Avaya Solution & Interoperability Test Lab

Application notes for SIPERA UC-Sec™ 4.0 Remote User Enablement Solution with Avaya™ Multimedia Communication System 5100 release 4.0 – Issue 1.0

Abstract

These Application Notes describe a solution comprised of Avaya™ Multimedia Communication System 5100 Rel. 4.0 and Sipera UC-Sec 4.0 Remote User Enablement Solution. The Sipera UC-Sec acts as a session border controller and enables secure communication between the MCS 5100 and its registered remote users. Multimedia Communication System 5100 SIP clients are able to place and receive calls between users with or without the UC-Sec. Telephony features such as three-way conference, transfers, presence, IM, and video, were executed.

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 provide detailed configurations of Avaya MCS 5100 rel. 4.0 and Sipera UC-Sec rel. 4.0 during the compatibility testing session. The Sipera UC-Sec rel 4.0 acts as Security Session Border Controller to allow or enable the MCS 5100's client to remotely connect MCS server in SIP environment.

1.1. Interoperability Compliance Testing

The focus of this interoperability compliance testing is to verify the authorize SIP clients (users) of MCS system are be able to communicate with each other through the Sipera UC-Sec securely within the MCS 5100 domain. The main objectives of the testing were to verify the Sipera UC-Sec represents the MCS clients/users successfully to:

- Register to the MCS 5100 domain.
- Perform basic call operation: DTMF transmission, voicemail with MWI notification, busy, hold.
- Redirect calls between users/clients/endpoints: blind/consultative transfers, call forward all calls, busy and no answer.
- Perform codec negotiation
- Perform conferencing: ad-hoc and meet-me conferencing.
- Perform the MCS multi-media functions: music on hold, meet-me conference, instant messaging, web collaboration, sim-ring, branding, present update, file transfer and video SIP calls

1.2. Support

For technical support on Sipera UC-Sec rel.4.0, please contact Sipera technical support at:

- Toll Free: (866) 861-3113
- Tel # : (214) 269-2424
- E-mail: support@sipera.com

2. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance testing event between the Avaya MCS 5100 rel.4.0 and the Sipera UC-Sec rel.4.0.

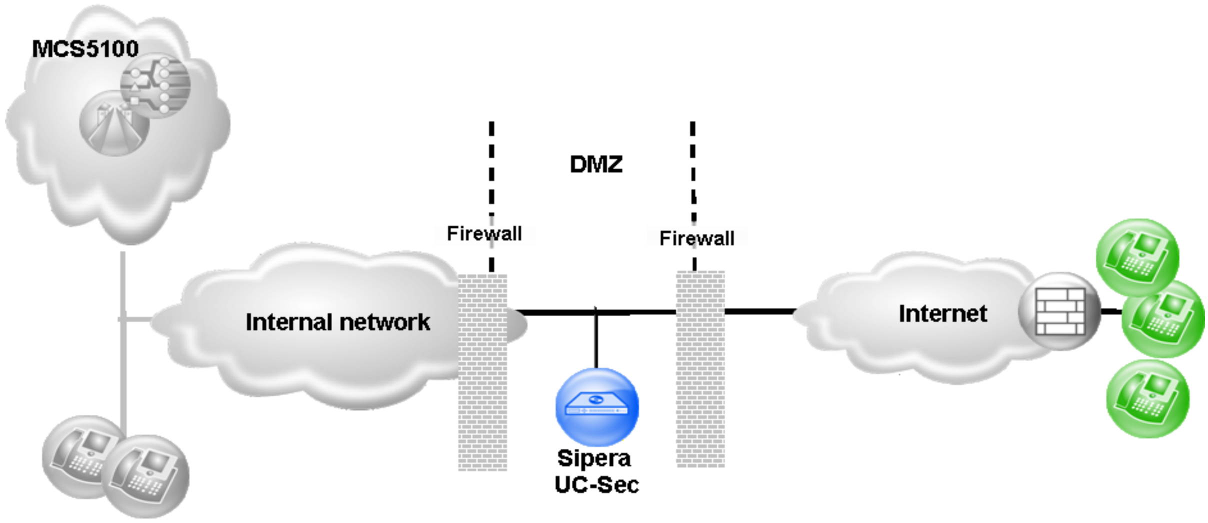


Figure 1: Lab Diagram

The following assumptions were made for this lab test configuration:

1. SIP and RTP are always proxied (anchored) through Sipera UC-Sec/.
2. NOTIFY message that carries the provisioning server's HTTP URL uses a domain name (instead of an IP address). Sipera UC-Sec DOES NOT modify this URL and passes it along to the external users.
3. External users resolve this domain name which maps to the public IP of the customer's internet-facing firewall (FW). This FW is then configured to map HTTP traffic back into the Application Server' internal Web (provisioning) server.
4. For Web collaboration related HTTP traffic, Sipera modifies the HTTP URL sent as part of an encrypted IM message (MESSAGE method). Sipera decrypts the IM message, modifies the URL to use Sipera's external interface's IP address (public IP).
5. When external users receive this Web push URL, their internet browser connects to Sipera's public IP. Configuration on Sipera UC-Sec proxies these HTTP messages over to an internal Web server that hosts the collaboration application (IBM Web Dialog application server).
6. The PC client's Raider.ini was modified to point to the public IP/hostname of the customer's internet-facing FW for allowing the remote users to use their Web-based SIP client.

3. Equipment and Software Validated

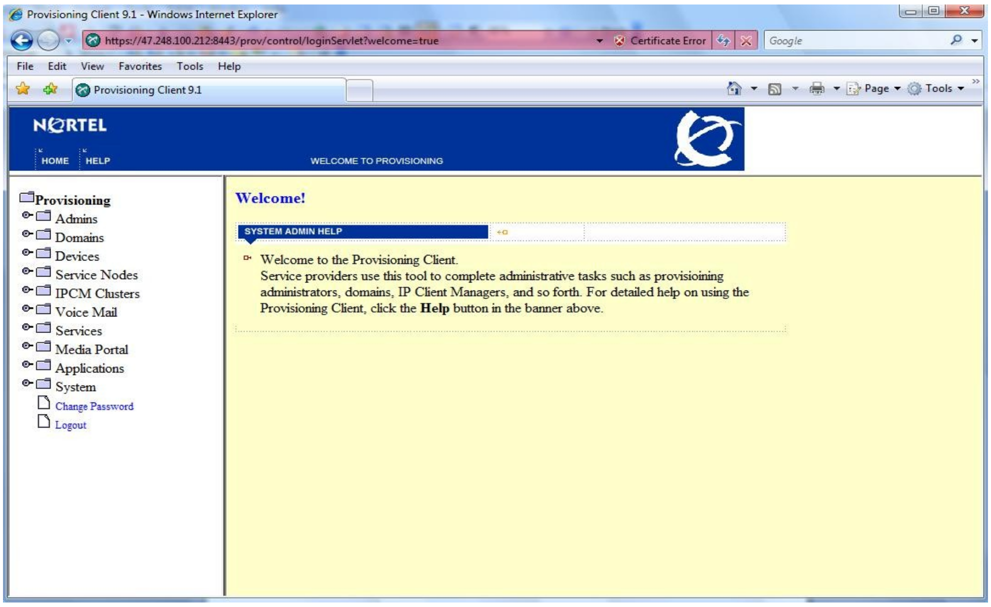
System	Software/Loadware Version
MCS 5100	• MCP version: MCP_9.1.0.0_2009-04-29-0711 • MAS: 9.1.478
Multimedia PC Client	• 5.0.530
11xx SIP client (Sigma)	• 02.02.16.00
Sipera UC-Sec	• 4.0

4. Configure the Avaya MCS 5100

This section describes the steps to configure SIP domain (domain, service package, users).

4.1. Launch MCS Provisioning Web Portal

Using IE to launch web MCS Provisioning portal at http://IP_Addrress_of_MCS_core/prov
Default username/password: admin/admin.



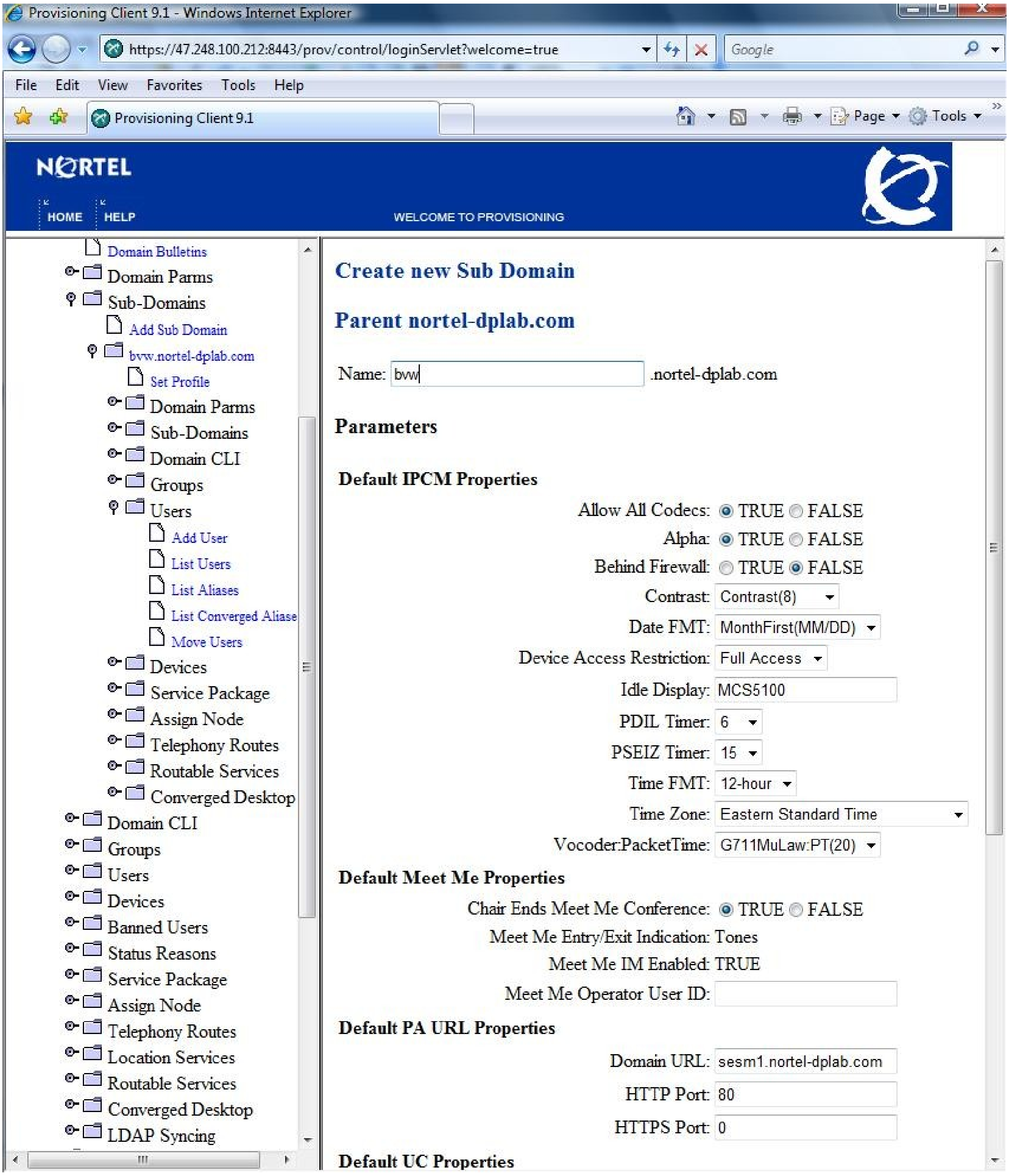
Welcome to the Provisioning Client.
Service providers use this tool to complete administrative tasks such as provisioining administrators, domains, IP Client Managers, and so forth. For detailed help on using the Provisioning Client, click the **Help** button in the banner above.

