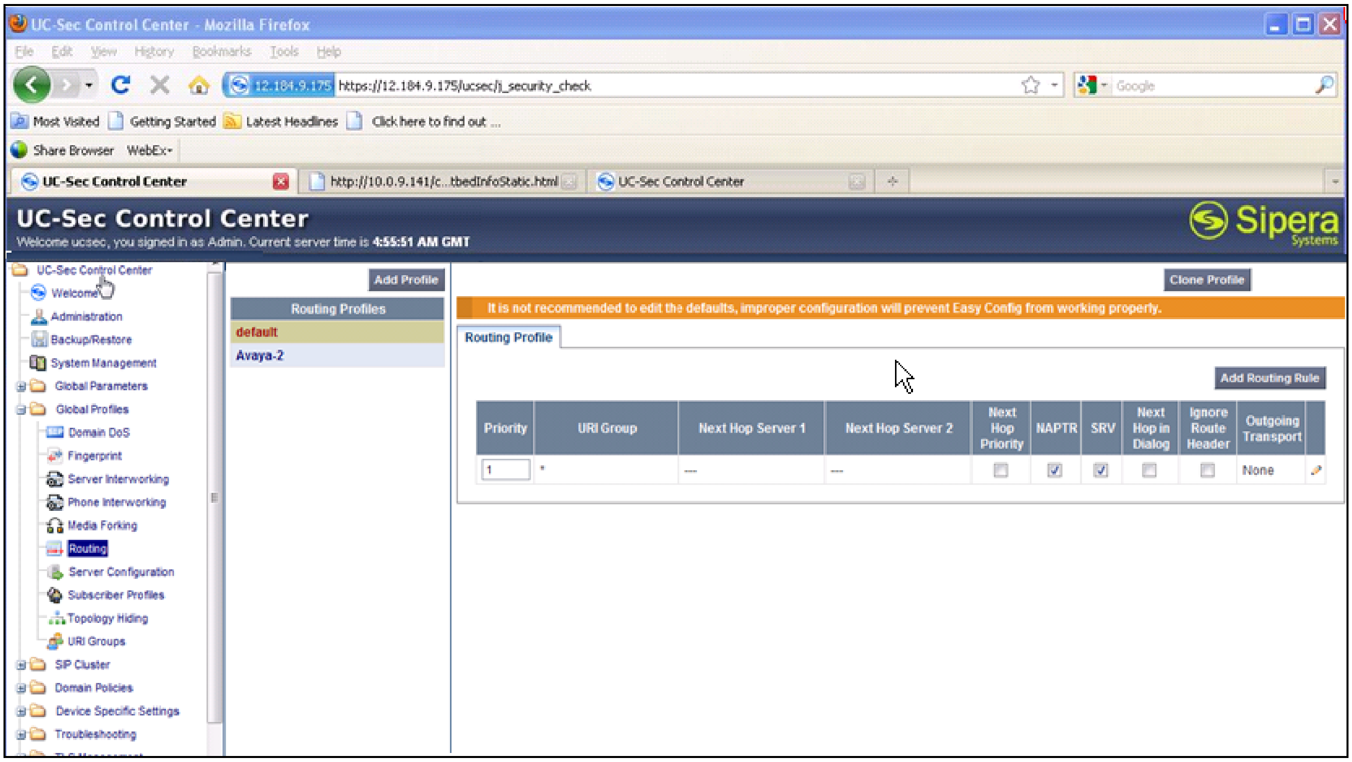
General	
Hold Support	RFC2543
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identify	No
P-Preferred-Identify	No
Privacy Header	
DTMF	
DTMF Support	None

Step 10: Server – Routing Profile

A routing profile defines how a call is to be routed. In this case, the routing profile is applied to calls from the server to UC-Sec.

To define a new routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing**. Select the **Add Profile** button in the middle pane to enter and submit the new information.

In the example below, two profiles are shown in the middle pane. Only the profiles named **default** and **Avaya-2** were used for the compliance test. By highlighting a profile in the middle pane, its details are shown in the right pane. The **Avaya-2** routing profile is described in **Step 17**. The **default** profile is shown below. The **default** profile is for routing traffic from the server destined for one of the remote endpoints. Thus, the routing profile is for all URI Groups (**URI Group** = *****) and no server IP address is specified in **Next Hop Server 1** or **Next Hop Server 2** fields. To locate the destination address, the UC-Sec will use its internal database to identify the IP address associated with the destination extension in the SIP message.



UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 4:55:51 AM GMT

Routing Profiles

- default
- Avaya-2

It is not recommended to edit the defaults, improper configuration will prevent Easy Config from working properly.

Routing Profile

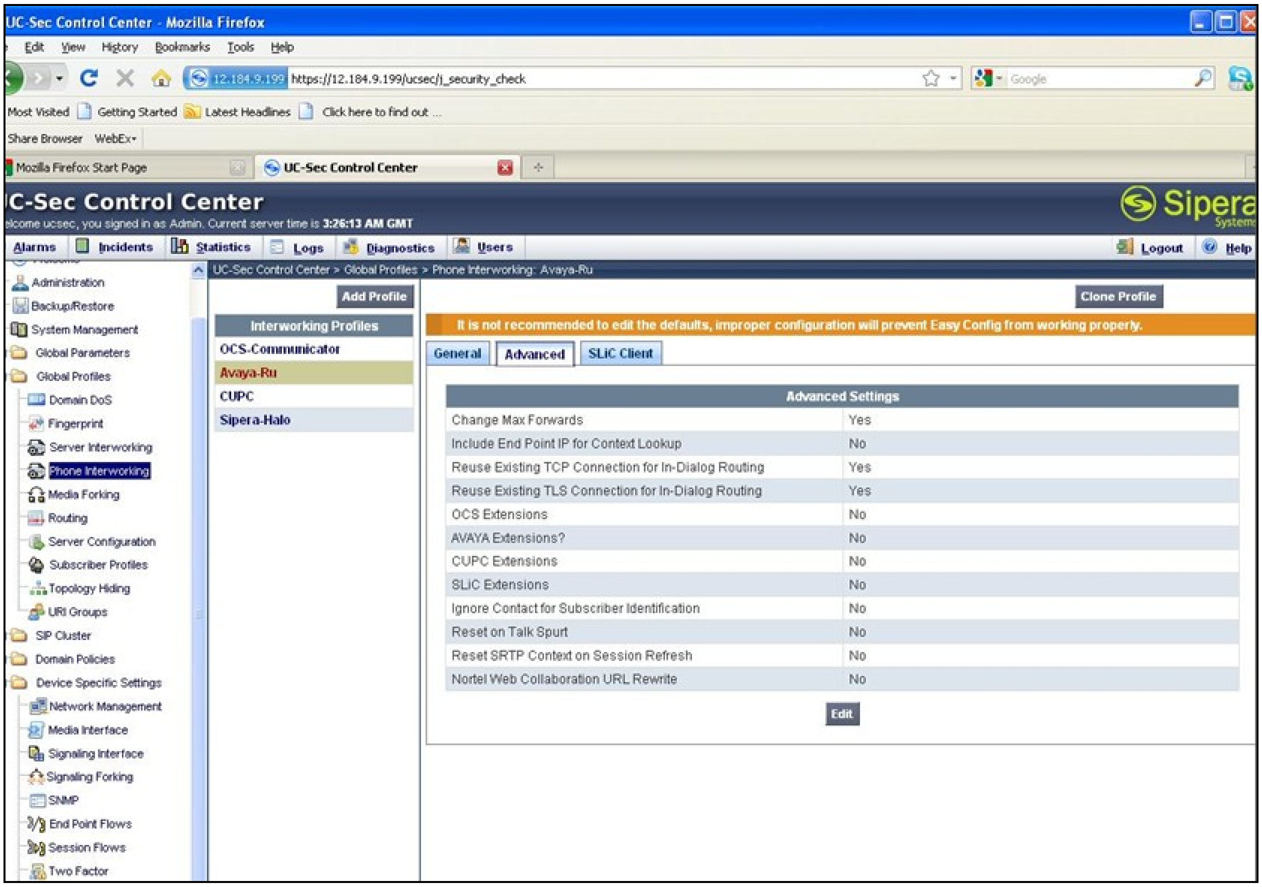
Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	---	---	□	☑	☑	□	□	None

Step 11: Phone- Interworking Profile

Phone Interworking profile defines how the interoperability with a Call Server provides features applicable to phones. This profile is used in End Point Subscriber Flow configuration (**Step 15**).

To define the **Phone- Interworking Profile**, navigate to **UC-Sec Control Center → Global Profiles → Phone Interworking**

In the example below, four profiles are shown in the middle pane. Only the profile named **Avaya-Ru** was used for the compliance testing. In this profile, **Reuse Existing TCP Connection for In-Dialog Routing** and **Reuse Existing TLS Connection for In-Dialog Routing** were set to **Yes** to enable Avaya phones with TCP and TLS support at the core side for reliable connection (TCP) and connection optimization (TLS). Click "Edit" tab and check the above two parameters, select **Finish** to continue (not shown).



UC-Sec Control Center, you signed in as Admin. Current server time is 3:26:13 AM GMT

UC-Sec Control Center > Global Profiles > Phone Interworking: Avaya-Ru

It is not recommended to edit the defaults, improper configuration will prevent Easy Config from working properly.

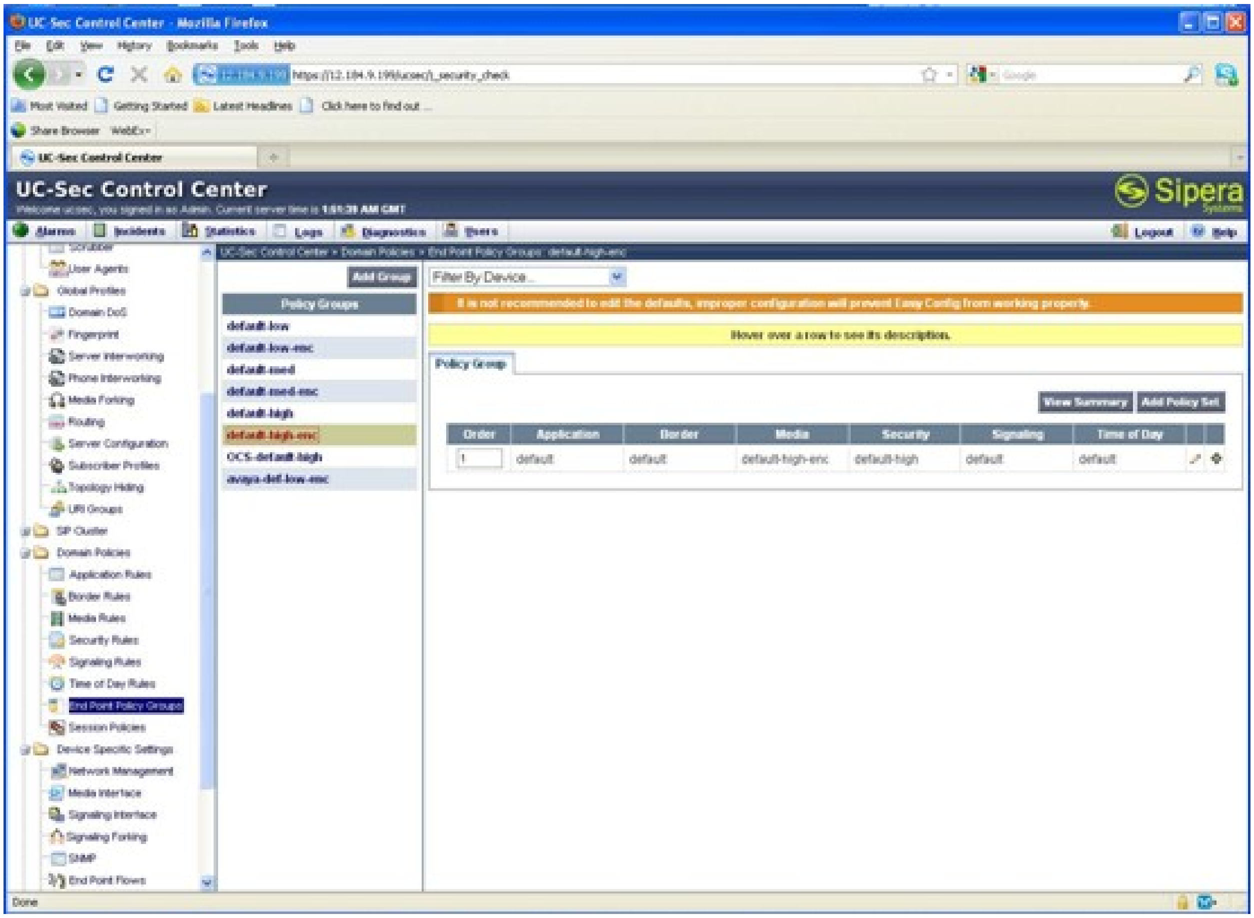
Advanced Settings	
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
Reuse Existing TCP Connection for In-Dialog Routing	Yes
Reuse Existing TLS Connection for In-Dialog Routing	Yes
OCS Extensions	No
AVAYA Extensions?	No
CUPC Extensions	No
SLiC Extensions	No
Ignore Contact for Subscriber Identification	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Nortel Web Collaboration URL Rewrite	No