Figure 2: Provisioning Home Page

4.2. Create a new sub domain

The fields in the following screens show the values used for the testing.

Create a new sub domain as shown in Figure 3, e.g., bvw.
For the Default PA URL Properties, enter the Domain URL which is used to configure a host on the DNS server. Because Sipera UC-Sec does not support HTTPS proxy, the HTTPS Port must be set to 0. Other fields are at default values.



Create new Sub Domain

Parent nortel-dplab.com

Name: bvw .nortel-dplab.com

Parameters

Default IPCM Properties

Allow All Codecs: ● TRUE ○ FALSE

Alpha: ● TRUE ○ FALSE

Behind Firewall: ○ TRUE ● FALSE

Contrast: Contrast(8)

Date FMT: MonthFirst(MM/DD)

Device Access Restriction: Full Access

Idle Display: MCS5100

PDIL Timer: 6

PSEIZ Timer: 15

Time FMT: 12-hour

Time Zone: Eastern Standard Time

Vocoder:PacketTime: G711MuLaw:PT(20)

Default Meet Me Properties

Chair Ends Meet Me Conference: ● TRUE ○ FALSE

Meet Me Entry/Exit Indication: Tones

Meet Me IM Enabled: TRUE

Meet Me Operator User ID:

Default PA URL Properties

Domain URL: sesm1.nortel-dplab.com

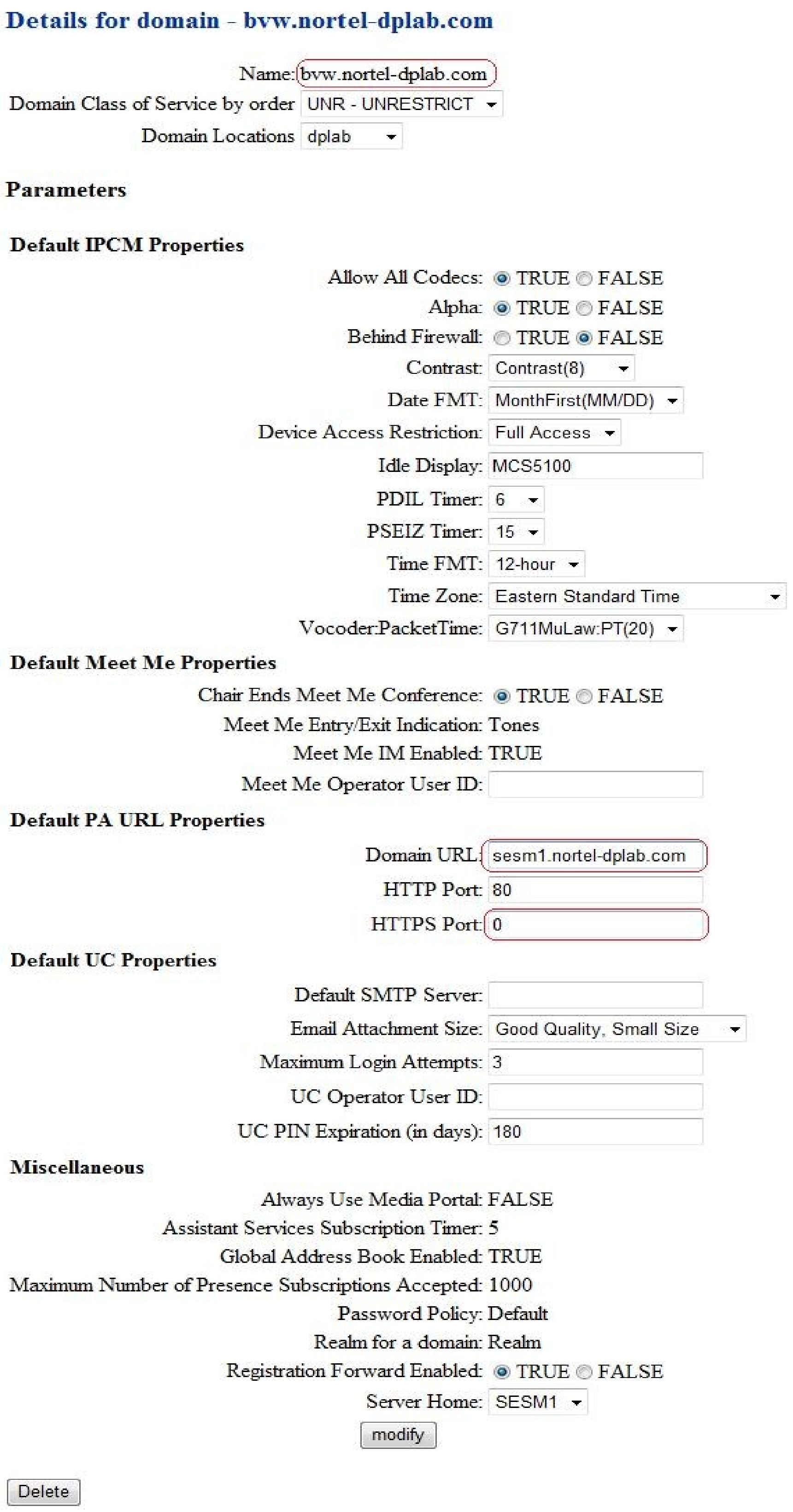
HTTP Port: 80

HTTPS Port: 0

Default UC Properties

Figure 3: Adding Domain Page

After creating the sub-domain, the user can view their created sub-domain configuration by choosing the sub-domain name, i.e., bvw.nortel-dplab.com



Details for domain - bvw.nortel-dplab.com

Name:	bvw.nortel-dplab.com
Domain Class of Service by order	UNR - UNRESTRICT
Domain Locations	dplab

Parameters

Default IPCM Properties

Allow All Codecs:	● TRUE ○ FALSE
Alpha:	● TRUE ○ FALSE
Behind Firewall:	○ TRUE ● FALSE
Contrast:	Contrast(8)
Date FMT:	MonthFirst(MM/DD)
Device Access Restriction:	Full Access
Idle Display:	MCS5100
PDIL Timer:	6
PSEIZ Timer:	15
Time FMT:	12-hour
Time Zone:	Eastern Standard Time
Vocoder:PacketTime:	G711MuLaw:PT(20)

Default Meet Me Properties

Chair Ends Meet Me Conference:	● TRUE ○ FALSE
Meet Me Entry/Exit Indication:	Tones
Meet Me IM Enabled:	TRUE
Meet Me Operator User ID:	

Default PA URL Properties

Domain URL:	sesm1.nortel-dplab.com
HTTP Port:	80
HTTPS Port:	0

Default UC Properties

Default SMTP Server:	
Email Attachment Size:	Good Quality, Small Size
Maximum Login Attempts:	3
UC Operator User ID:	
UC PIN Expiration (in days):	180

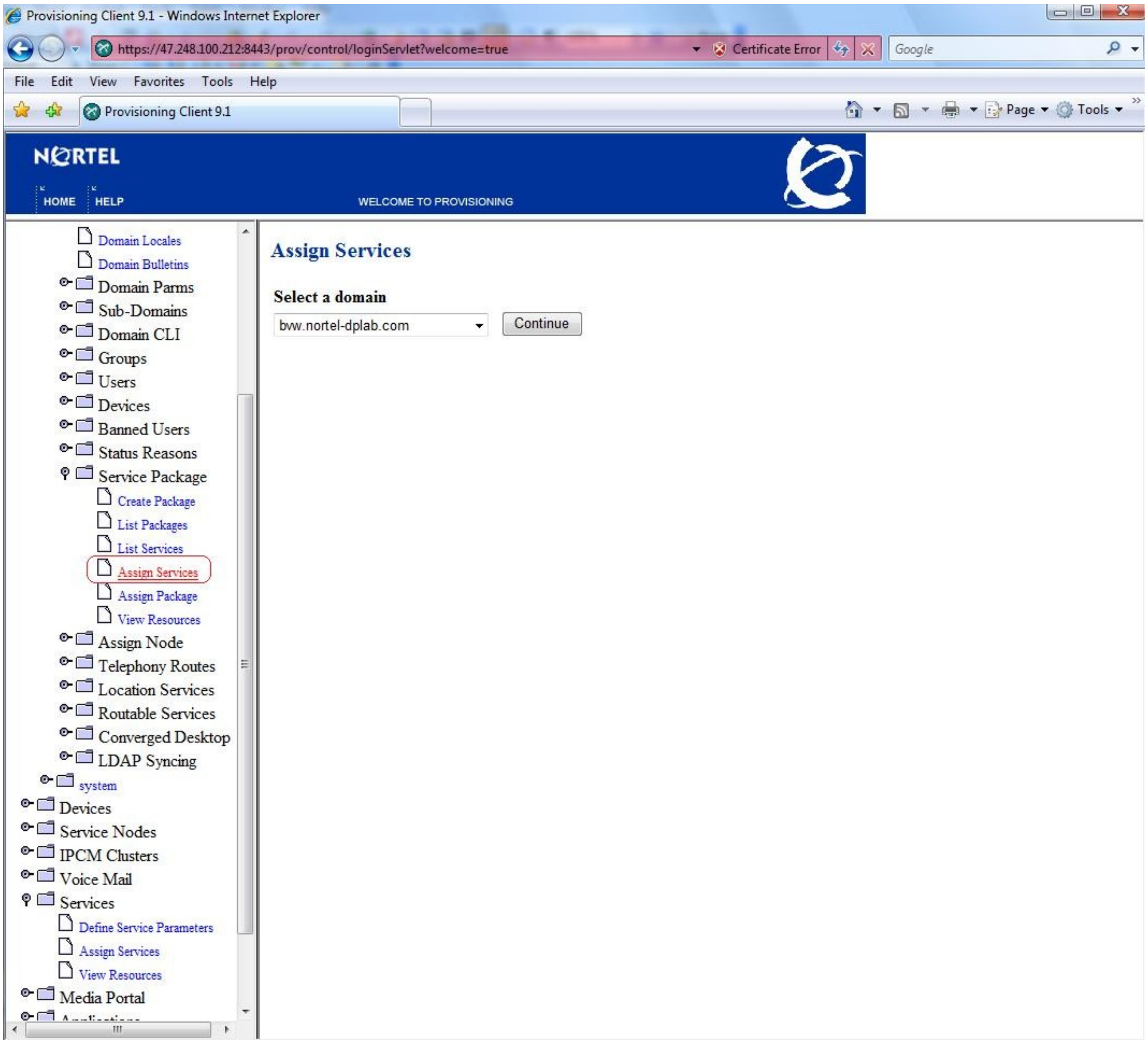
Miscellaneous

Always Use Media Portal:	FALSE
Assistant Services Subscription Timer:	5
Global Address Book Enabled:	TRUE
Maximum Number of Presence Subscriptions Accepted:	1000
Password Policy:	Default
Realm for a domain:	Realm
Registration Forward Enabled:	● TRUE ○ FALSE
Server Home:	SESM1

Figure 4: Detail Added Sub Domain

4.3. Assign service to sub domain

To assign a service select “Assign Services”, select the domain, and click continue.



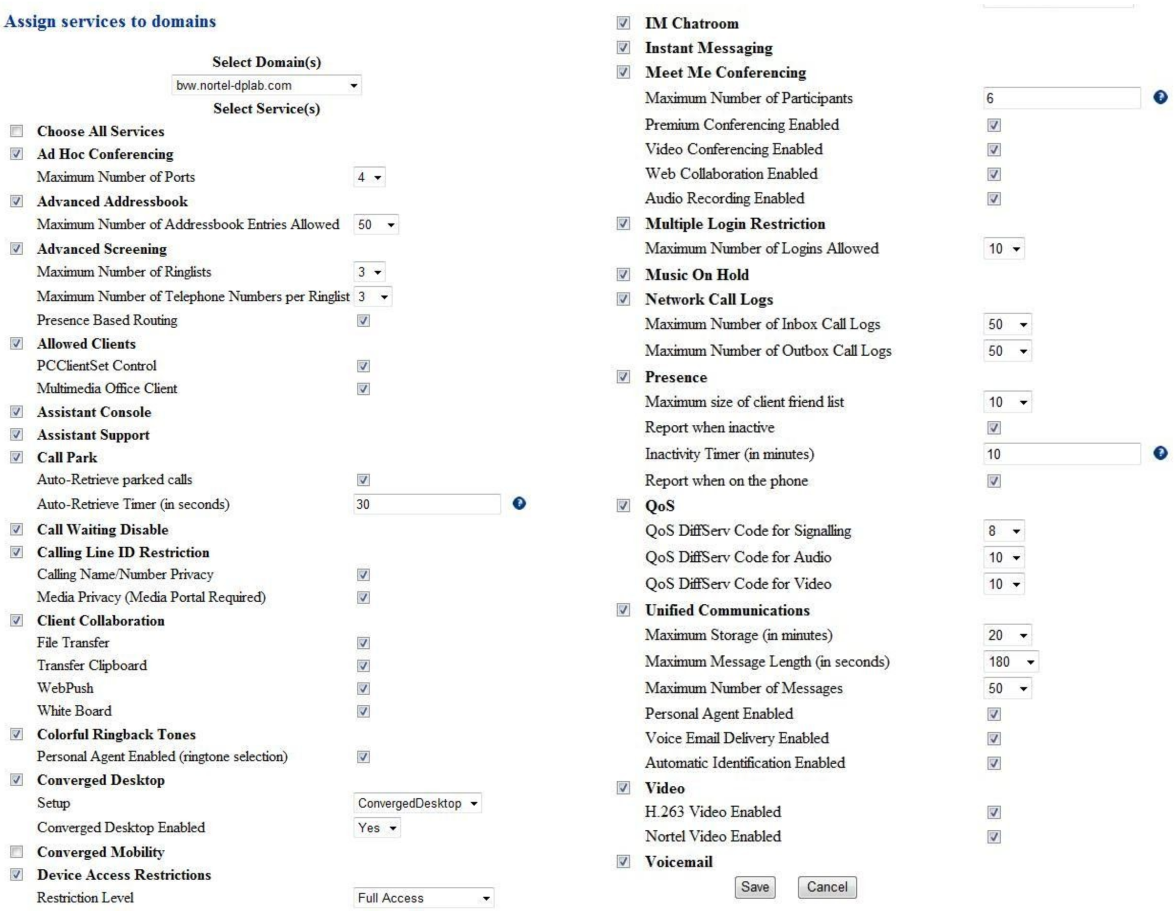
Assign Services

Select a domain

bvw.nortel-dplab.com ▾ Continue

Figure 5: Assign Services to Sub Domain

In Figure 6, choose the appropriate services for the domain and click save. The values shown below were used during testing.



Assign services to domains

Select Domain(s)

bvw.nortel-dplab.com ▾

Select Service(s)

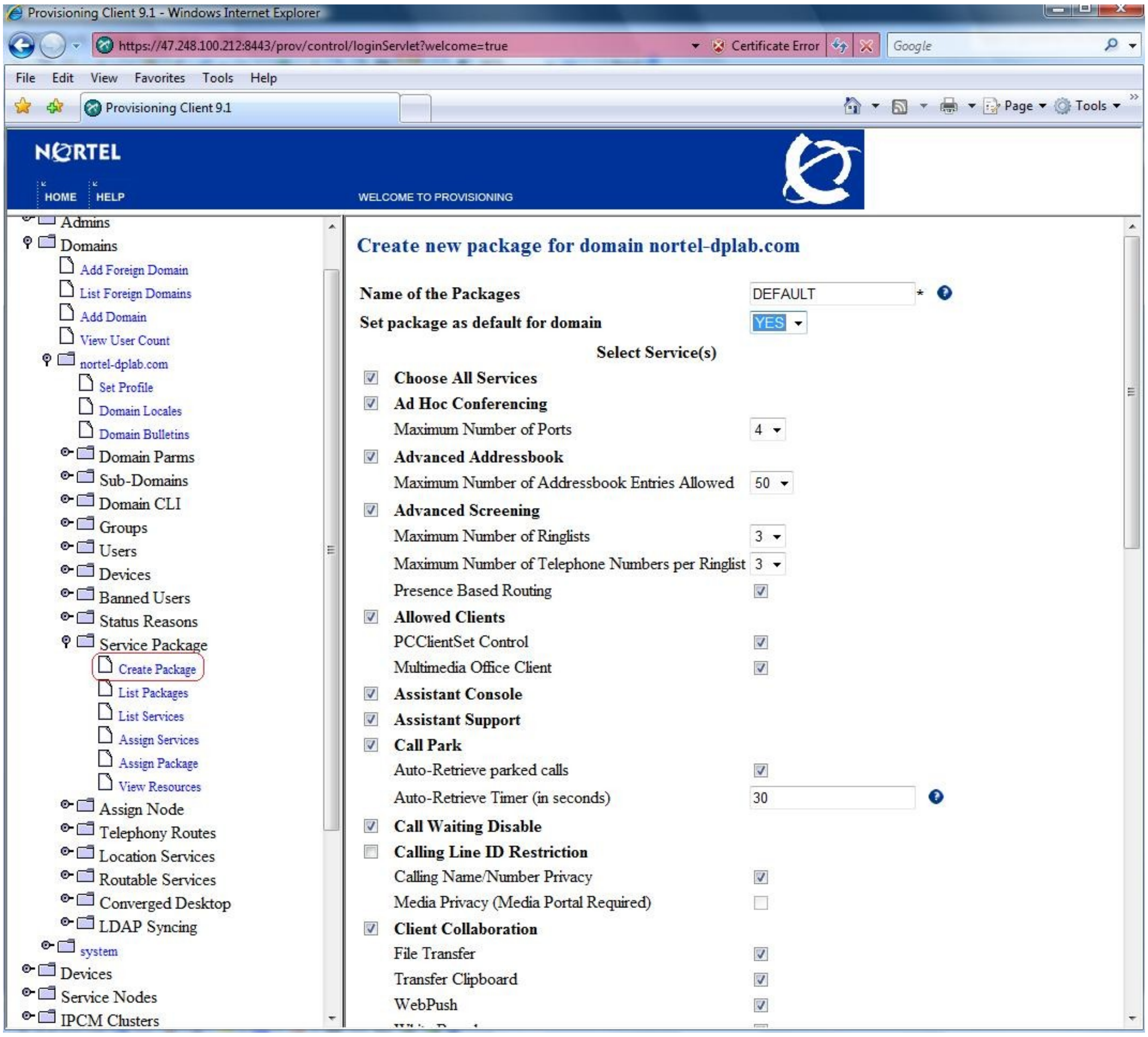
☐	**Choose All Services**	
☑	**Ad Hoc Conferencing**	
	Maximum Number of Ports	4 ▾
☑	**Advanced Addressbook**	
	Maximum Number of Addressbook Entries Allowed	50 ▾
☑	**Advanced Screening**	
	Maximum Number of Ringlists	3 ▾
	Maximum Number of Telephone Numbers per Ringlist	3 ▾
	Presence Based Routing	☑
☑	**Allowed Clients**	
	PCClientSet Control	☑
	Multimedia Office Client	☑
☑	**Assistant Console**	
☑	**Assistant Support**	
☑	**Call Park**	
	Auto-Retrieve parked calls	☑
	Auto-Retrieve Timer (in seconds)	30
☑	**Call Waiting Disable**	
☑	**Calling Line ID Restriction**	
	Calling Name/Number Privacy	☑
	Media Privacy (Media Portal Required)	☑
☑	**Client Collaboration**	
	File Transfer	☑
	Transfer Clipboard	☑
	WebPush	☑
	White Board	☑
☑	**Colorful Ringback Tones**	
	Personal Agent Enabled (ringtone selection)	☑
☑	**Converged Desktop**	
	Setup	ConvergedDesktop ▾
	Converged Desktop Enabled	Yes ▾
☐	**Converged Mobility**	
☑	**Device Access Restrictions**	
	Restriction Level	Full Access ▾

☑	**IM Chatroom**	
☑	**Instant Messaging**	
☑	**Meet Me Conferencing**	
	Maximum Number of Participants	6
	Premium Conferencing Enabled	☑
	Video Conferencing Enabled	☑
	Web Collaboration Enabled	☑
	Audio Recording Enabled	☑
☑	**Multiple Login Restriction**	
	Maximum Number of Logins Allowed	10 ▾
☑	**Music On Hold**	
☑	**Network Call Logs**	
	Maximum Number of Inbox Call Logs	50 ▾
	Maximum Number of Outbox Call Logs	50 ▾
☑	**Presence**	
	Maximum size of client friend list	10 ▾
	Report when inactive	☑
	Inactivity Timer (in minutes)	10
	Report when on the phone	☑
☑	**QoS**	
	QoS DiffServ Code for Signalling	8 ▾
	QoS DiffServ Code for Audio	10 ▾
	QoS DiffServ Code for Video	10 ▾
☑	**Unified Communications**	
	Maximum Storage (in minutes)	20 ▾
	Maximum Message Length (in seconds)	180 ▾
	Maximum Number of Messages	50 ▾
	Personal Agent Enabled	☑
	Voice Email Delivery Enabled	☑
	Automatic Identification Enabled	☑
☑	**Video**	
	H.263 Video Enabled	☑
	Nortel Video Enabled	☑
☑	**Voicemail**	

Figure 6: Detail Assigned Services

4.4. Create Service Package for users

Select the appropriate package. The DEFAULT package was created as the base package for this test.