Step 12: End Point Policy Groups

An end point policy group defines a set of rules that may be applied to different aspects of the data traffic. For the compliance test, the end point policy group was used to specify if (and how) the media stream should be encrypted and the security level.

To define a new policy group, navigate to **UC-Sec Control Center → Domain Policies → End Point Policy Groups**. Select the **Add Group** button in the middle pane to enter and submit the information.

For the compliance test, only the **default-high-enc** and **server-def-low** groups were used. Policy group **default-high-enc** defines the use of encrypted media (SRTP). Policy group **server-def-low** defines the use of unencrypted media (RTP, if SRTP is not needed). The details on the media can be obtained by clicking the Media link in the Policy Group displays shown below. These policy groups will be used in the server and subscriber flows defined in the following steps (**Steps 14-15**).



Policy Groups
default-low
default-low-enc
default-med
default-med-enc
default-high
default-high-enc
OCS-default-high
avaya-def-low-enc

It is not recommended to edit the defaults, improper configuration will prevent Easy Config from working properly.

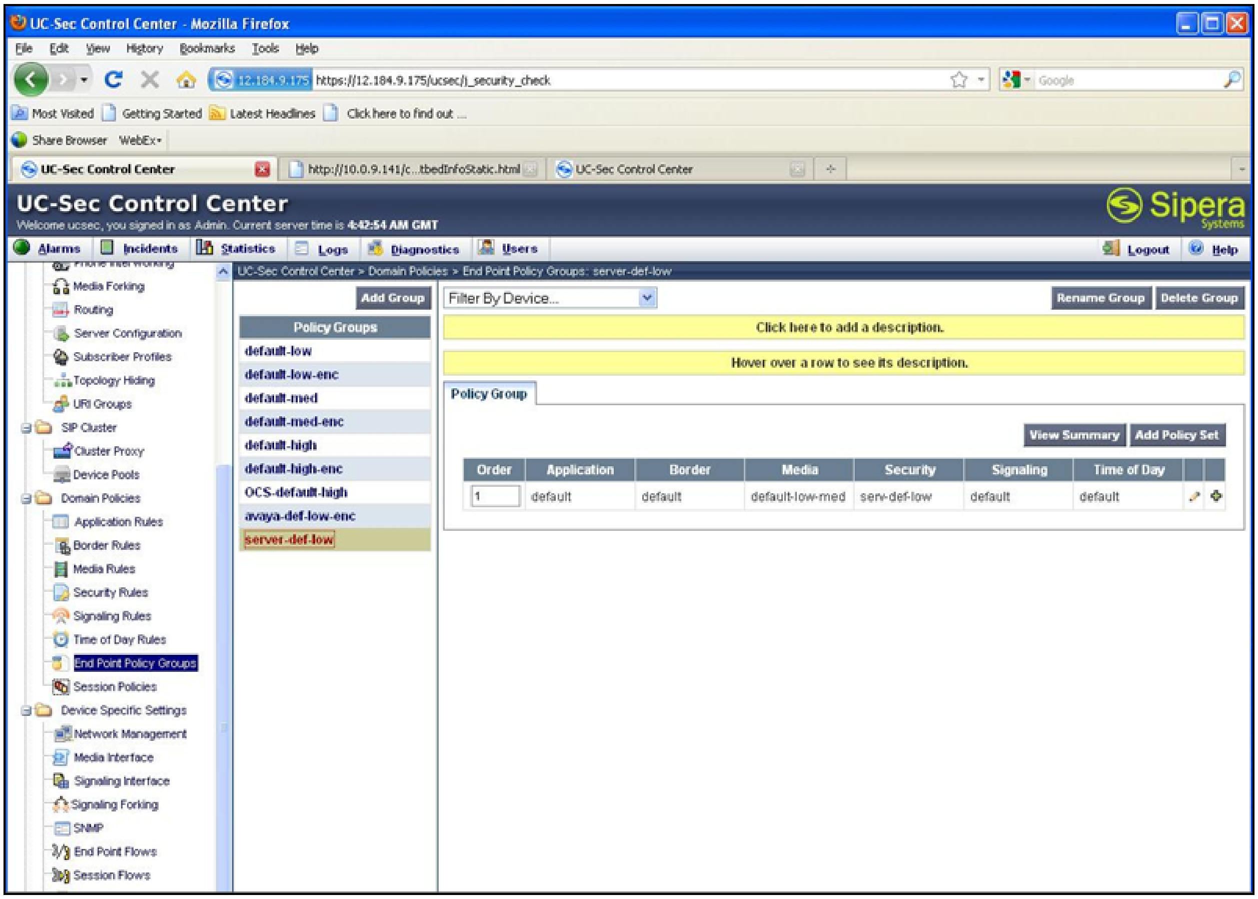
Hover over a row to see its description.

Policy Group

Order	Application	Border	Media	Security	Signaling	Time of Day
1	default	default	default-high-enc	default-high	default	default

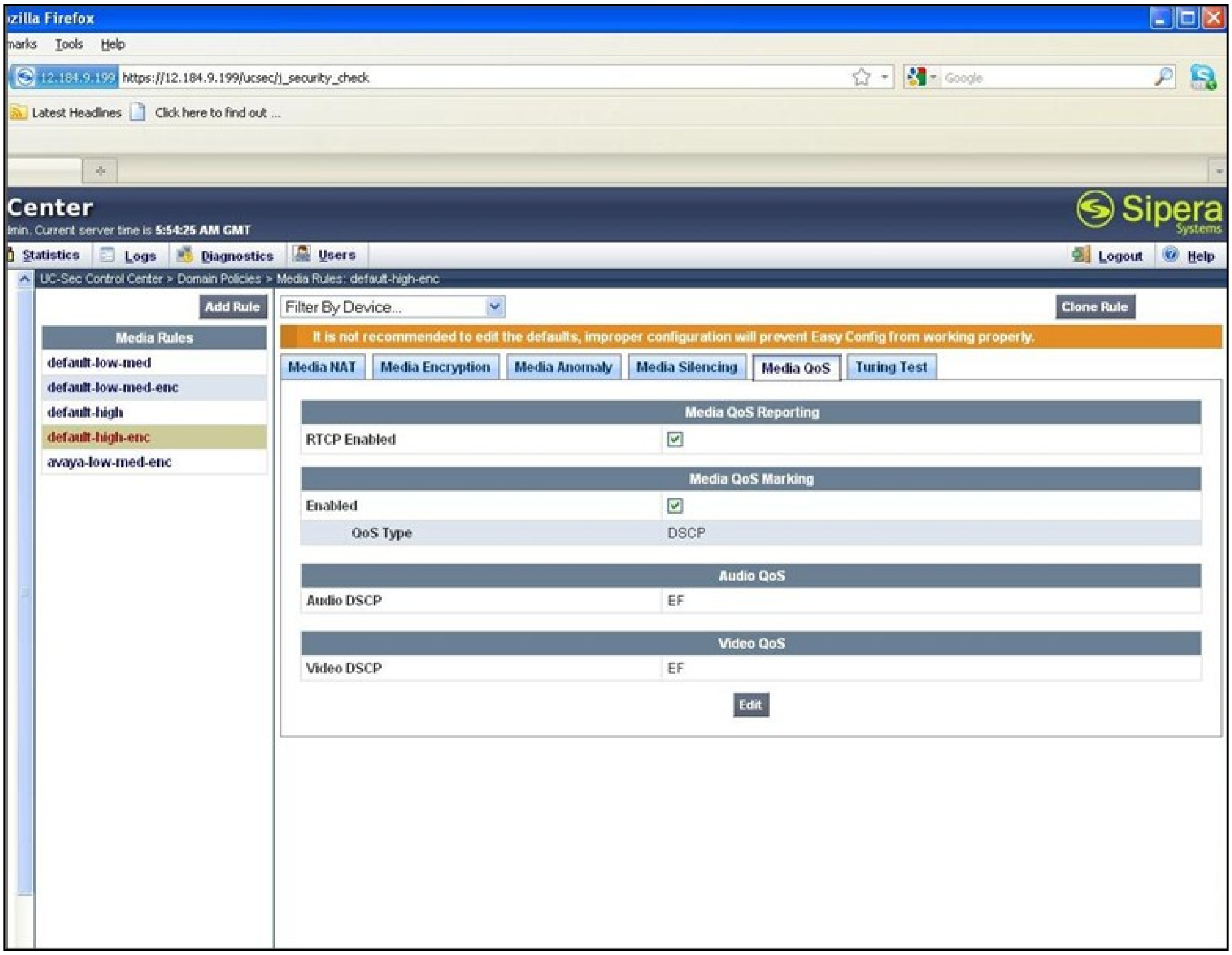
Step 13: End Point Policy Groups – Continued

Click **server-def-low** policy group in the middle panel, and the details of this policy group will be shown in the right panel. Policy group **server-def-low** defines the use of unencrypted media (RTP).



Order	Application	Border	Media	Security	Signaling	Time of Day
1	default	default	default-low-med	serv-def-low	default	default

For compliance testing, media QoS was enabled. To enable media QoS, navigate to **UC-Sec Control Center → Domain Policies → Media Rules → default-high-enc**. Select **Media QoS** from the right panel. Click the **Edit** tab and check the checkboxes under the title **Media QoS Reporting**" and "**Media QoS Marking**". Choose **DSCP**, and use default value (i.e. **EF**). Select **Finish** to continue (not shown).



It is not recommended to edit the defaults, improper configuration will prevent Easy Config from working properly.