Create new package for domain nortel-dplab.com

Name of the Packages: DEFAULT *

Set package as default for domain: YES

Select Service(s)

☑ Choose All Services

☑ Ad Hoc Conferencing

Maximum Number of Ports: 4

☑ Advanced Addressbook

Maximum Number of Addressbook Entries Allowed: 50

☑ Advanced Screening

Maximum Number of Ringlists: 3

Maximum Number of Telephone Numbers per Ringlist: 3

Presence Based Routing ☑

☑ Allowed Clients

PCClientSet Control ☑

Multimedia Office Client ☑

☑ Assistant Console

☑ Assistant Support

☑ Call Park

Auto-Retrieve parked calls ☑

Auto-Retrieve Timer (in seconds): 30

☑ Call Waiting Disable

□ Calling Line ID Restriction

Calling Name/Number Privacy ☑

Media Privacy (Media Portal Required) □

☑ Client Collaboration

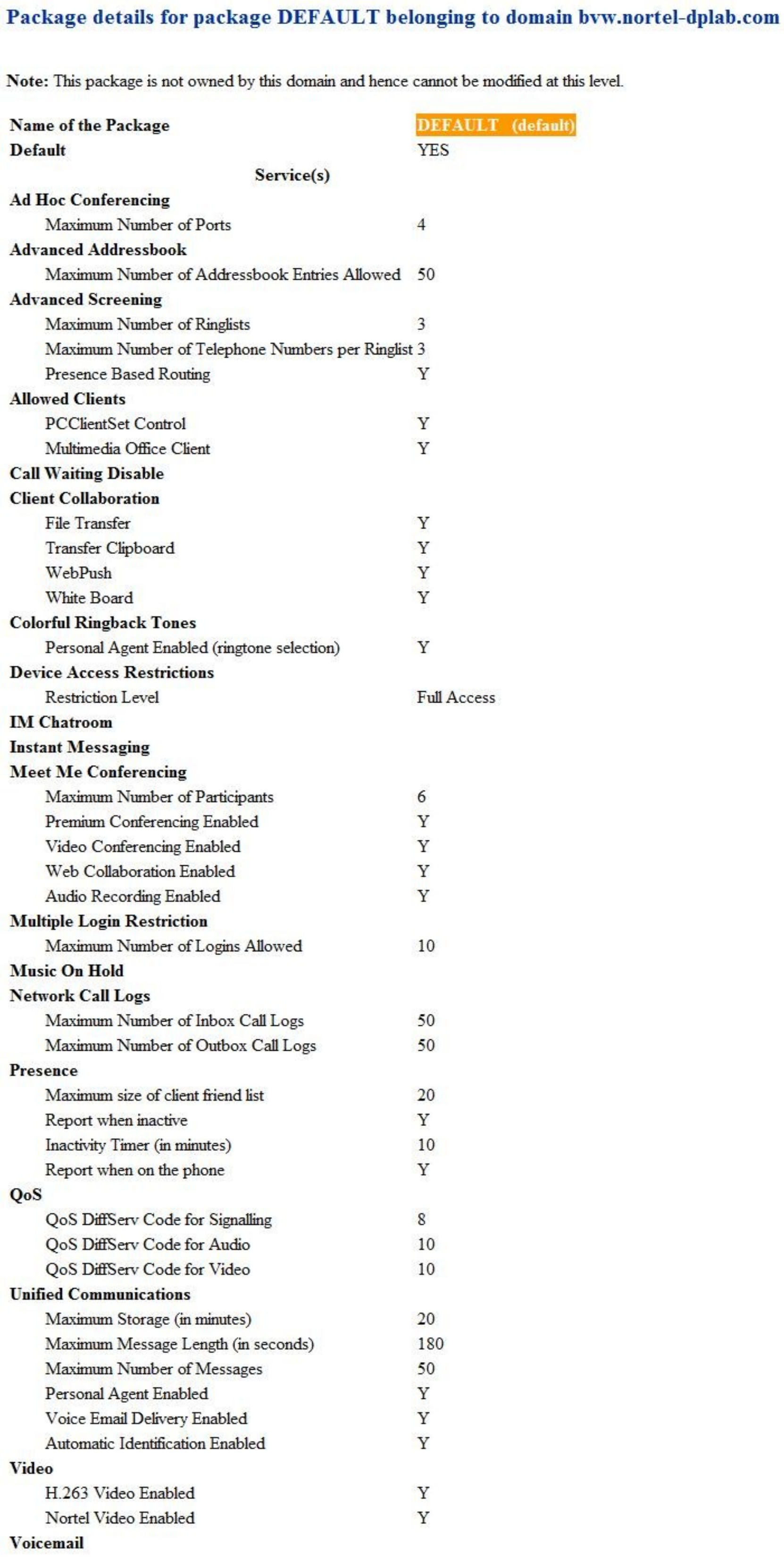
File Transfer ☑

Transfer Clipboard ☑

WebPush ☑

Figure 7: Creating Service Package Page

Figure 8 shows the details of the service package for the users in the domain bvw.nortel-dplab.com



Package details for package DEFAULT belonging to domain bvw.nortel-dplab.com

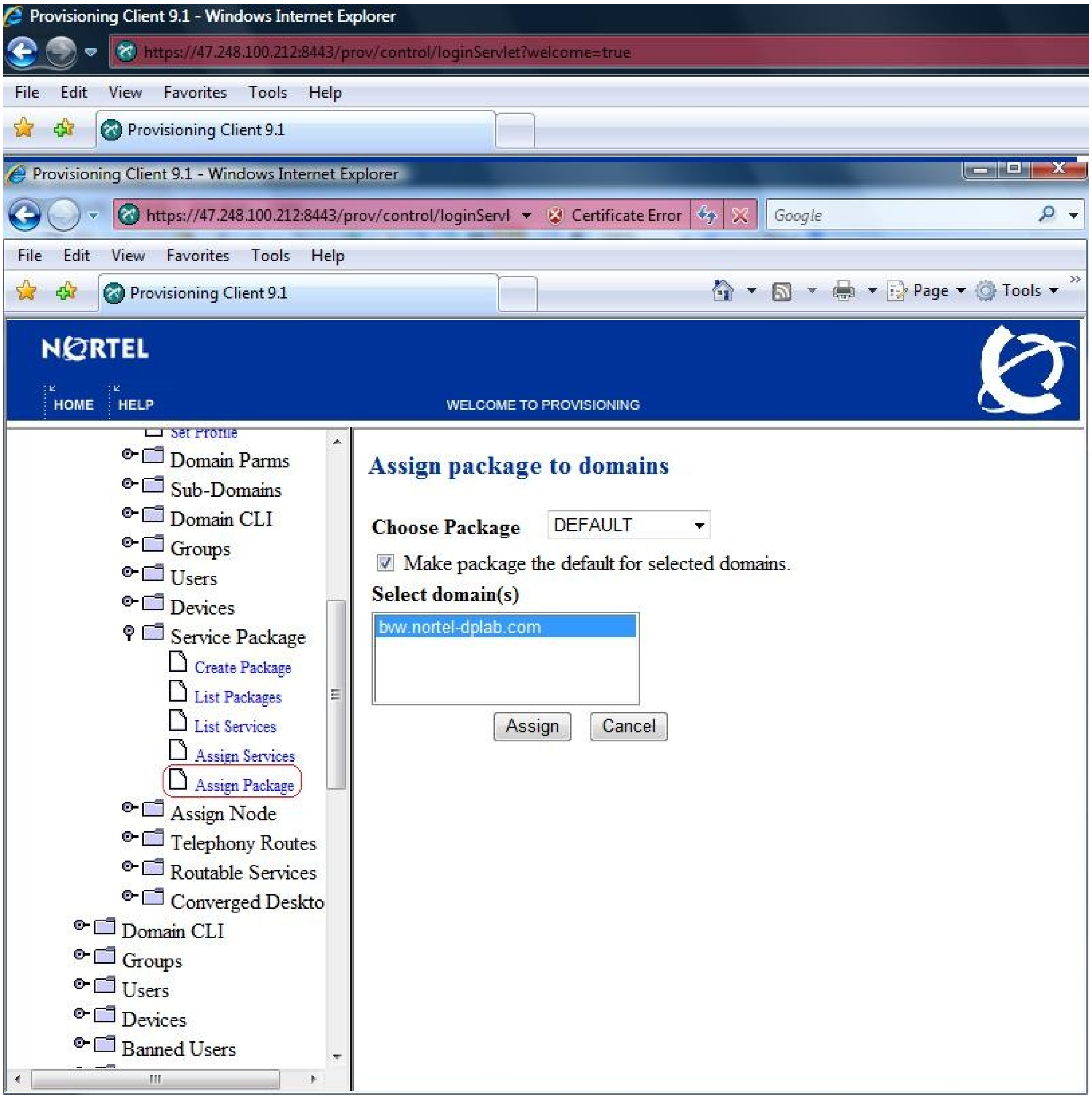
Note: This package is not owned by this domain and hence cannot be modified at this level.

Name of the Package	DEFAULT (default)
Default	YES
Service(s)	
Ad Hoc Conferencing	
Maximum Number of Ports	4
Advanced Addressbook	
Maximum Number of Addressbook Entries Allowed	50
Advanced Screening	
Maximum Number of Ringlists	3
Maximum Number of Telephone Numbers per Ringlist	3
Presence Based Routing	Y
Allowed Clients	
PCClientSet Control	Y
Multimedia Office Client	Y
Call Waiting Disable	
Client Collaboration	
File Transfer	Y
Transfer Clipboard	Y
WebPush	Y
White Board	Y
Colorful Ringback Tones	
Personal Agent Enabled (ringtone selection)	Y
Device Access Restrictions	
Restriction Level	Full Access
IM Chatroom	
Instant Messaging	
Meet Me Conferencing	
Maximum Number of Participants	6
Premium Conferencing Enabled	Y
Video Conferencing Enabled	Y
Web Collaboration Enabled	Y
Audio Recording Enabled	Y
Multiple Login Restriction	
Maximum Number of Logins Allowed	10
Music On Hold	
Network Call Logs	
Maximum Number of Inbox Call Logs	50
Maximum Number of Outbox Call Logs	50
Presence	
Maximum size of client friend list	20
Report when inactive	Y
Inactivity Timer (in minutes)	10
Report when on the phone	Y
QoS	
QoS DiffServ Code for Signalling	8
QoS DiffServ Code for Audio	10
QoS DiffServ Code for Video	10
Unified Communications	
Maximum Storage (in minutes)	20
Maximum Message Length (in seconds)	180
Maximum Number of Messages	50
Personal Agent Enabled	Y
Voice Email Delivery Enabled	Y
Automatic Identification Enabled	Y
Video	
H.263 Video Enabled	Y
Nortel Video Enabled	Y
Voicemail	

Figure 8: Detail Service Package Page

4.5. Assign Service Package to domains

Assign a service package to the domain as shown in Figure 9.



Assign package to domains

Choose Package DEFAULT

☑ Make package the default for selected domains.

Select domain(s)