Media Rules
default-low-med
default-low-med-enc
default-high
default-high-enc
avaya-low-med-enc

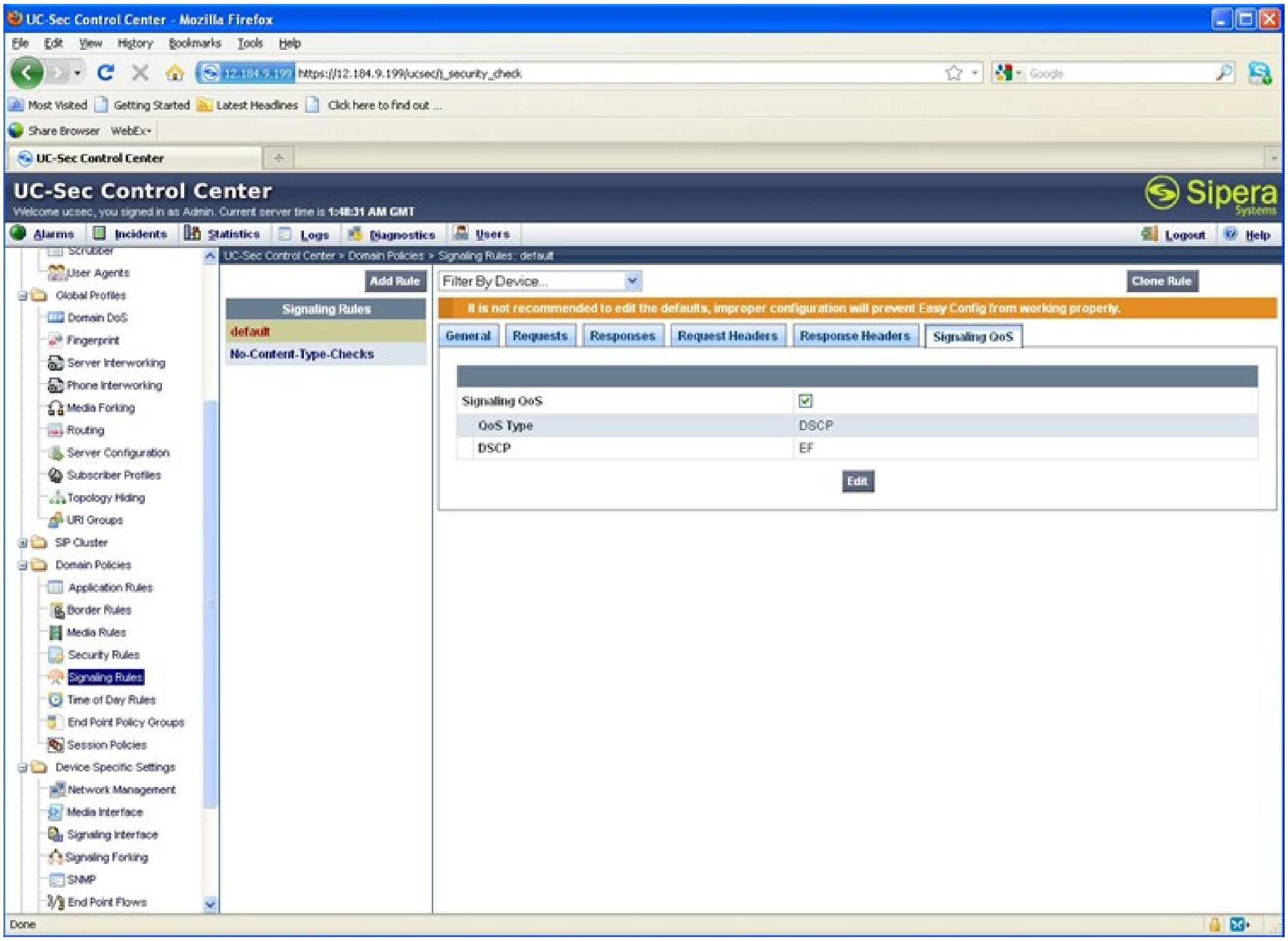
Media QoS Reporting	
RTCP Enabled	☑

Media QoS Marking	
Enabled	☑
QoS Type	DSCP

Audio QoS	
Audio DSCP	EF

Video QoS	
Video DSCP	EF

For compliance testing, Signaling QoS was enabled. To enable signaling QoS, navigate to **UC-Sec Control Center → Domain Policies → Signaling Rules → default,** select **Signaling QoS** from the right pane. Select **Edit** and check the **Signaling QoS** checkbox, Change the **QoS Type** to **DSCP**, set the Value as default (i.e. **EF**). Select **Finish** to continue (not shown).



It is not recommended to edit the defaults, improper configuration will prevent Easy Config from working properly.

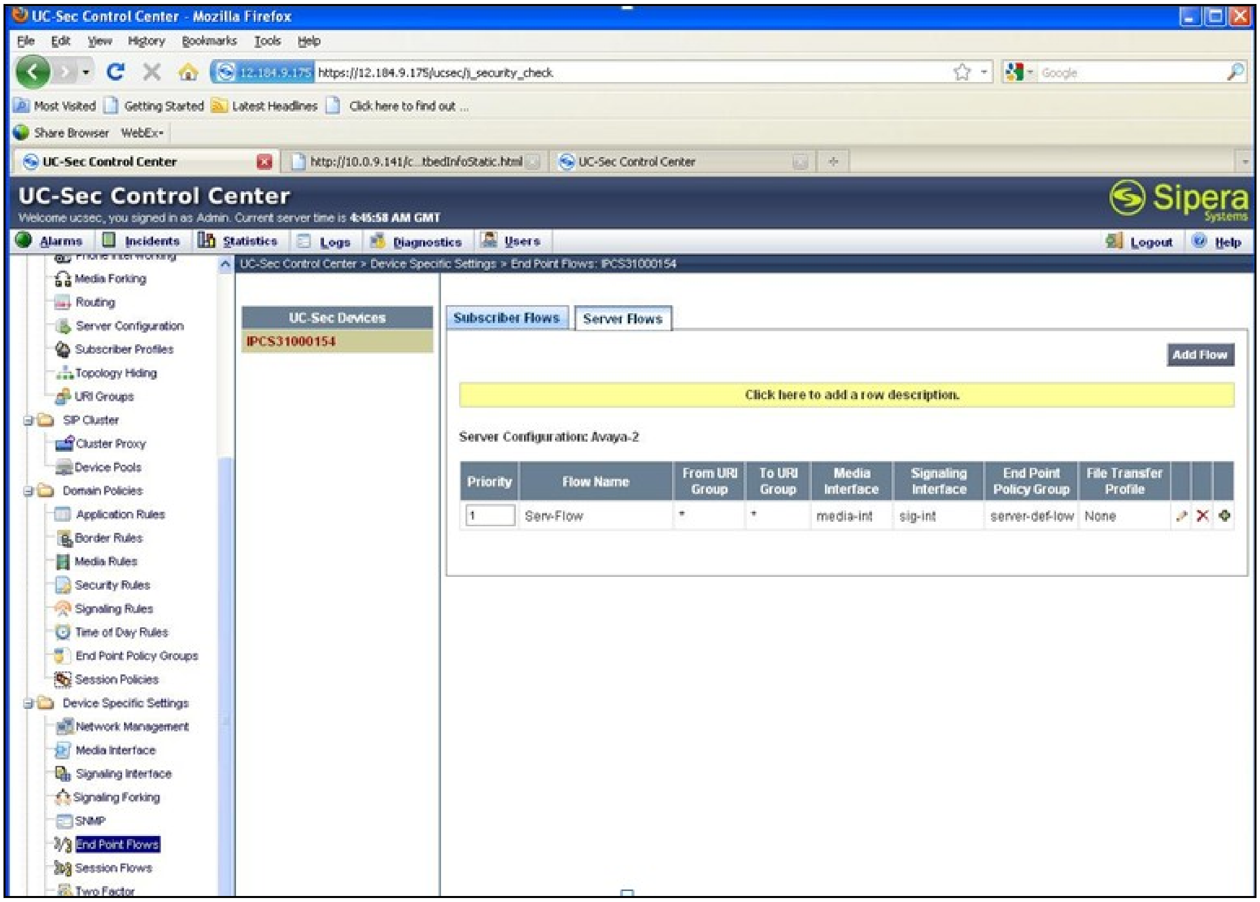
Signaling QoS	☑
QoS Type	DSCP
DSCP	EF

Step 14: Server Flow

Many of the previous steps have defined policies that will be applied to traffic if it is present. The server flow defines what traffic is actually allowed between the UC-Sec and the specified server, as well as which interfaces and media encryption will be used.

To define a new server flow, navigate to **UC-Sec Control Center → Device Specific Settings → Endpoint Flows**. Select the **Server Flows** tab. Select the **Add Flow** button in the right pane to enter and submit the new information.

The example below shows one server flow used for the compliance test. It specifies that all traffic to or from any URI Group will be allowed to the server named Avaya-2 (Session Manager 6.0). Media traffic will use **Media Interface** – media-int (**Step 6**) and signaling traffic will use **Signaling Interface** – **sig-int** (**Step 5**). The **Endpoint Policy Group** named **server-def-low** (**Step 13**) will be applied to this traffic which specifies that the media is unencrypted.



Server Configuration: Avaya-2

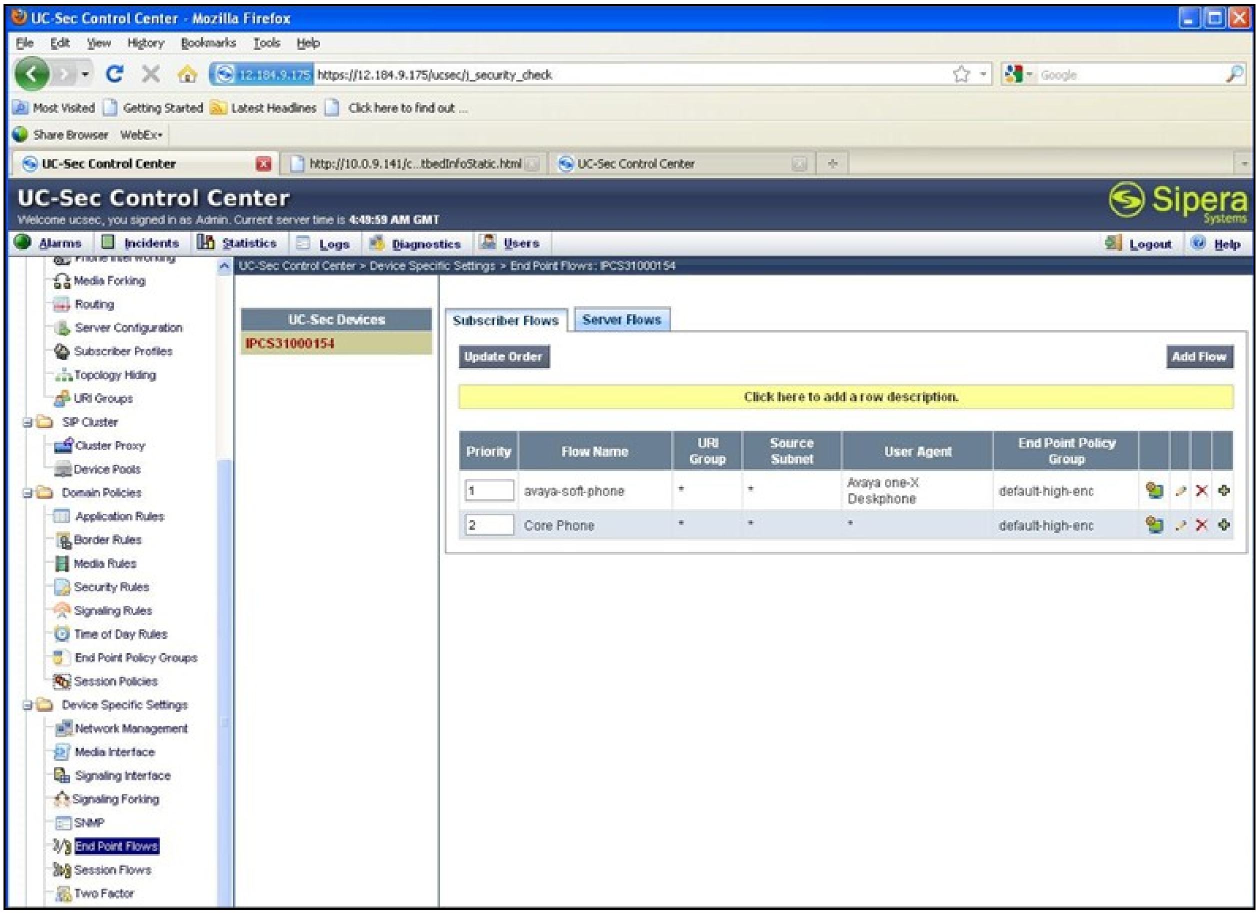
Priority	Flow Name	From URI Group	To URI Group	Media Interface	Signaling Interface	End Point Policy Group	File Transfer Profile
1	Serv-Flow	*	*	media-int	sig-int	server-def-low	None

Step 15: Subscriber Flows

A subscriber flow defines what traffic is allowed between the UC-Sec and the specified endpoints in much the same way the server flow defines the traffic allowed between the UC-Sec and the server.