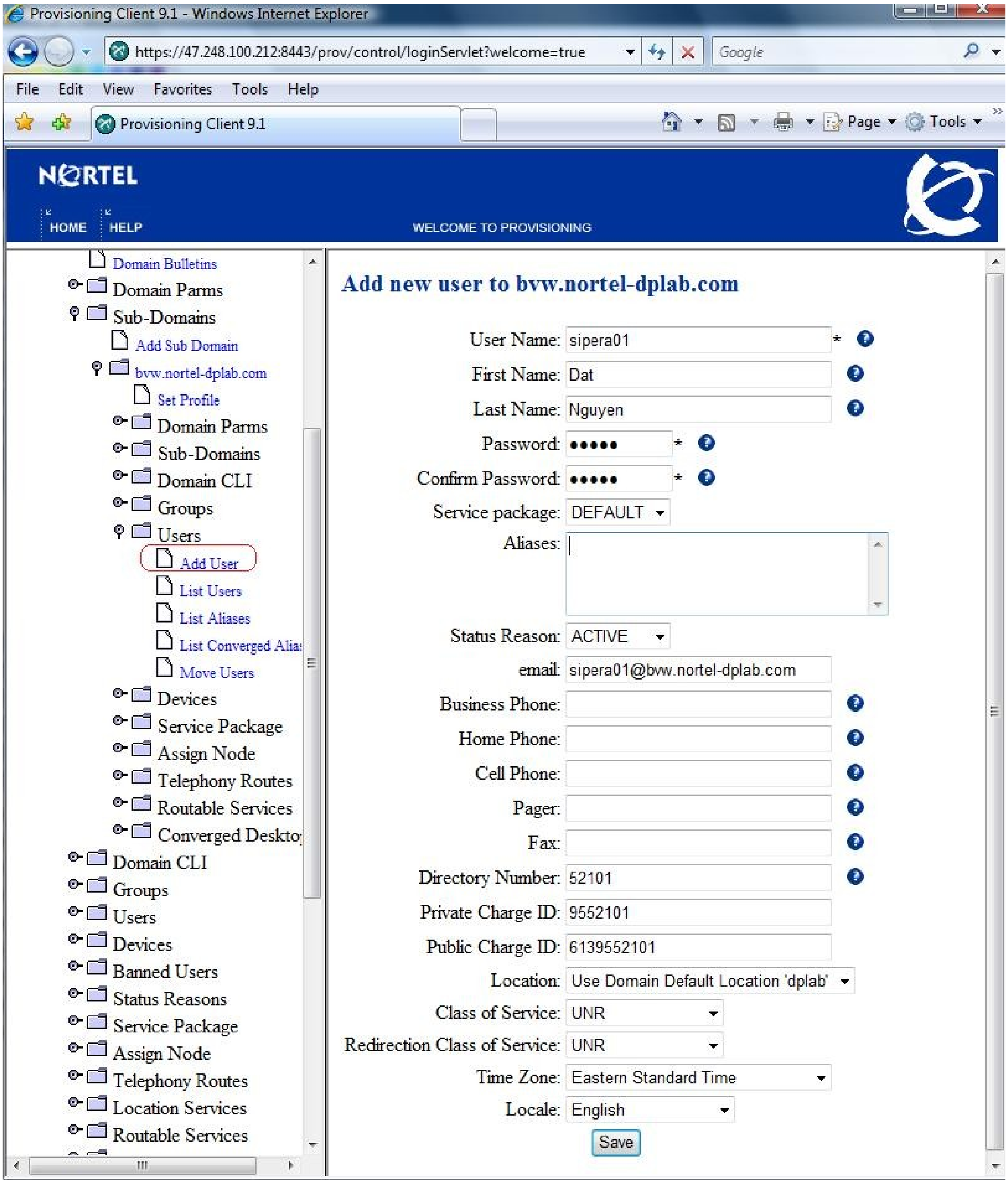
bvw.nortel-dplab.com

Assign Cancel

Figure 9: Assign package to Domains Page

4.6. Add a user

Add a user(s) to the domain of bvw.nortel-dplab.com as shown in Figure 10. The values shown were assigned and used during the testing.



Add new user to bvw.nortel-dplab.com

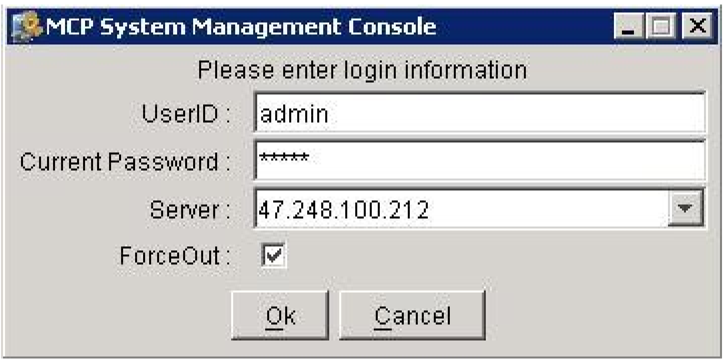
User Name:	sipera01 *
First Name:	Dat
Last Name:	Nguyen
Password:	●●●●● *
Confirm Password:	●●●●● *
Service package:	DEFAULT
Aliases:	
Status Reason:	ACTIVE
email:	sipera01@bvw.nortel-dplab.com
Business Phone:	
Home Phone:	
Cell Phone:	
Pager:	
Fax:	
Directory Number:	52101
Private Charge ID:	9552101
Public Charge ID:	6139552101
Location:	Use Domain Default Location 'dplab'
Class of Service:	UNR
Redirection Class of Service:	UNR
Time Zone:	Eastern Standard Time
Locale:	English

Save

Figure 10: Add User Page

4.7. Launch MCS 5100 MCP Console

The MCP System Management Console is used to manage all network data and network elements. Using IE to launch http://IP_Addrress_of_MCS_core:12120 and then click “Launch MCP System Management Console”.



MCP System Management Console

Please enter login information

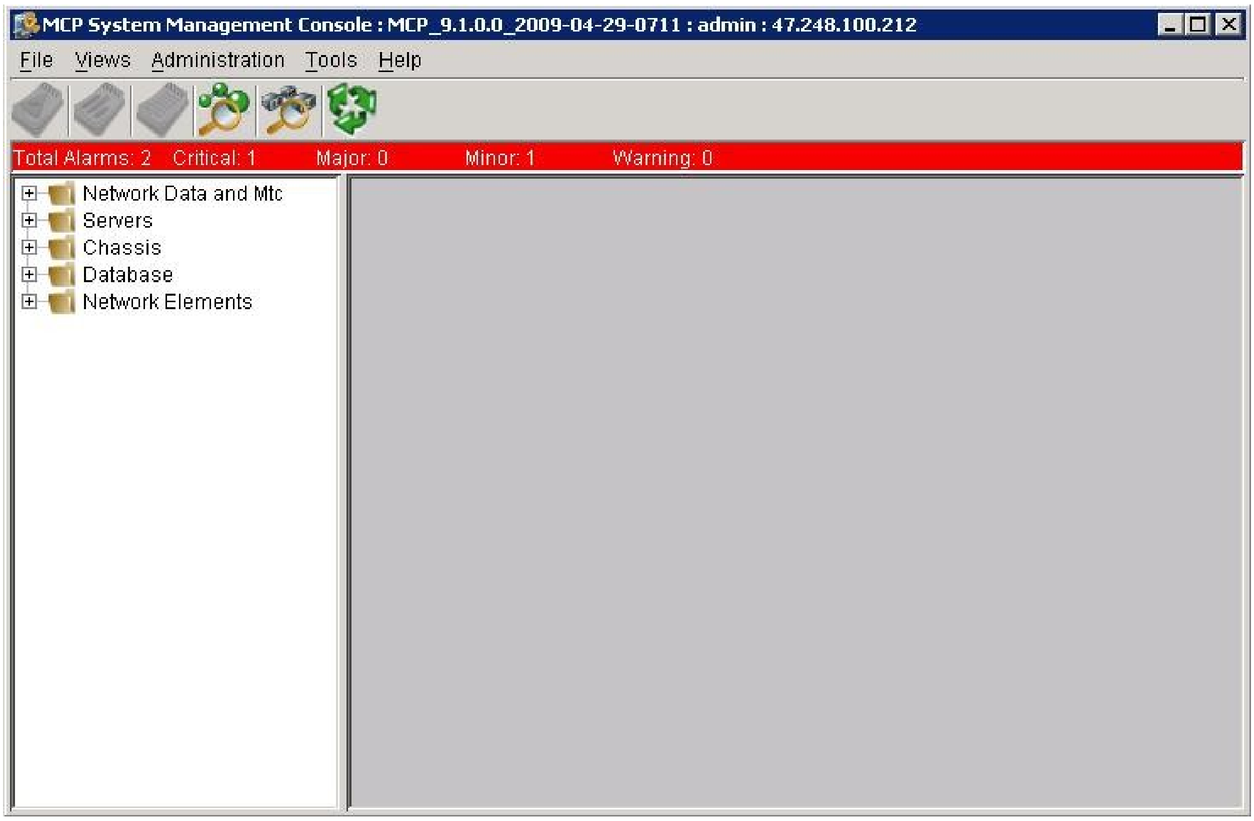
UserID : admin

Current Password : *****

Server : 47.248.100.212

ForceOut : ☑

Figure 11: MCP Console Login



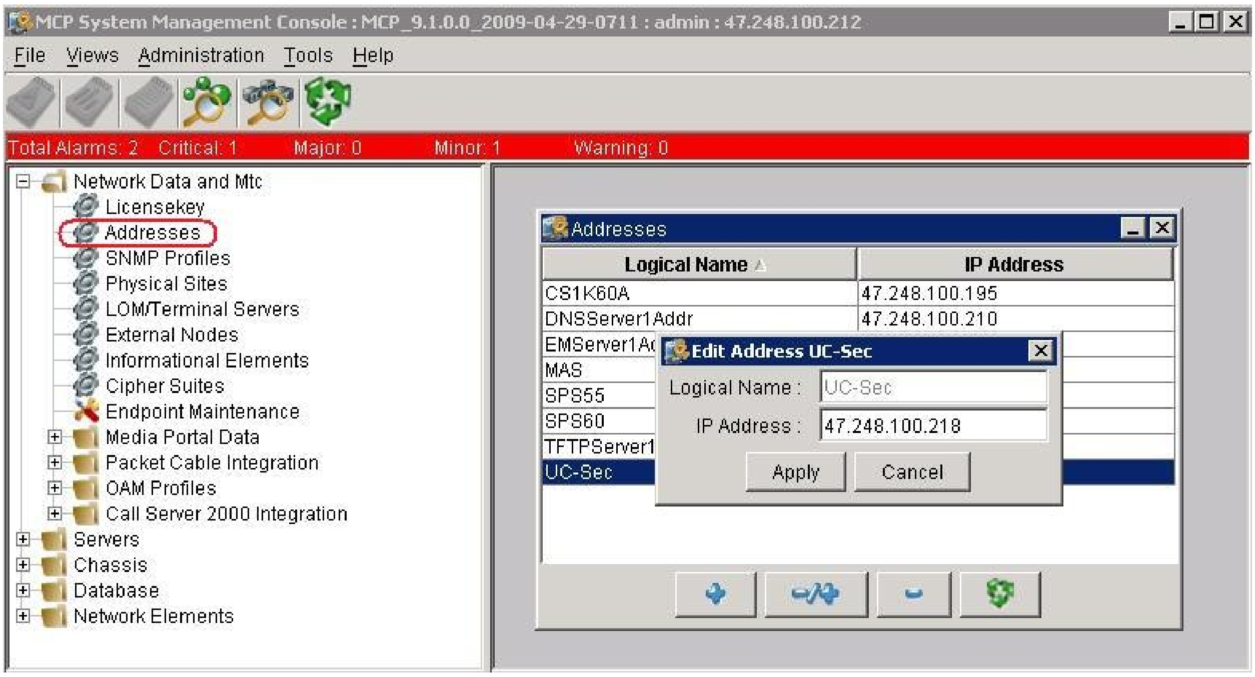
MCP System Management Console : MCP_9.1.0.0_2009-04-29-0711 : admin : 47.248.100.212

Total Alarms: 2 Critical: 1 Major: 0 Minor: 1 Warning: 0

Figure 12: MCP Console Window

4.8. Add Sipera UC-Sec IP address to Addresses list

Add the UC-Sec IP address as shown in Figure 13.