To define a new subscriber flow, navigate to **UC-Sec Control Center →Device Specific Settings → Endpoint Flows**. Select the **Subscriber Flows** tab. Select the **Add Flow** button in the right pane to enter and submit the new information.

Two subscriber flows were created for the compliance test. If the traffic does not match the first flow, then the next flow in the list will be tested until a match is found. The detailed matching criteria are shown in **Step 17**. The **Endpoint Policy Group** named **default-high-enc** (**Step 13**) will be applied to this traffic which specifies that the media is encrypted. The second flow will match all traffic from the core Avaya IP Telephones. Again the **Endpoint Policy Group** named **default-high-enc** (**Step 13**) will be applied to this traffic which specifies that the media is also encrypted. To see the complete details of a flow, click the monitor icon associated with the flow of interest in the right pane.

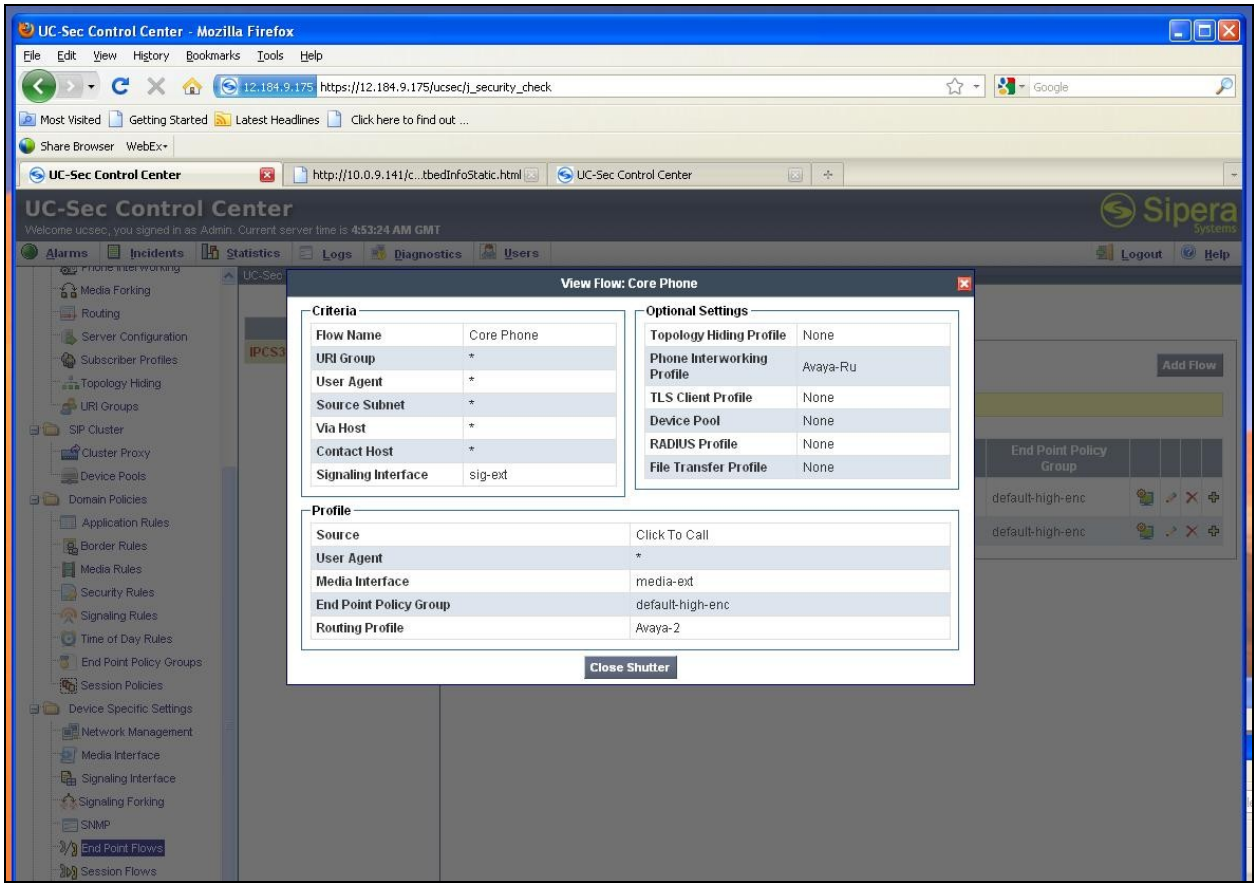


Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group
1	avaya-soft-phone	*	*	Avaya one-X Deskphone	default-high-enc
2	Core Phone	*	*	*	default-high-enc

Step 16: Subscriber Flow – Details

The example below shows the details of the second flow (***Core Phone***) in the list in **Step 15**. Select the **monitor** icon (not shown), for the second flow. Unlike the server flow, parameters such as **Topology Hiding Profile** and **Routing Profile** are defined within the subscriber flow itself. For the server traffic, these parameters were not defined in the flow but were defined in the server configuration.

This flow will match traffic from the core Avaya 9600 Series IP Telephones since the **Signaling Interface** field is set to **sig-ext** (**Step 5**) in the **Criteria** section. Media traffic will use **Media Interface – media-ext** (**Step 6**). The **End Point Policy Group** used is **default-high-enc** (**Step 13**). The **Phone Interworking Profile** used is **Avaya-Ru** (**Step 11**). The **Routing Profile** used is **Avaya-2** (**Step 17**).



View Flow: Core Phone

Criteria

Flow Name	Core Phone
URI Group	*
User Agent	*
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	sig-ext

Optional Settings

Topology Hiding Profile	None
Phone Interworking Profile	Avaya-Ru
TLS Client Profile	None
Device Pool	None
RADIUS Profile	None
File Transfer Profile	None

Profile

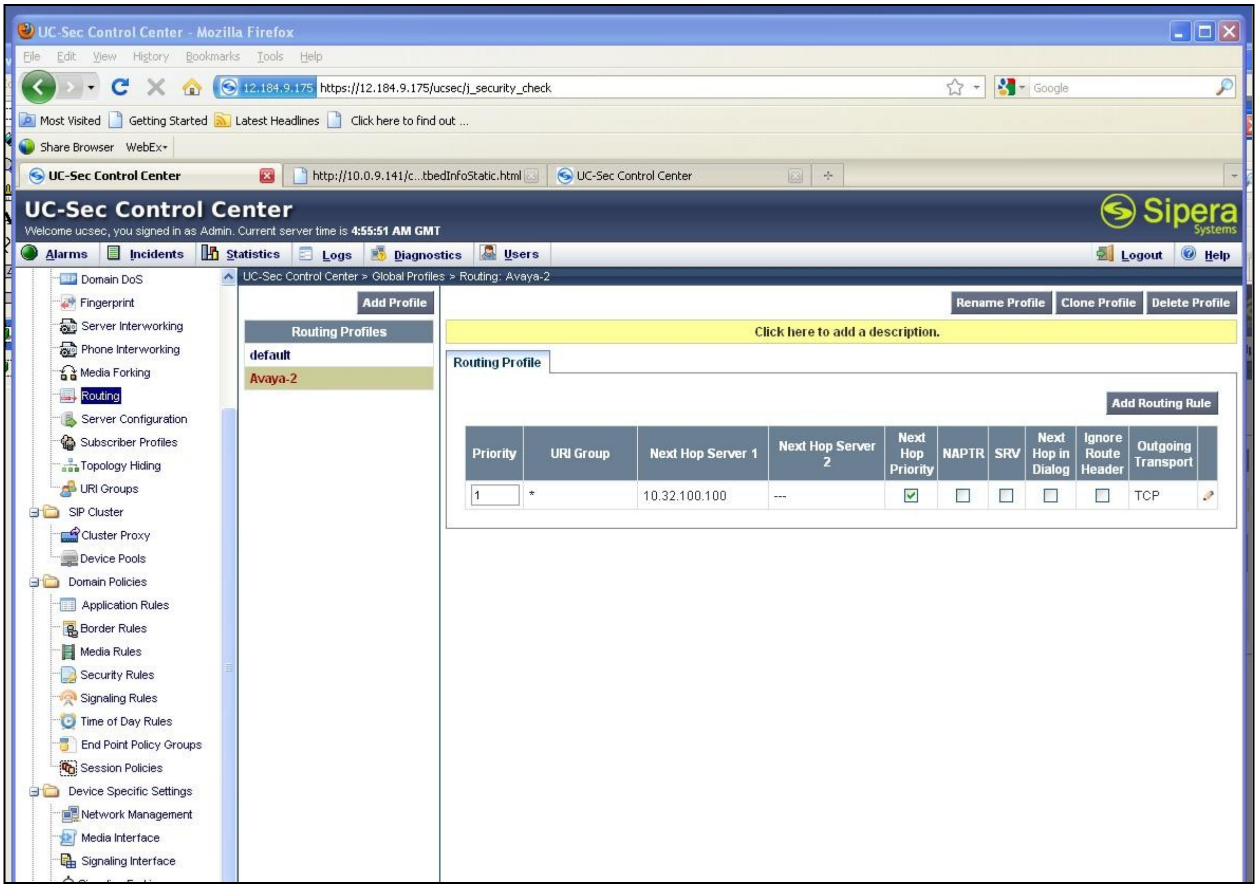
Source	Click To Call
User Agent	*
Media Interface	media-ext
End Point Policy Group	default-high-enc
Routing Profile	Avaya-2

Step 17: Subscriber – Routing Profile

A routing profile defines how a call is to be routed. In this case, the routing profile is applied to calls from the subscriber to UC-Sec.

To define a new routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing**. Select the **Add Profile** button in the middle pane to enter and submit the new information.

The example below shows the routing profile named **Avaya-2** used by all the subscriber flows defined in **Steps 15-16**. It shows that all traffic (**URI Group** = *) using this profile will be routed to IP address 10.32.100.100 (Session Manager 6.0) as the next hop as defined in the **Next Hop Server 1** field.



UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 4:55:51 AM GMT

UC-Sec Control Center > Global Profiles > Routing: Avaya-2

Routing Profiles

- default
- Avaya-2

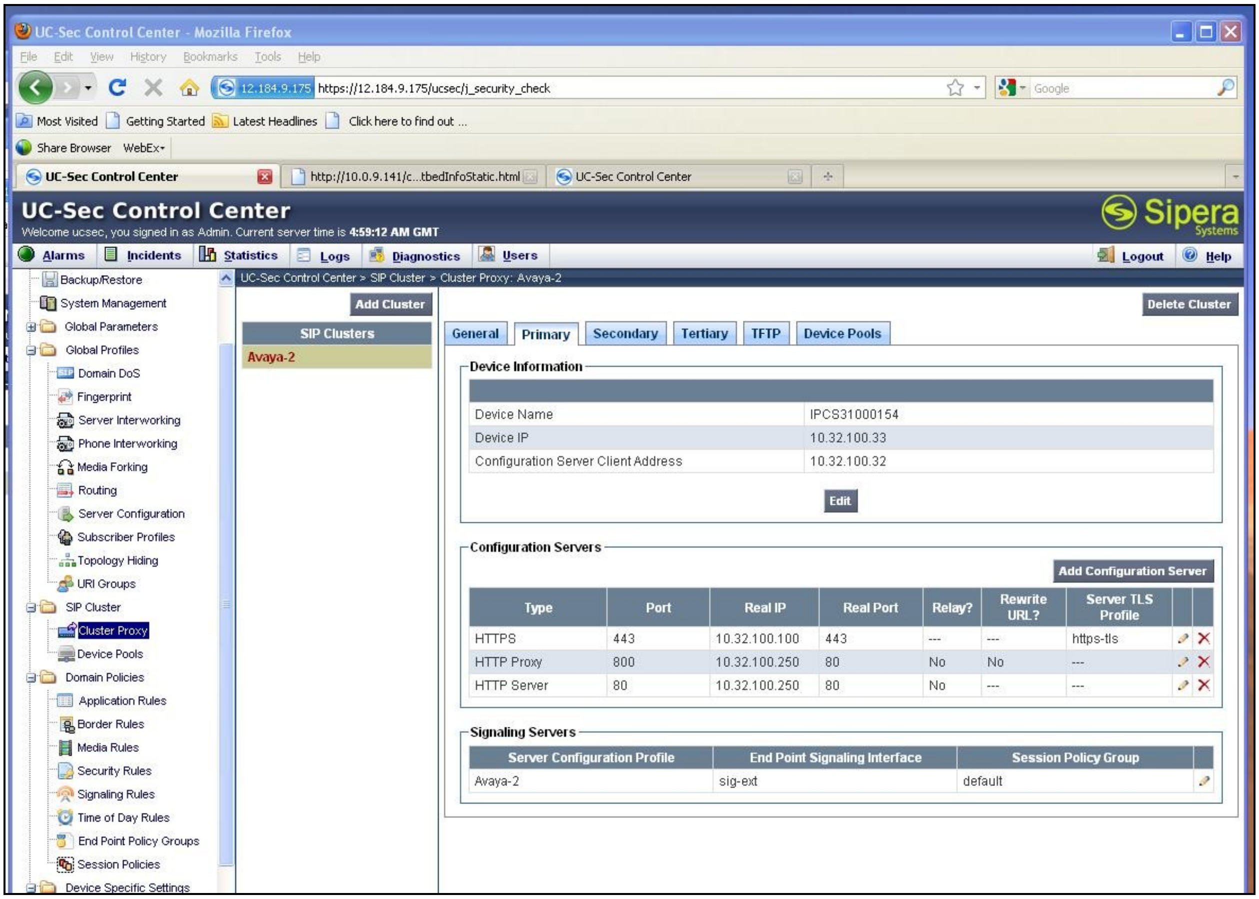
Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.32.100.100	---	☑	□	□	□	□	TCP

Step 18: SIP Clusters

As part of the compliance test, SIP clusters were used to define how HTTP/HTTPS traffic will be routed for different groups of endpoints. For compliance test, HTTPS was used. Example shows configuration for both HTTP/HTTPS.

To define a new cluster, navigate to **UC-Sec Control Center → SIP Cluster**. Select the **Add Cluster** button in the middle pane to enter and submit the new information.

The cluster used for the compliance test is shown in the middle pane. By highlighting a profile in the middle pane, its details are shown in the right pane. The example below shows the cluster named **Avaya-2**. It defines that HTTP/HTTPS traffic from the **Device IP 10.32.100.33** will be routed out the **Configuration Server Client Address 10.32.100.32** to the internal HTTP server address **10.32.100.100** as specified in the **Real IP** field. This enables the Avaya IP Telephones to get their configuration data via the UC-Sec.



UC-Sec Control Center > SIP Cluster > Cluster Proxy: Avaya-2

Device Information

Device Name	IPCS31000154
Device IP	10.32.100.33
Configuration Server Client Address	10.32.100.32

Configuration Servers

Type	Port	Real IP	Real Port	Relay?	Rewrite URL?	Server TLS Profile
HTTPS	443	10.32.100.100	443	---	---	https-tls
HTTP Proxy	800	10.32.100.250	80	No	No	---
HTTP Server	80	10.32.100.250	80	No	---	---

Signaling Servers

Server Configuration Profile	End Point Signaling Interface	Session Policy Group
Avaya-2	sig-ext	default

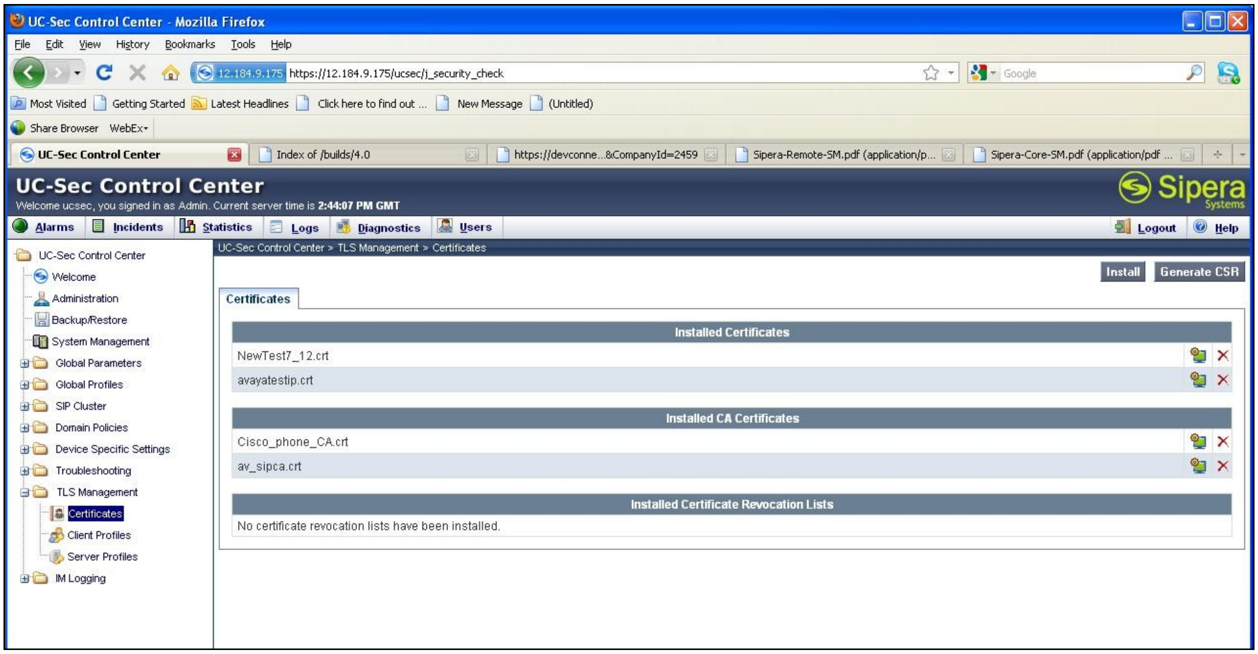
Step 19: TLS Certificate

A TLS certificate is used for establishing TLS connection between Avaya phones/clients and Sipera UC-Sec. Below are the two certificates that were used for TLS authentication:

1. Using a third party certificate, configure the TRUSTCERTS option in Avaya 46xxsettings file to include this certificate. Upload its corresponding root CA (Certificate Authority) certificate to the http/https server (For details how to configure TRUSTCERTS and upload the corresponding root CA certificate to http/https server, please reference to **Section 10, [1]** through **[3].**

2. Using a root CA certificate from Avaya Aura® Session Manager. (Obtain the CA certificate from Avaya) and install it on the Sipera UC-Sec

To look at the details of the certificate, navigate to **UC-Sec Control Center → TLS management → Certificates.** The example below shows the two TLS certificates named ***NewTest7_12.crt*** and ***avayatestip.crt. NewTest7_12.crt*** is the one used for setting up TLS for signaling message between the Avaya phones and the Sipera UC-Sec. (***avayatestip.crt***, on the other hand, is used to set up the HTTPS connection between the Avaya phones to the Sipera UC-Sec, used in step 18). The CA certificate, ***av_sipca.crt***, is the one extracted from Session Manager and is used to authenticate the certificate provided from the phones.


UC-Sec Control Center - Mozilla Firefox
File Edit View History Bookmarks Tools Help
12.184.9.175 https://12.184.9.175/ucsec/j_security_check
Google
Most Visited Getting Started Latest Headlines Click here to find out ... New Message (Untitled)
Share Browser WebEx
UC-Sec Control Center
Index of /builds/4.0
https://devconne...&CompanyId=2459
Sipera-Remote-SM.pdf (application/p...
Sipera-Core-SM.pdf (application/pdf ...
UC-Sec Control Center
Sipera Systems
Alarms Incidents Statistics Logs Diagnostics Users
Logout Help
UC-Sec Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
Device Specific Settings
Troubleshooting
TLS Management
Certificates
Client Profiles
Server Profiles
IM Logging
UC-Sec Control Center > TLS Management > Certificates
Install
Generate CSR
Certificates

Welcome ucsec, you signed in as Admin. Current server time is **2:44:07 PM GMT**

Installed Certificates
NewTest7_12.crt
avayatestip.crt

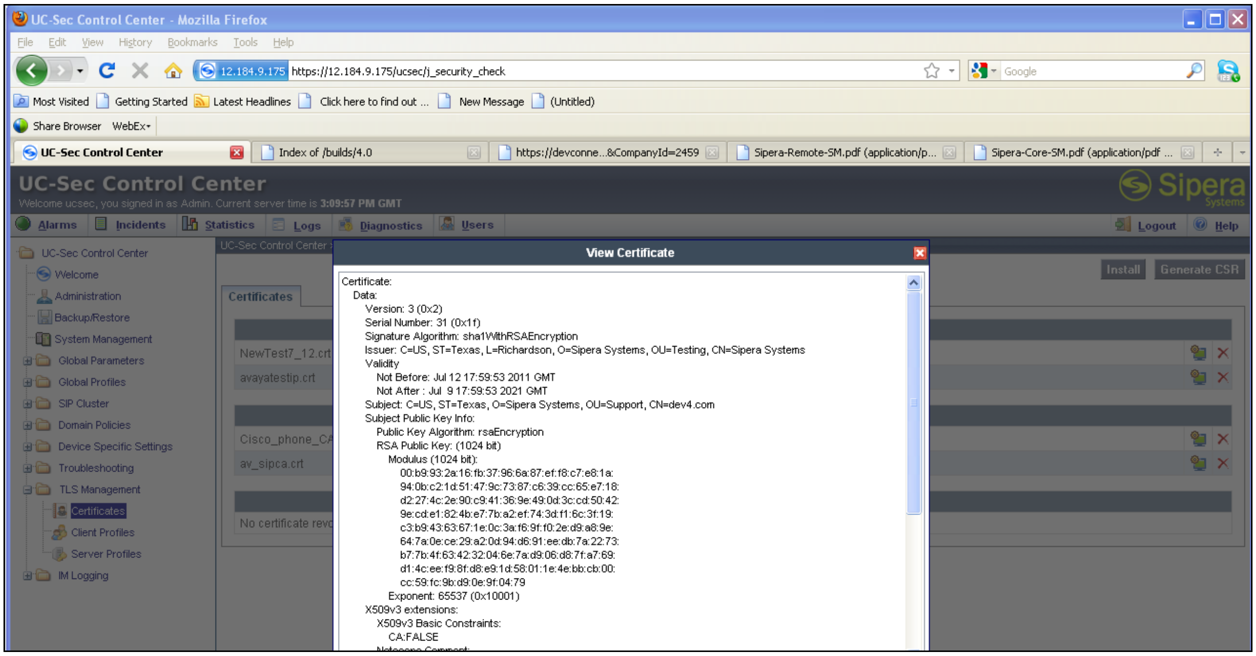
Installed CA Certificates
Cisco_phone_CA.crt
av_sipca.crt

Installed Certificate Revocation Lists
No certificate revocation lists have been installed.