Logical Name	IP Address
CS1K60A	47.248.100.195
DNSServer1Addr	47.248.100.210
EMServer1A(	
MAS	
SPS55	
SPS60	
TFTPServer1	
UC-Sec	

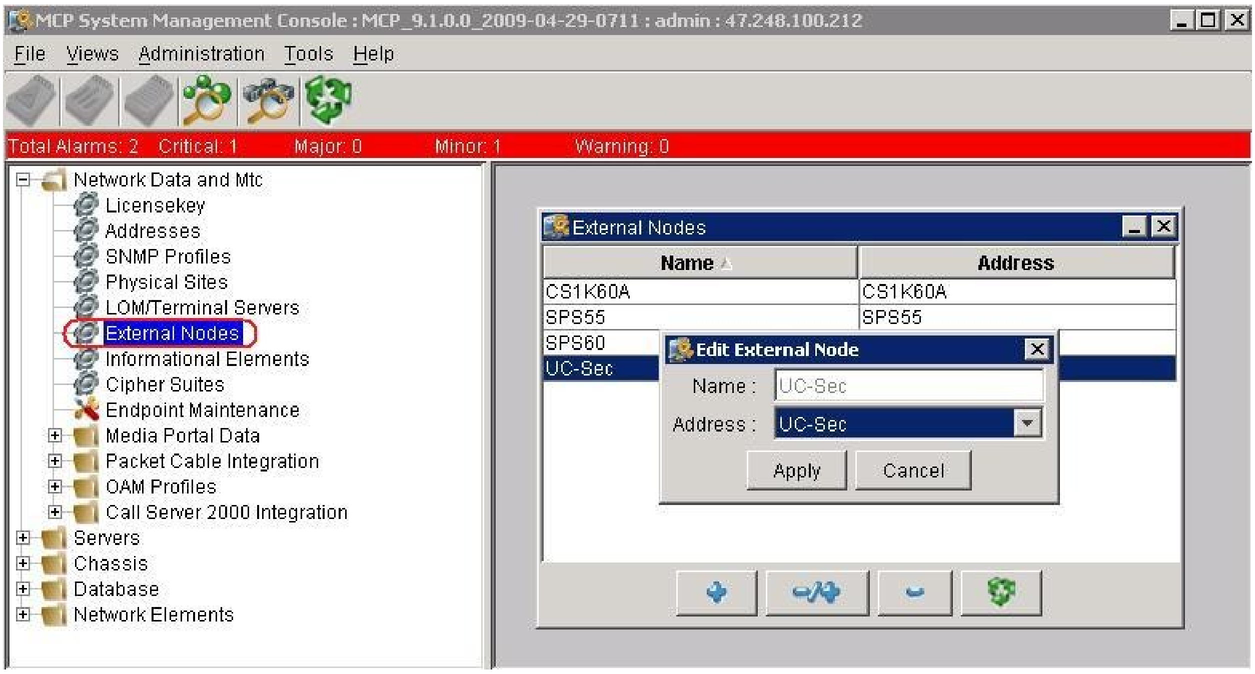
Logical Name : UC-Sec

IP Address : 47.248.100.218

Figure 13: Adding Sipera UC-Sec IP address

4.9. Add Sipera UC-Sec as an External Node

Add the UC-Sec as an external node as shown in Figure 14.



Name	Address
CS1K60A	CS1K60A
SPS55	SPS55
SPS60	
UC-Sec	

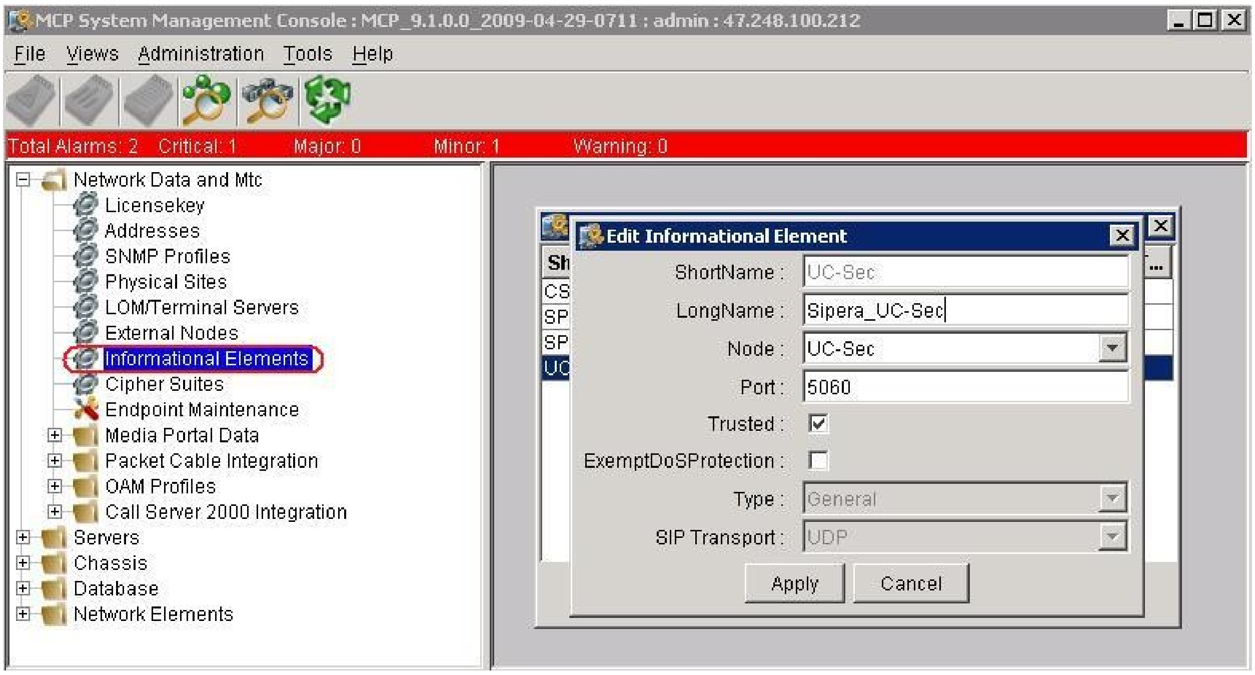
Name : UC-Sec

Address : UC-Sec

Figure 14: Adding Sipera UC-Sec as an external node

4.10. Configure Sipera UC-Sec as a trusted node

Add the UC-Sec as a trusted node as shown in Figure 15. Sipera UC-Sec should be configured as a trusted node to eliminate the unnecessary authentication messages back and forth between UC-Sec and MCS 5100.



MCP System Management Console : MCP_9.1.0.0_2009-04-29-0711 : admin : 47.248.100.212

Total Alarms: 2 Critical: 1 Major: 0 Minor: 1 Warning: 0

Edit Informational Element

ShortName : UC-Sec

LongName : Sipera_UC-Sec

Node : UC-Sec

Port : 5060

Trusted : ☑

ExemptDoSProtection : □

Type : General

SIP Transport : UDP

Figure 15: Configuring Sipera UC-Sec as a trusted node

5. Configure the Sipera UC-Sec

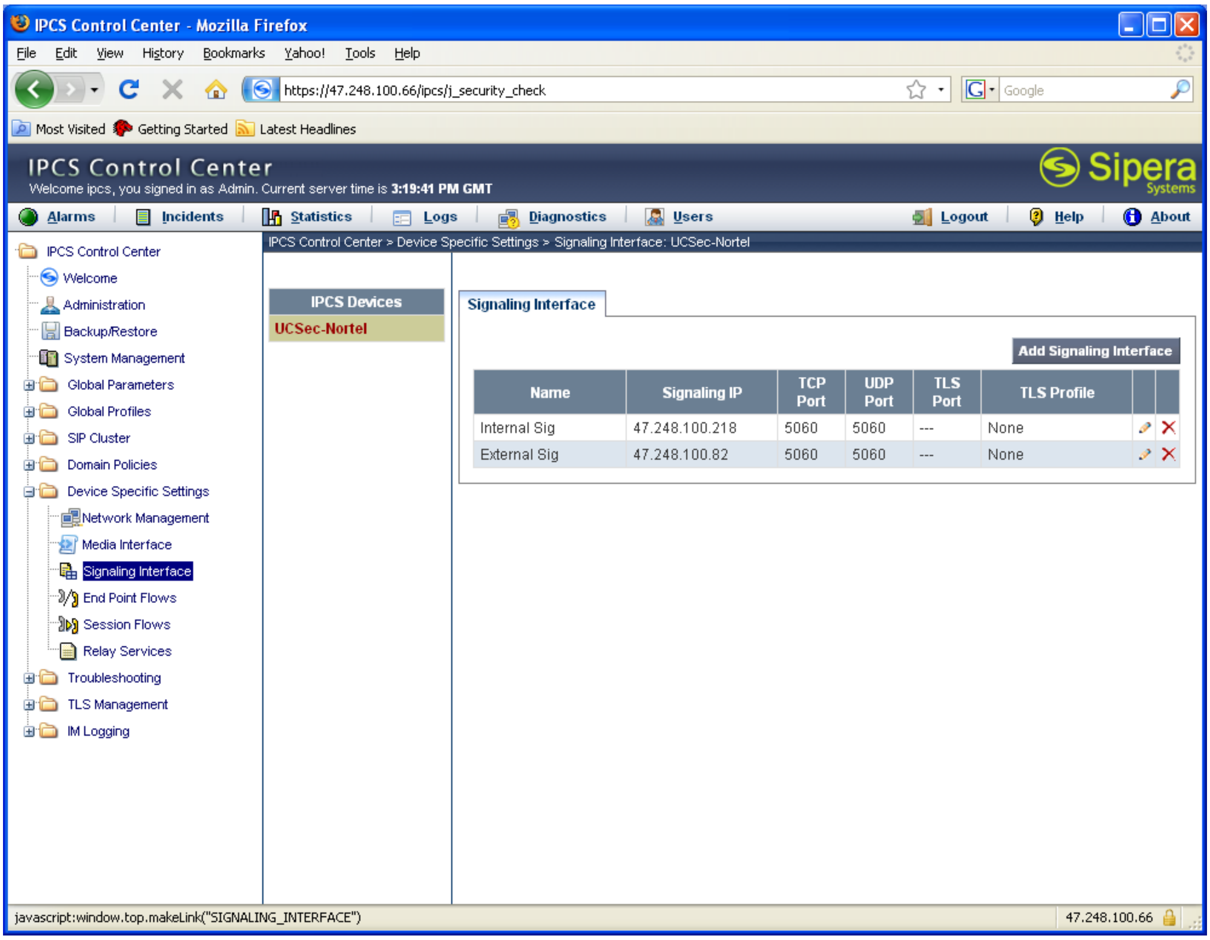
The following information shows the configuration used for the Sipera Systems UC-Sec for the compliance test. Values that are unchanged from the default Sipera Systems deployment are not provided unless specifically relevant to Avaya. Where applicable, values that were changed from the default values are noted.