Step 20: TLS Certificate – Continued

Press the **View** button to shows details of the certificate.

The example below is for ***NewTest7_12.crt***. This certificate was generated at Sipera, and its corresponding root CA certificate (***sipera-ca.crt***) is uploaded to the Avaya http/https server, so that the Avaya phone will download this root CA certificate during the Session Manager PPM process and use it to authenticate this server certificate.



```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 31 (0x1f)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=US, ST=Texas, L=Richardson, O=Sipera Systems, OU=Testing, CN=Sipera Systems
    Validity
      Not Before: Jul 12 17:59:53 2011 GMT
      Not After : Jul  9 17:59:53 2021 GMT
    Subject: C=US, ST=Texas, O=Sipera Systems, OU=Support, CN=dev4.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:b9:93:2a:16:fb:37:96:6a:87:ef:f8:c7:e8:1a:
          94:0b:c2:1d:51:47:9c:73:87:c6:39:cc:65:e7:18:
          d2:27:4c:2e:90:c9:41:36:9e:49:0d:3c:cd:50:42:
          9e:cd:e1:82:4b:e7:7b:a2:ef:74:3d:f1:6c:3f:19:
          c3:b9:43:63:67:1e:0c:3a:f6:9f:f0:2e:d9:a8:9e:
          64:7a:0e:ce:29:a2:0d:94:d6:91:ee:db:7a:22:73:
          b7:7b:4f:63:42:32:04:6e:7a:d9:06:d8:7f:a7:69:
          d1:4c:ee:f9:8f:d8:e9:1d:58:01:1e:4e:bb:cb:00:
          cc:59:fc:9b:d9:0e:9f:04:79
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      Netscape Comment:
```

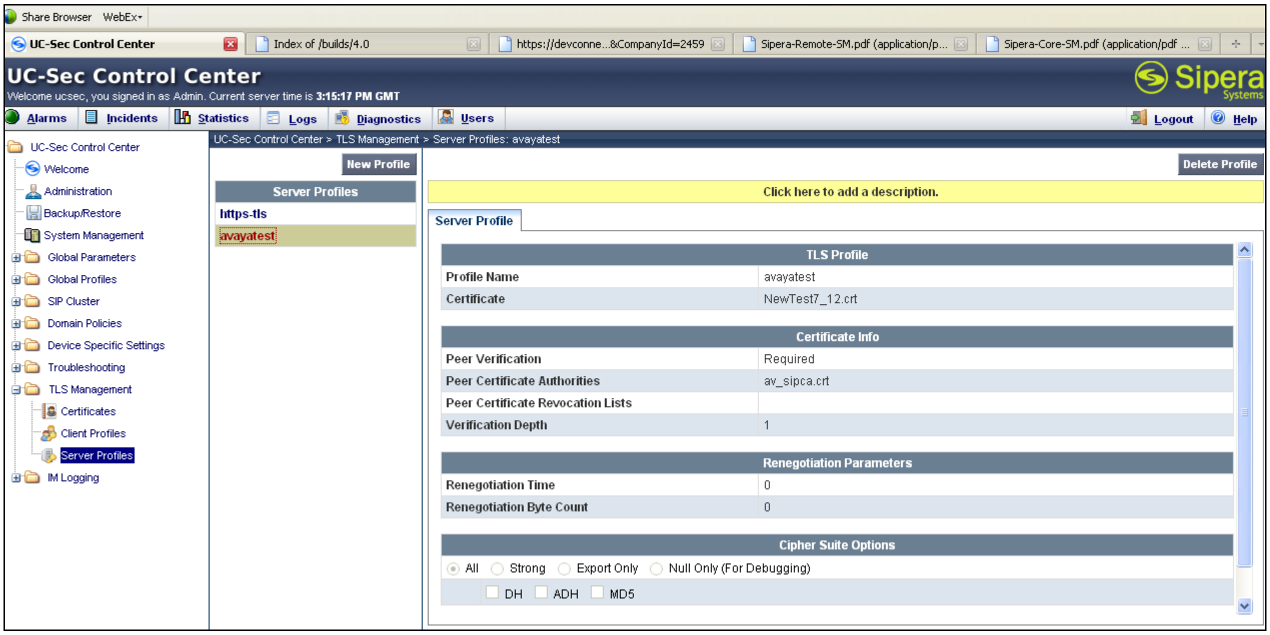
To install a 3rd party certificate, click the **Install** button (not shown). Then choose the certificate file and key file stored in the desktop and click the **Upload** button (not shown). This will allow the certificate to upload to EMS. Additional commands must be run to download these certificates to the Sipera UC-Sec. Please refer to UC-Sec Administration Guide [10].

After installing the certificate, navigate to **UC-Sec Control Center → TLS management → Server Profiles,** and select **New Profile**. Include the certificate (***NewTest7_12.crt)*** and root CA certificate (***sipera-ca.crt***) that has been installed, and select **Finish**. Use this certificate server profile in the appropriate signaling interface (for TLS).

Also install another certificate and TLS server profile using the above steps. Then navigate to **UC-Sec Control Center → SIP Cluster → Cluster Proxy → <name of the SIP cluster> → Primary**, and under the **Configuration Servers**, add the HTTPS server, and include this new TLS server profile. This is used for HTTPS connection **(step 18).**

Step 21: TLS Certificate – Continued

As mentioned in above step, a certificate server profile needs to be created to include the above certificates, as show below.



TLS Profile	
Profile Name	avayatest
Certificate	NewTest7_12.crt

Certificate Info	
Peer Verification	Required
Peer Certificate Authorities	av_sipca.crt
Peer Certificate Revocation Lists	
Verification Depth	1

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Cipher Suite Options

● All ○ Strong ○ Export Only ○ Null Only (For Debugging)

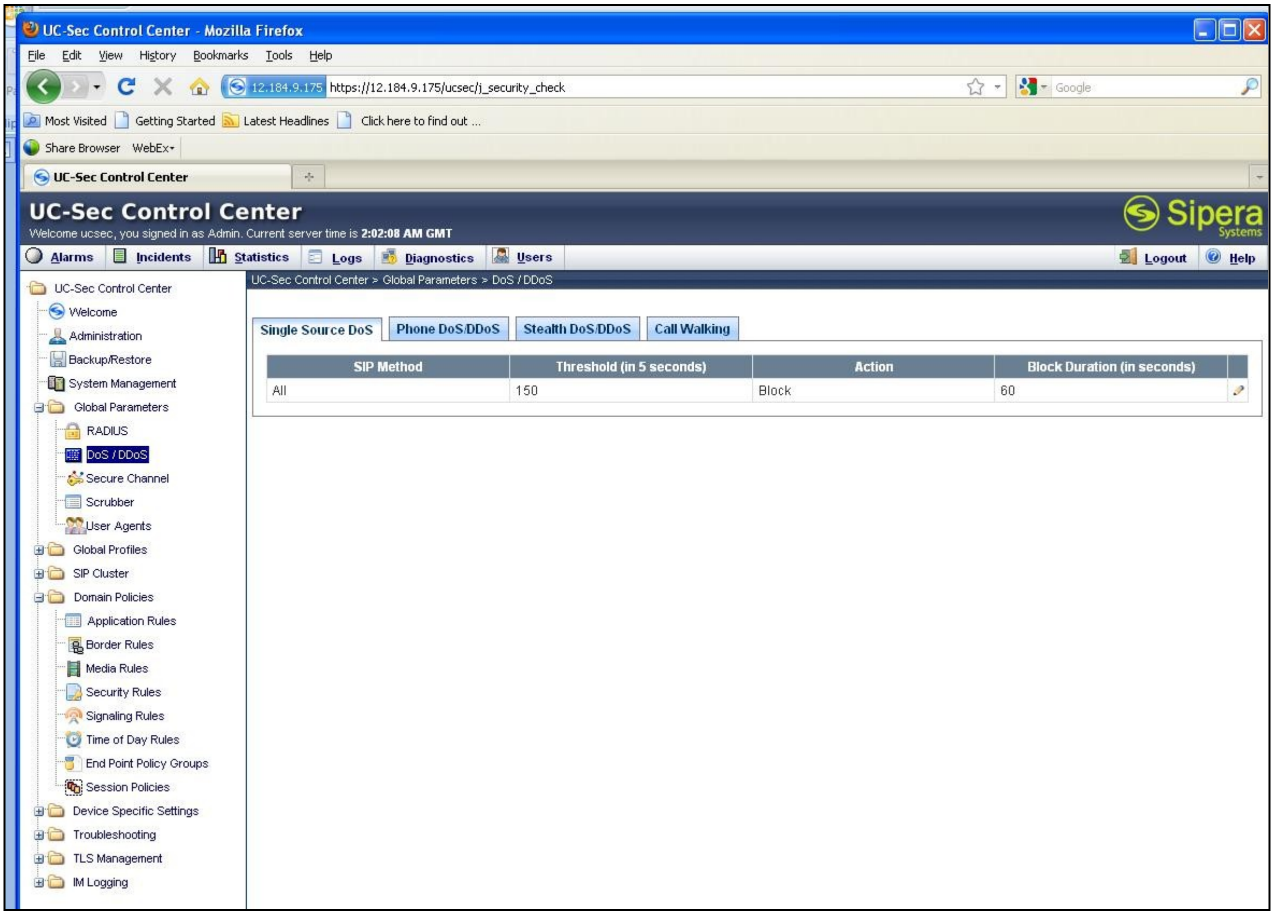
□ DH □ ADH □ MD5

This server profile contains the server certificate ***NewTest7_12.crt***, as well as the root CA certificate ***av-sipca.crt***. Together they will be used to setup a TLS connection between Avaya phones and UC-Sec with mutual authentication.

This certificate server profile should be incorporated into signaling interface, as in **Step 5.**

Step 22: Configure the four different DoS in GUI

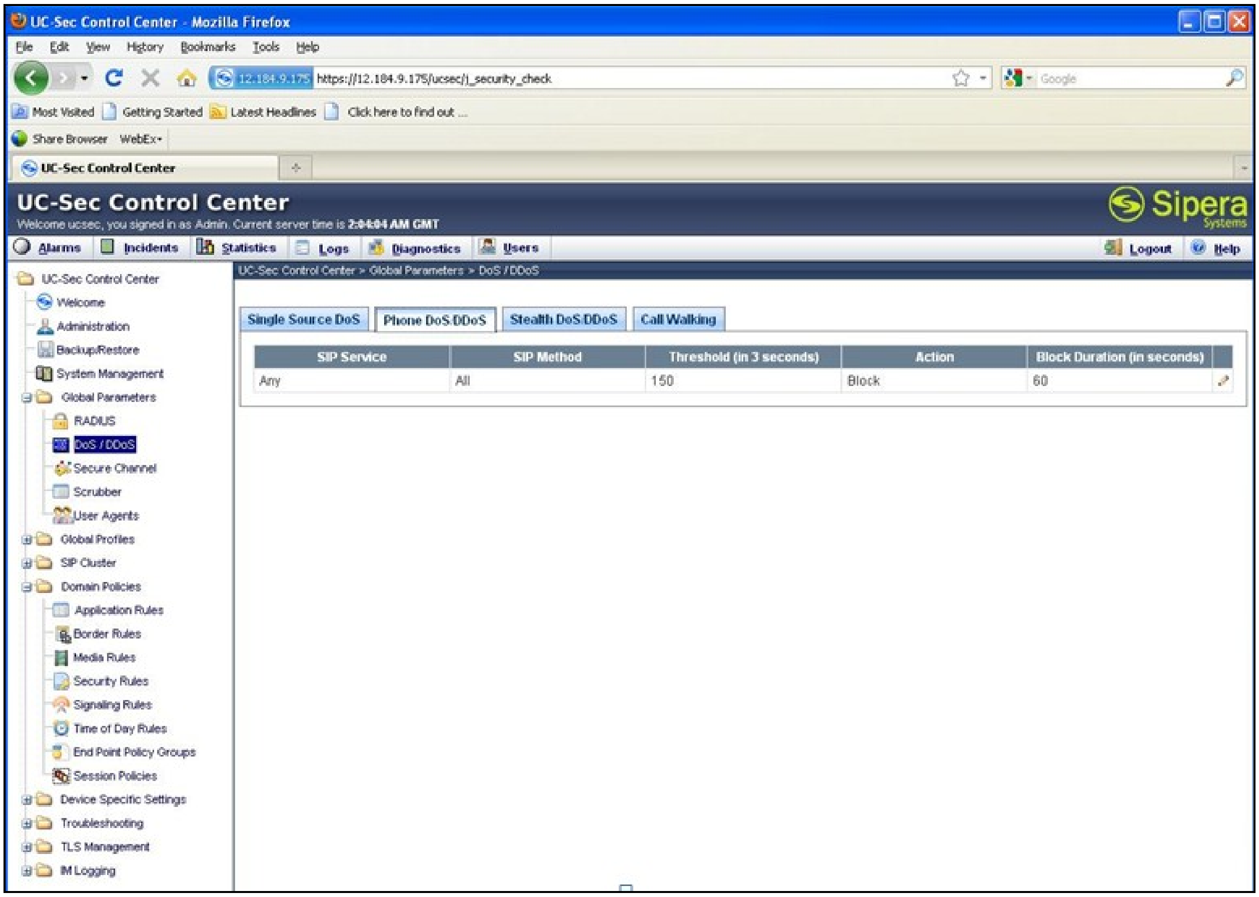
Navigate to **UC-Sec Control Center → Global Parameters → DoS/DDoS → Single Source DoS.** Select the **Edit** icon. Change the **Threshold (in 5 seconds)** and **Action** to desired values (in this example, **Threshold (in 5 seconds)** is set to **150** and **Action** is **Block**). Select **Finish** (not shown)**.** Select **Phone DoS/DDoS** to continue.



SIP Method	Threshold (in 5 seconds)	Action	Block Duration (in seconds)
All	150	Block	60

Step 23: Configure the four different DoS in GUI (continued)

Select the **Edit** icon. Change the **Threshold (in 3 seconds), Action** and **Block Duration (in seconds)** to desired values (in this example, **Threshold (in 3 seconds)** is set to **150**, **Action** is **Block,** and **Block Duration** is **60**). Select **Finish** (not shown). Select **Stealth DoS/DDoS** to continue.



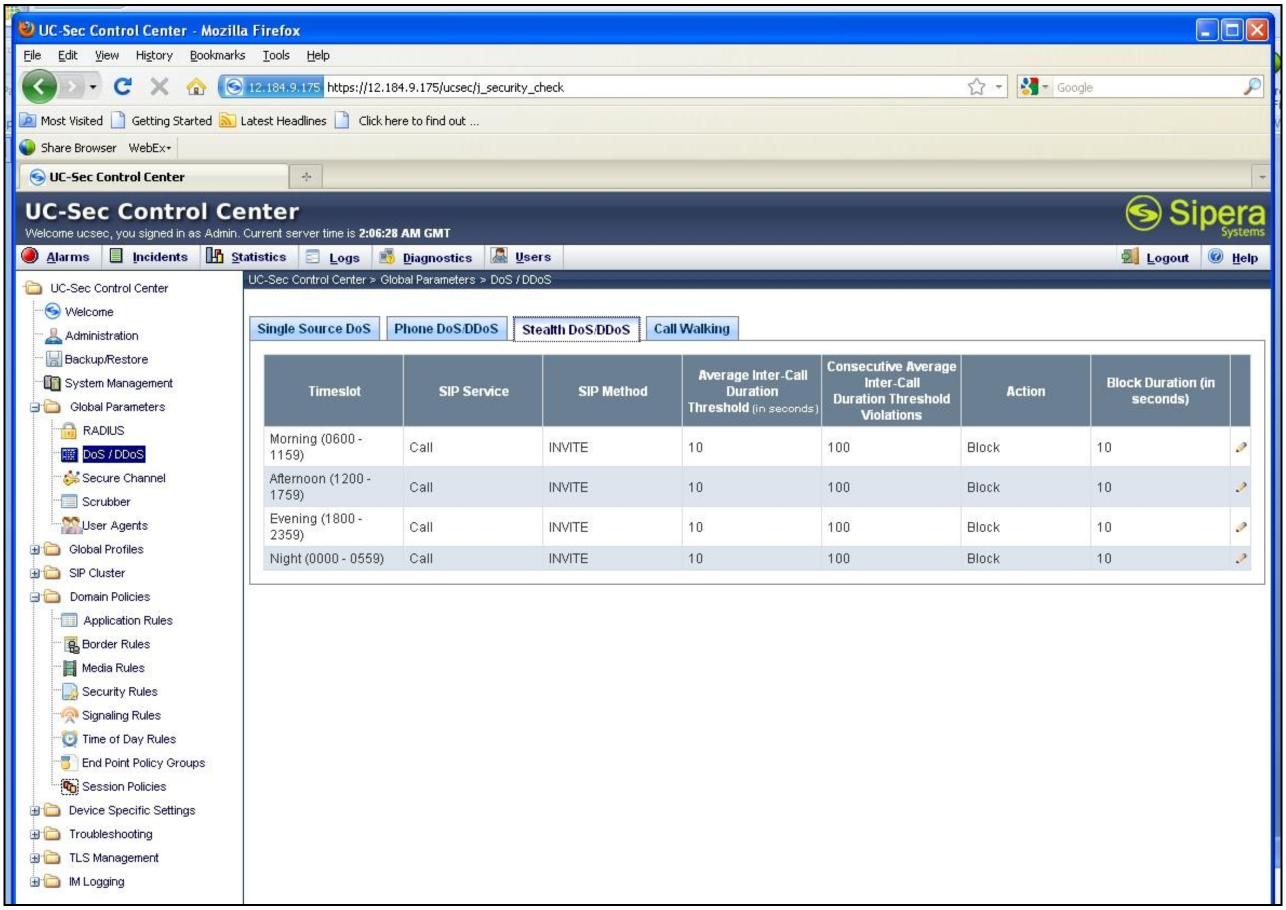
UC-Sec Control Center > Global Parameters > DoS / DDoS

UC-Sec Control Center - Mozilla Firefox
https://12.184.9.175/ucsec/j_security_check
UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 2:04:04 AM GMT
Alarms
Incidents
Statistics
Logs
Diagnostics
Users
Logout
Help
Single Source DoS
Phone DoS/DDoS
Stealth DoS/DDoS
Call Walking

SIP Service	SIP Method	Threshold (in 3 seconds)	Action	Block Duration (in seconds)
Any	All	150	Block	60

Step 24: Configure the four different DoS in GUI (continued)

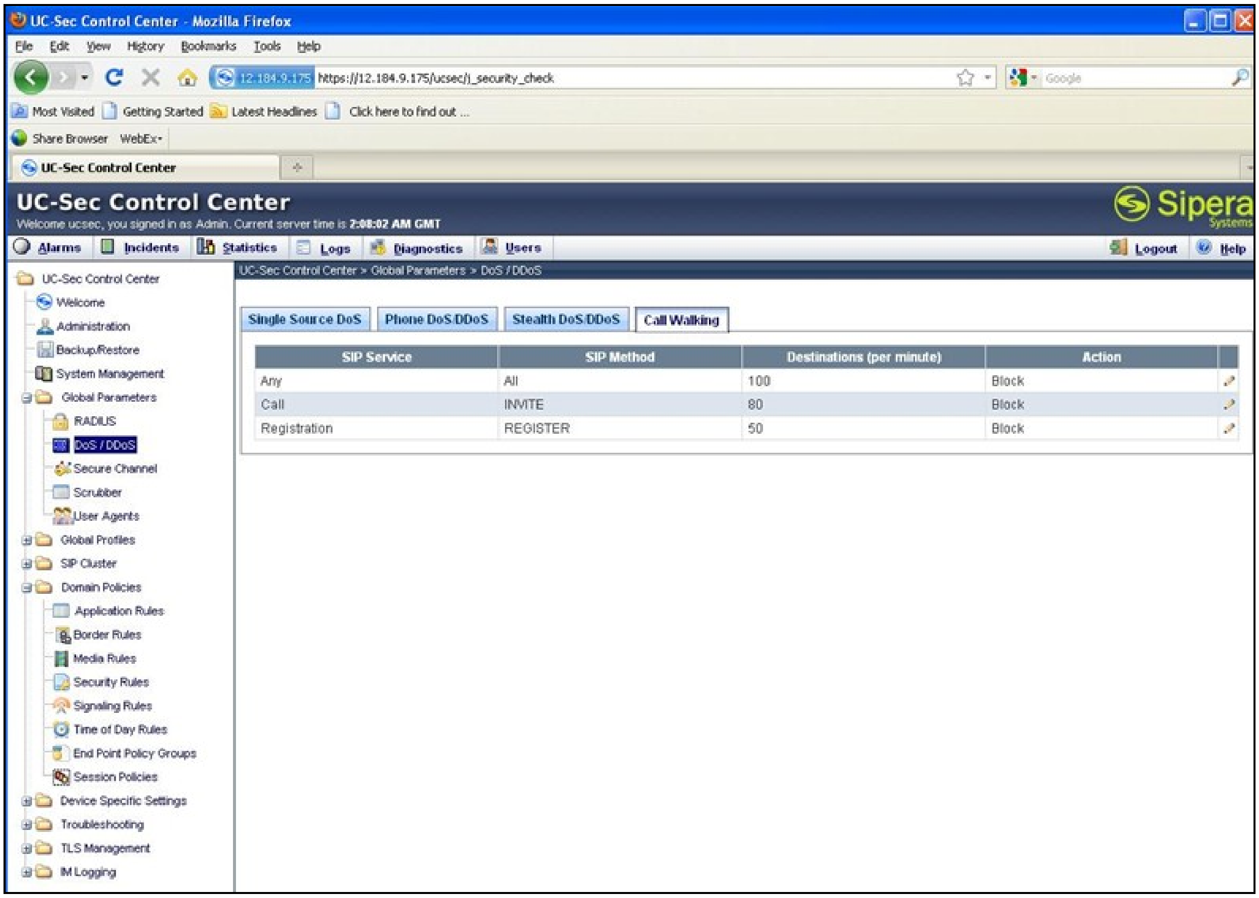
Select the **Edit** icon. Change the **Average Inter-Call Duration Threshold, Consecutive Average Inter-Call Duration Threshold Violations**, and **Action** to desired values (in this example, **Average Inter-Call Duration Threshold** is set to 10, **Consecutive Average Inter-Call Duration Threshold Violations** is set to **100**, and the **Action** is set to **Block**). Select **Finish** (not shown). Select **Call Walking** to continue.