Note: *The following sections show how the UC-Sec was configured and appear in the same order as the configuration was done unless otherwise noted. Configuration of UC-Sec type (SIP) along with the addresses used for the internal and external networks is done as part of the initial UC-Sec commissioning which is not shown.*

5.1. Signalling and Media Configuration

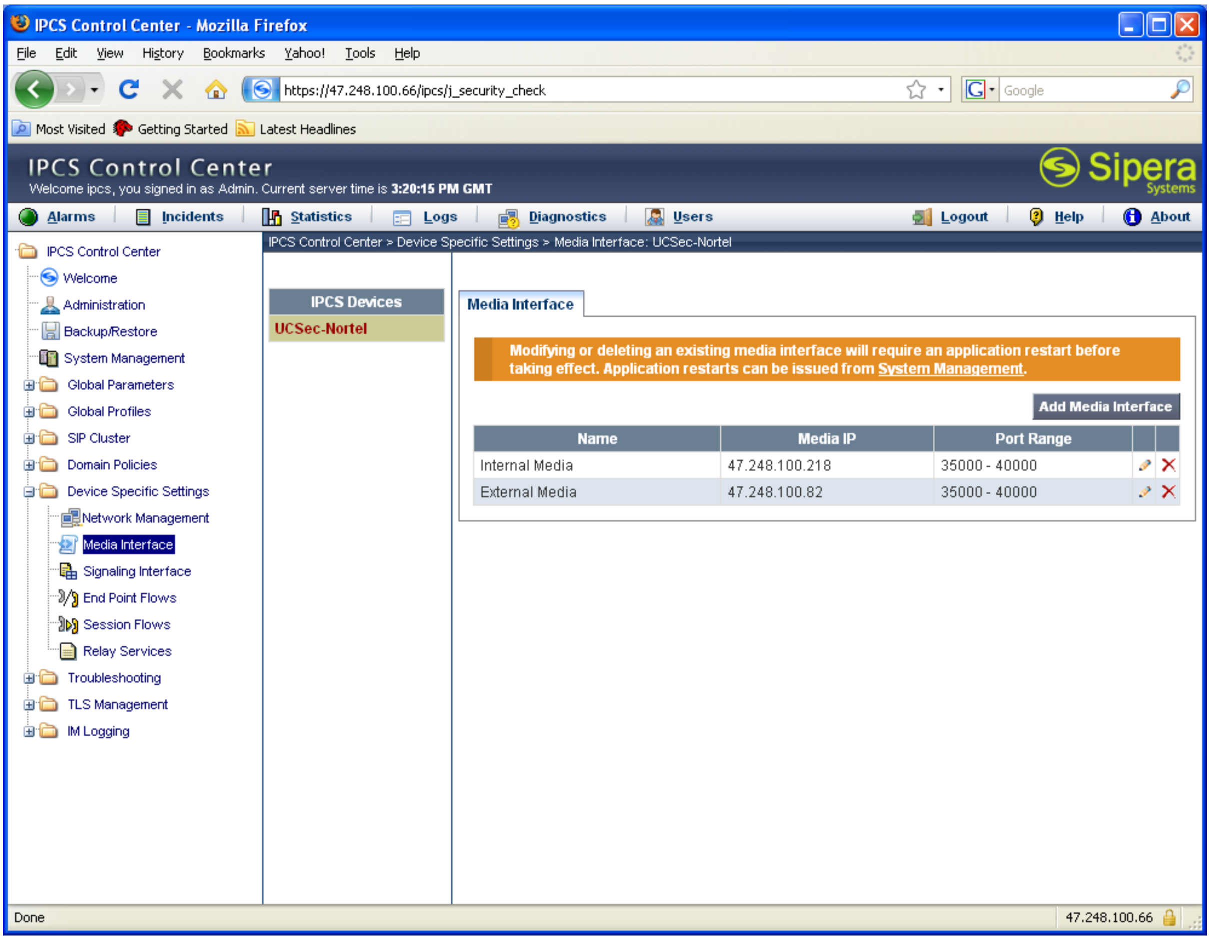
The signalling and Media interfaces were configured, as shown in Figures 16 and 17, to allow connections on the external network for remote users and the internal network for the call server. This configures the address and ports used for both signalling and media traffic through the UC-Sec.

For External configurations select the IP address that remote users connect to. For Internal configurations select the IP address used to communicate with the call server.


IPCS Control Center - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://47.248.100.66/ipcs/j_security_check
Most Visited Getting Started Latest Headlines
IPCS Control Center
Welcome ipcs, you signed in as Admin. Current server time is 3:19:41 PM GMT
Sipera Systems
Alarms Incidents Statistics Logs Diagnostics Users Logout Help About
IPCS Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
Device Specific Settings
Network Management
Media Interface
Signaling Interface
End Point Flows
Session Flows
Relay Services
Troubleshooting
TLS Management
IM Logging
IPCS Control Center > Device Specific Settings > Signaling Interface: UCSec-Nortel
IPCS Devices
UCSec-Nortel
Signaling Interface
Add Signaling Interface
javascript:window.top.makeLink("SIGNALING_INTERFACE")
47.248.100.66

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
Internal Sig	47.248.100.218	5060	5060	---	None
External Sig	47.248.100.82	5060	5060	---	None

Figure 16: Signaling Interface Configuration – Internal & External



IPCS Control Center - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://47.248.100.66/ipcs/j_security_check
Most Visited Getting Started Latest Headlines
IPCS Control Center
Welcome ipcs, you signed in as Admin. Current server time is 3:20:15 PM GMT
Sipera Systems
Alarms Incidents Statistics Logs Diagnostics Users Logout Help About
IPCS Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
Device Specific Settings
Network Management
Media Interface
Signaling Interface
End Point Flows
Session Flows
Relay Services
Troubleshooting
TLS Management
IM Logging
IPCS Control Center > Device Specific Settings > Media Interface: UCSec-Nortel
IPCS Devices
UCSec-Nortel
Media Interface
Add Media Interface
Done
47.248.100.66

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

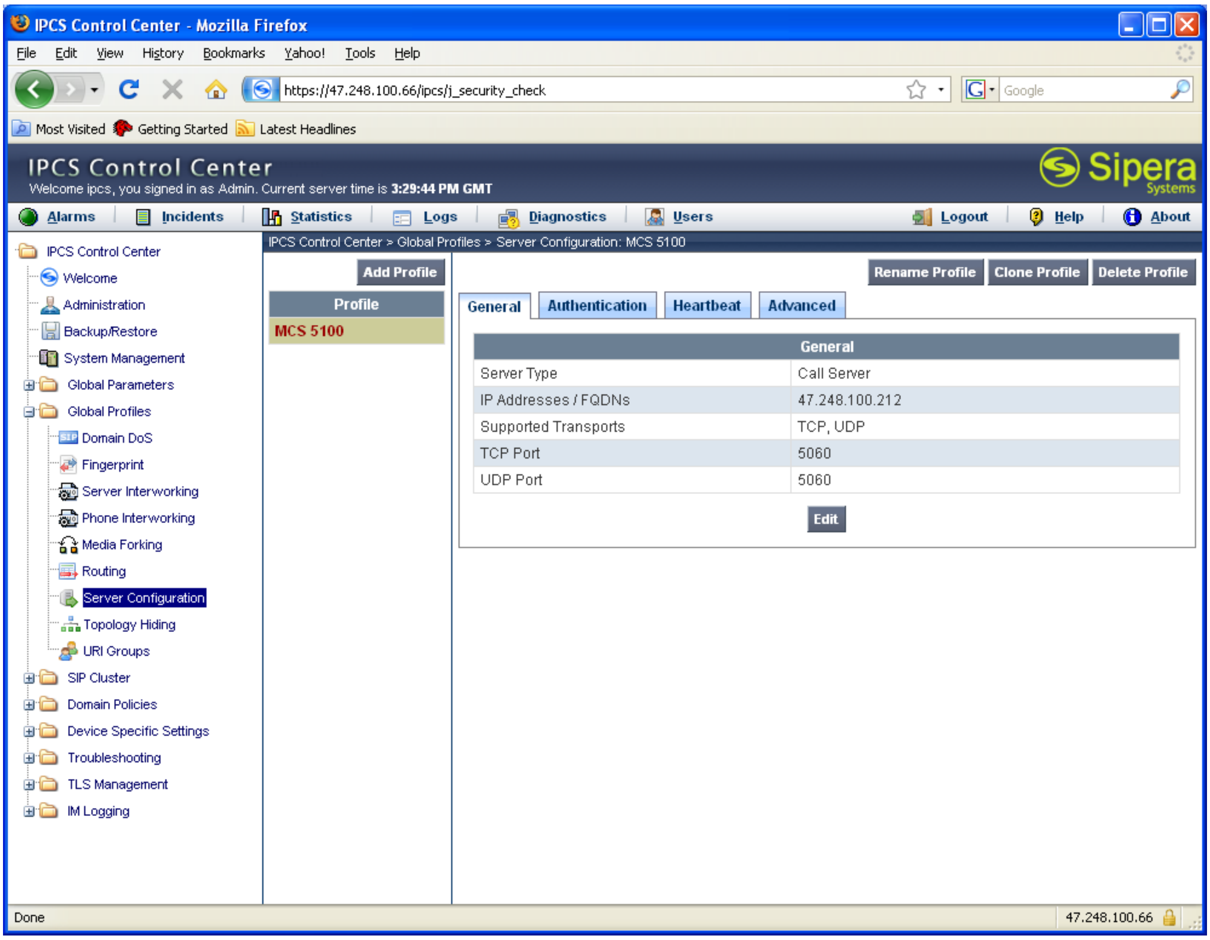
Name	Media IP	Port Range
Internal Media	47.248.100.218	35000 - 40000
External Media	47.248.100.82	35000 - 40000

Figure 17: Media Interface Configuration – Internal & External

5.2. Server Configuration

The server configuration was used to configure the information relevant to the call server. For the compliance test, the server type, IP address and transport information were all that was configured. The values for authentication, heartbeat and advanced tabs are all defaulted (nothing special selected).

Authentication was performed by the Avaya MCS call server. By default authentication is unchecked in the Authentication tab (not shown).

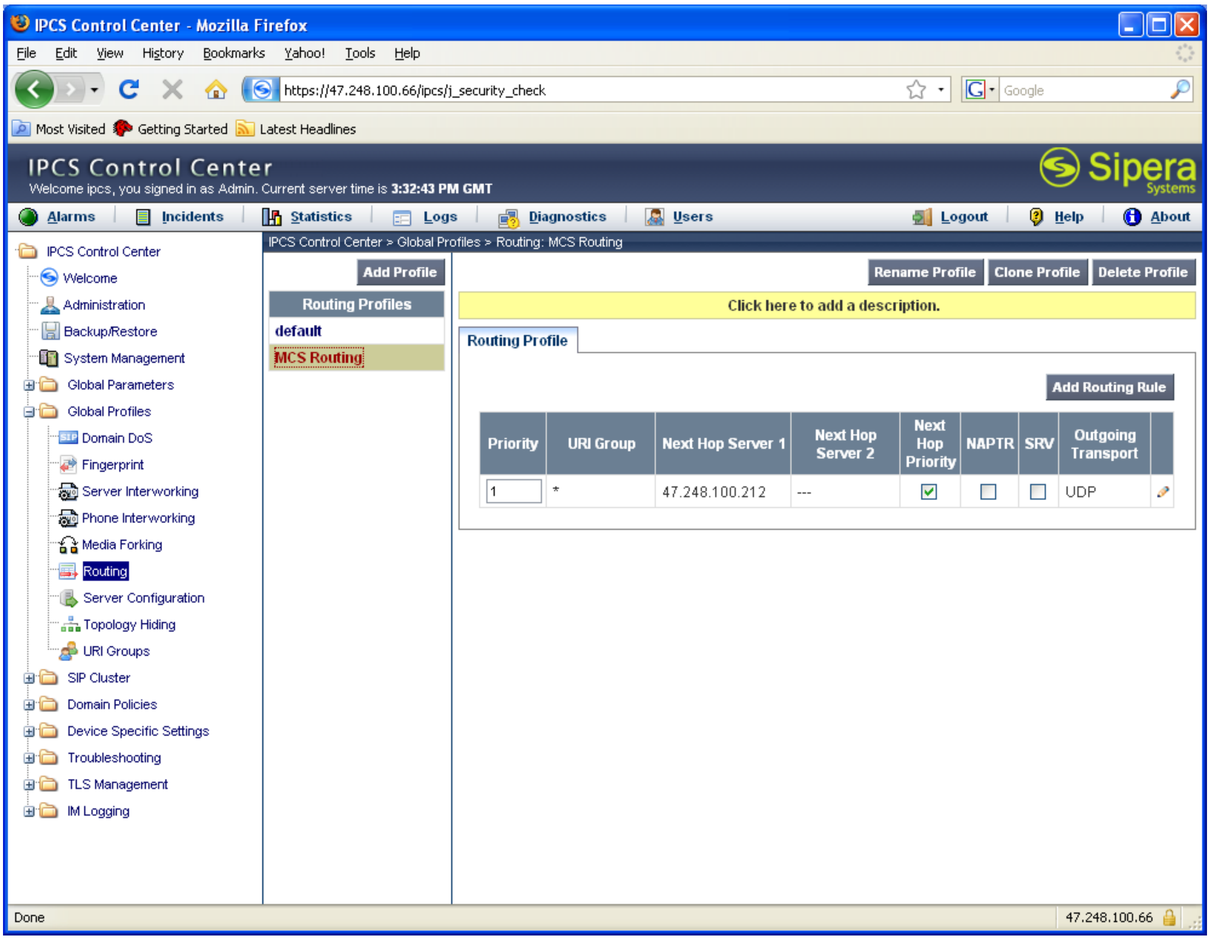

IPCS Control Center - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://47.248.100.66/ipcs/j_security_check
Most Visited Getting Started Latest Headlines
IPCS Control Center
Welcome ipcs, you signed in as Admin. Current server time is 3:29:44 PM GMT
Sipera Systems
Alarms Incidents Statistics Logs Diagnostics Users Logout Help About
IPCS Control Center > Global Profiles > Server Configuration: MCS 5100
IPCS Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Fingerprint
Server Interworking
Phone Interworking
Media Forking
Routing
Server Configuration
Topology Hiding
URI Groups
SIP Cluster
Domain Policies
Device Specific Settings
Troubleshooting
TLS Management
IM Logging
Add Profile
Profile
MCS 5100
Rename Profile Clone Profile Delete Profile
General Authentication Heartbeat Advanced
Edit
Done
47.248.100.66