Timeslot	SIP Service	SIP Method	Average Inter-Call Duration Threshold (in seconds)	Consecutive Average Inter-Call Duration Threshold Violations	Action	Block Duration (in seconds)	
Morning (0600 - 1159)	Call	INVITE	10	100	Block	10	✎
Afternoon (1200 - 1759)	Call	INVITE	10	100	Block	10	✎
Evening (1800 - 2359)	Call	INVITE	10	100	Block	10	✎
Night (0000 - 0559)	Call	INVITE	10	100	Block	10	✎

Step 25: Configure the four different DoS in GUI (continued)

Select the **Edit** icon. Change the **Destinations (per minute)** and **Action** to desired values for each SIP service. (in this example, **Destinations (per minute)** is set **to 100** for **Any**, **80** for **Call** and **50** for **Registration**, and **Action** is **Block**).



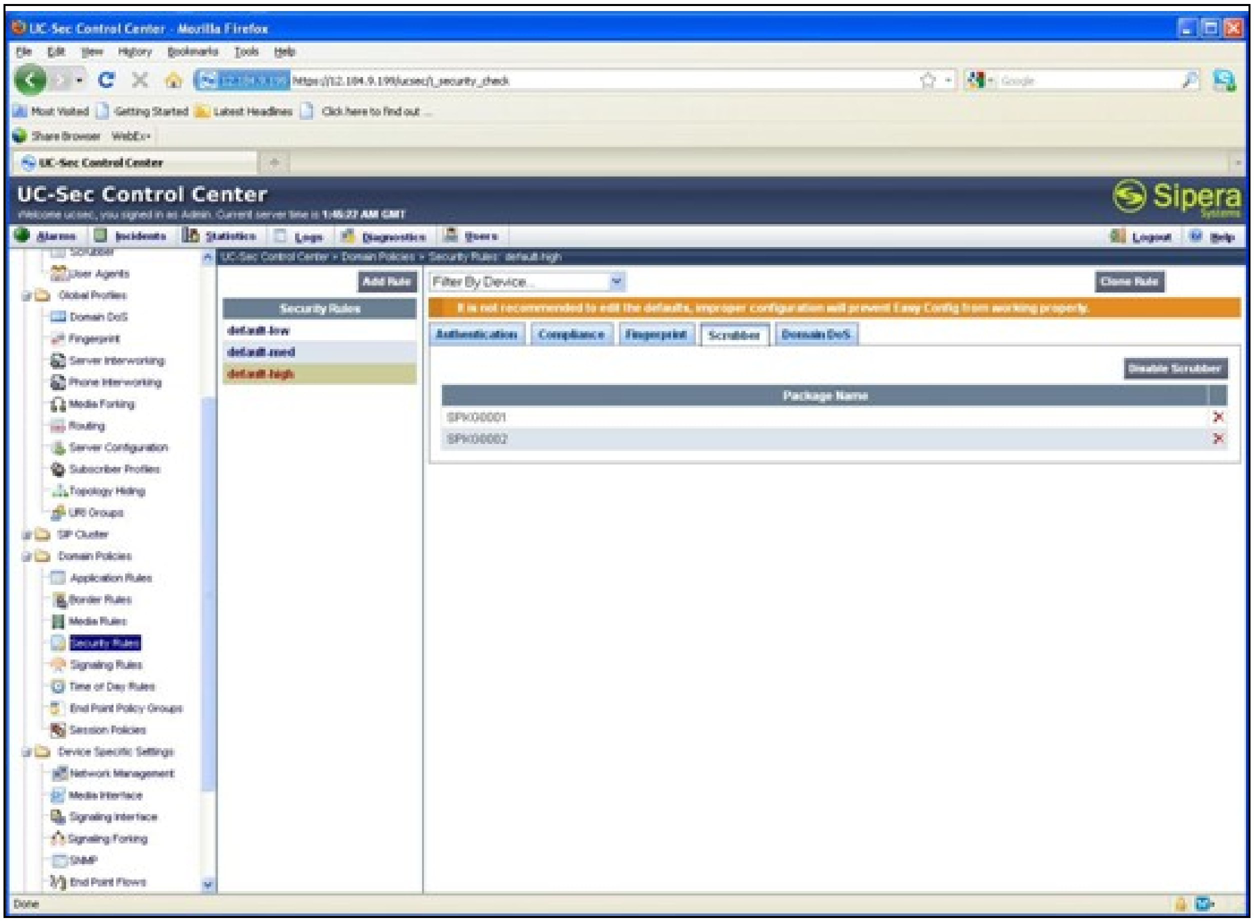
SIP Service	SIP Method	Destinations (per minute)	Action
Any	All	100	Block
Call	INVITE	80	Block
Registration	REGISTER	50	Block

Step 26: Security Feature - Scrubber

Below is the screen verifying that the scrubber is turned on. Navigate to **UC-Sec Control Center → Global Parameters → Scrubber → Packages.**

This screen is an example of how to configure scrubber feature.

For detailed information on the configuration of scrubber, please refer to UC-Sec administration guide in **Section 10, [9]** and **[10],** or contact Sipera Customer Support.



UC-Sec Control Center > Domain Policies > Security Rules: default-high

Security Rules
default-low
default-med
default-high

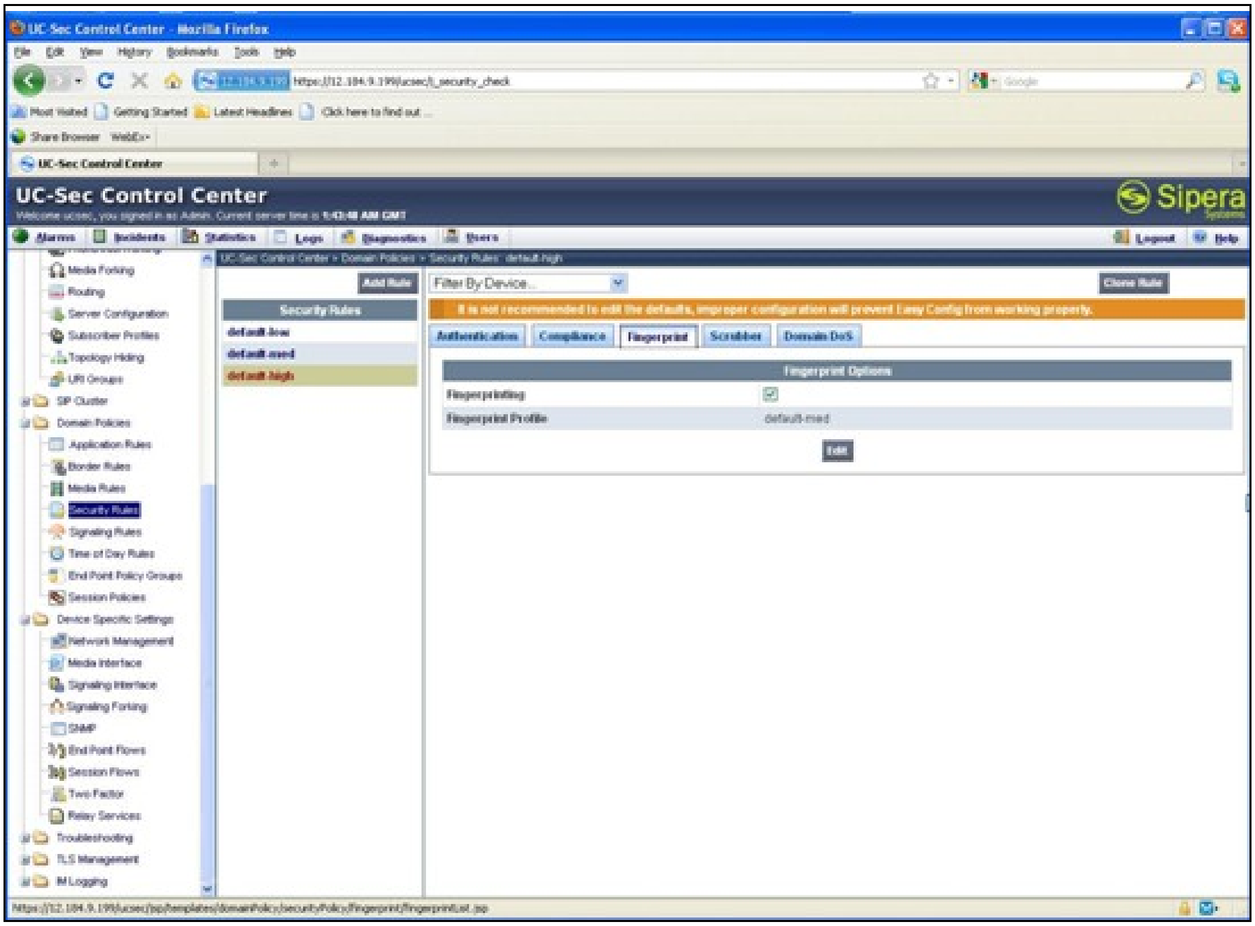
It is not recommended to edit the defaults, improper configuration will prevent Easy Config from working properly.

Package Name	
SPK00001	✕
SPK00002	✕

Step 27: Security Feature - FingerPrinting

Navigate to **UC-Sec Control Center → Domain Policies → Security Rules,** choose the appropriate security rule, and click on the **Fingerprint** tab. Select **Edit**, check the checkbox for **Fingerprinting**, and choose the appropriate fingerprint Profile. Click **Finish** (not shown).

For detailed information on the configuration of finger printing, please refer to UC-Sec administration guide in **Section 10, [9]** and **[10]**, or contact Sipera Customer Support.



UC-Sec Control Center > Domain Policies > Security Rules: default-high

It is not recommended to edit the defaults, improper configuration will prevent Easy Config from working properly.

Fingerprint Options	
Fingerprinting	☑
Fingerprint Profile	default-med

8. Verification Steps

The following steps may be used to verify the configuration:

- From the Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- From the Avaya Aura® System Manager Web administration interface, verify that all core endpoints are registered with Avaya Aura® Session Manage using the private IP address of Sipera UC-Sec. To view, navigate to **Elements → Session Manager → System Status → User Registrations.**
- Calls to core Avaya SIP endpoints registered through the Sipera from Avaya SIP, H.323, Digital, Analog phones registered directly to Session Manager and Communication Manager and PSTN users.
- Calls from core Avaya SIP endpoints registered through the Sipera to Avaya SIP, H.323, Digital, Analog phones registered directly to Session Manager and Communication Manager and PSTN users.
- Calls to core Avaya SIP endpoints registered through the Sipera from core Avaya SIP endpoints registered through the Sipera.
- From the Communication Manager SAT, use the **list trace tac** command to verify that the calls between remote users and endpoints at the main site are routed through the configured SIP trunks.

9. Conclusion

The Sipera Systems UC-Sec Secure Access Proxy for enterprise core users passed compliance testing. These Application Notes describe the procedures required to configure the Sipera Systems UC-Sec Appliance to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to support enterprise core users as shown in **Figure 1**.

10. Additional References

This section references the Avaya and Sipera documentation relevant to these Application Notes.

Product documentation for Avaya products may be found at http://support.avaya.com.

[1] *Installing and Configuring Avaya Aura® Session Manager, Doc ID 03-603473 Release 6.*

[2] *Administering Avaya Aura® Session Manager, Doc ID 03-603324, Release 6.0, June 2010*

[3] *Installing and Configuring Avaya Aura® Communication Manager, Doc ID 03-603558, Release 6.0 June, 2010*

[4] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.1, Document Number 16-300698.*

[5] *Modular Messaging Admin Guide Release 5.2 with Avaya MSS*

[6] *Avaya Aura® Communication Manager Messaging Installation and Initial Configuration.*

[7] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.1,* Document Number 16-300698.

[8] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.6,* Document Number 16-601944.

Product documentation for UC-Sec can be obtained from Sipera. Contact Sipera using the contact link at http://www.sipera.com.

[9] *UC-Sec Install Guide (102-5224-400v1.01).*

[10] *UC-Sec Administration Guide (010-5423-400v106).*

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.