General	
Server Type	Call Server
IP Addresses / FQDNs	47.248.100.212
Supported Transports	TCP, UDP
TCP Port	5060
UDP Port	5060

Figure 18: Server Configuration General Tab

5.3. Routing

A routing profile was configured to direct incoming remote user SIP messaging to the Avaya Call server. The Service Address of the Call server is provided as the *Next Hop Server* in order to properly route messaging.

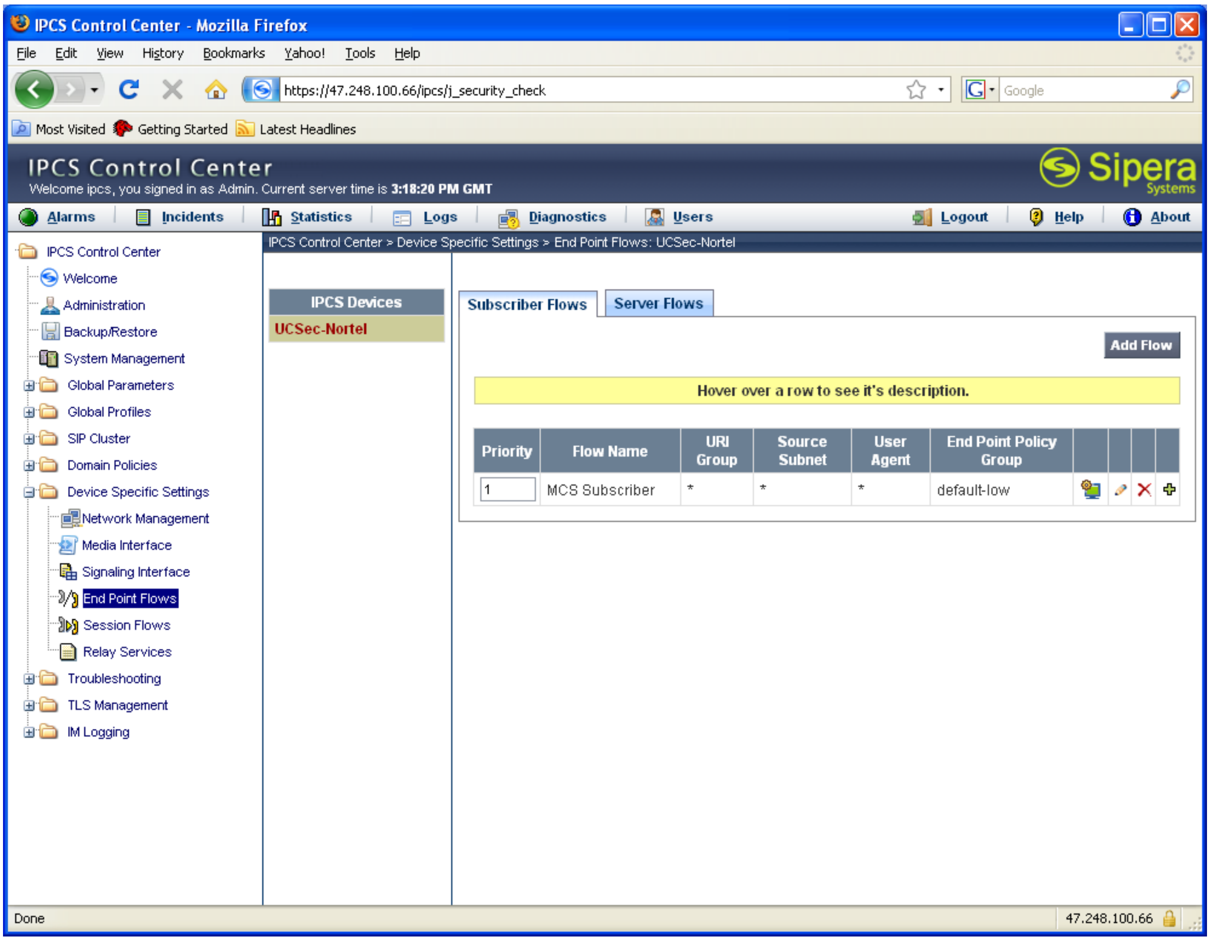

IPCS Control Center - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://47.248.100.66/ipcs/j_security_check
Google
Most Visited Getting Started Latest Headlines
IPCS Control Center
Welcome ipcs, you signed in as Admin. Current server time is 3:32:43 PM GMT
Sipera Systems
Alarms Incidents Statistics Logs Diagnostics Users Logout Help About
IPCS Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Fingerprint
Server Interworking
Phone Interworking
Media Forking
Routing
Server Configuration
Topology Hiding
URI Groups
SIP Cluster
Domain Policies
Device Specific Settings
Troubleshooting
TLS Management
IM Logging
IPCS Control Center > Global Profiles > Routing: MCS Routing
Add Profile
Routing Profiles
default
MCS Routing
Rename Profile Clone Profile Delete Profile
Click here to add a description.
Routing Profile
Add Routing Rule
Done
47.248.100.66

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Outgoing Transport
1	*	47.248.100.212	---	☑	□	□	UDP

Figure 19: Routing to Call server

5.4. End Point Flows

End point flows were created, as shown in Figures 20 and 21, to allow SIP traffic through the UC-Sec and bridge the connection between the remote user and the Avaya Call server. For this compliance test no additional filtering was configured.

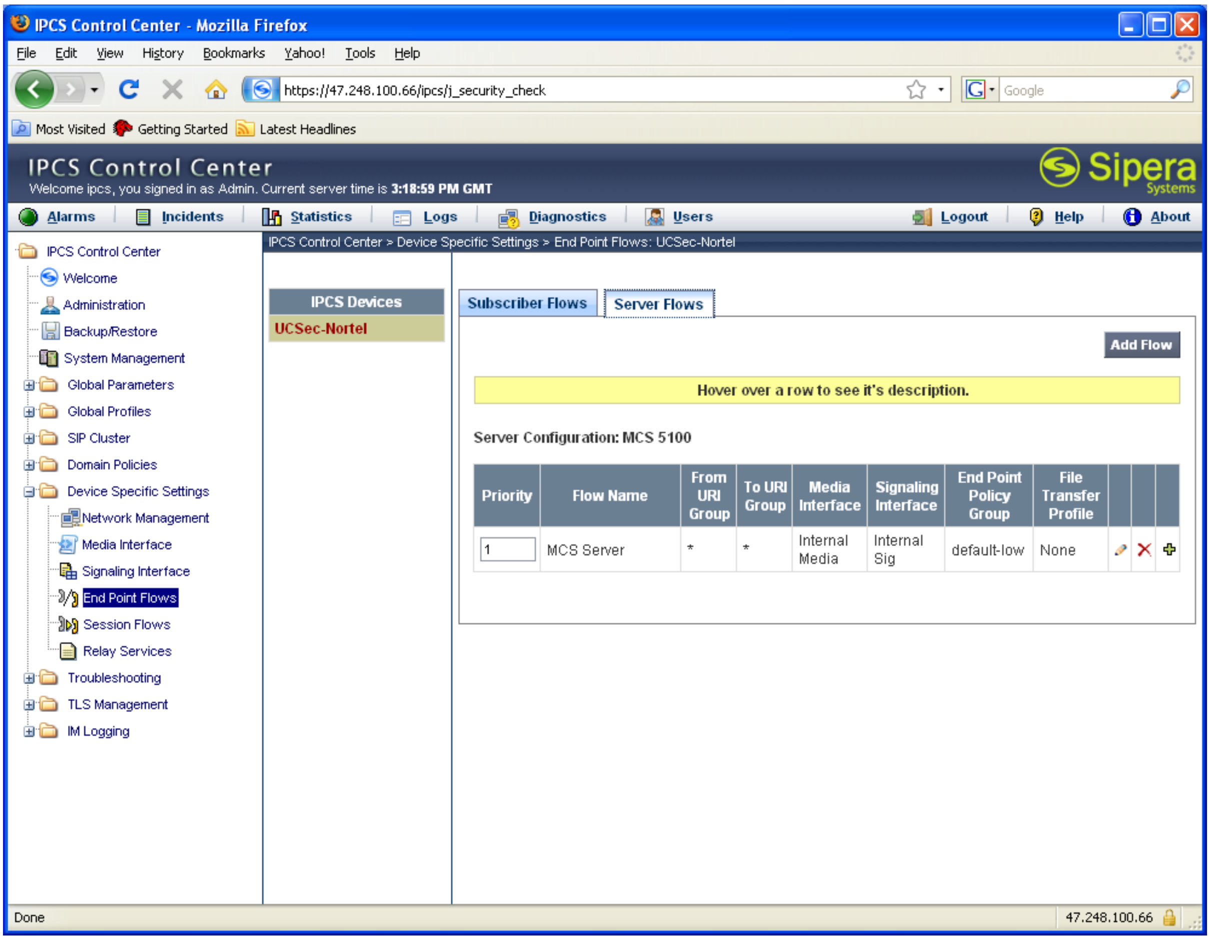


IPCS Control Center > Device Specific Settings > End Point Flows: UCSec-Nortel

Hover over a row to see it's description.

Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group
1	MCS Subscriber	*	*	*	default-low

Figure 20: Subscriber End Point Flow


IPCS Control Center - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://47.248.100.66/ipcs/j_security_check
Most Visited Getting Started Latest Headlines
IPCS Control Center
Welcome ipcs, you signed in as Admin. Current server time is 3:18:59 PM GMT
Sipera Systems
Alarms Incidents Statistics Logs Diagnostics Users Logout Help About
IPCS Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
Device Specific Settings
Network Management
Media Interface
Signaling Interface
End Point Flows
Session Flows
Relay Services
Troubleshooting
TLS Management
IM Logging
IPCS Control Center > Device Specific Settings > End Point Flows: UCSec-Nortel
IPCS Devices
UCSec-Nortel
Subscriber Flows
Server Flows
Add Flow
Hover over a row to see it's description.
Done
47.248.100.66

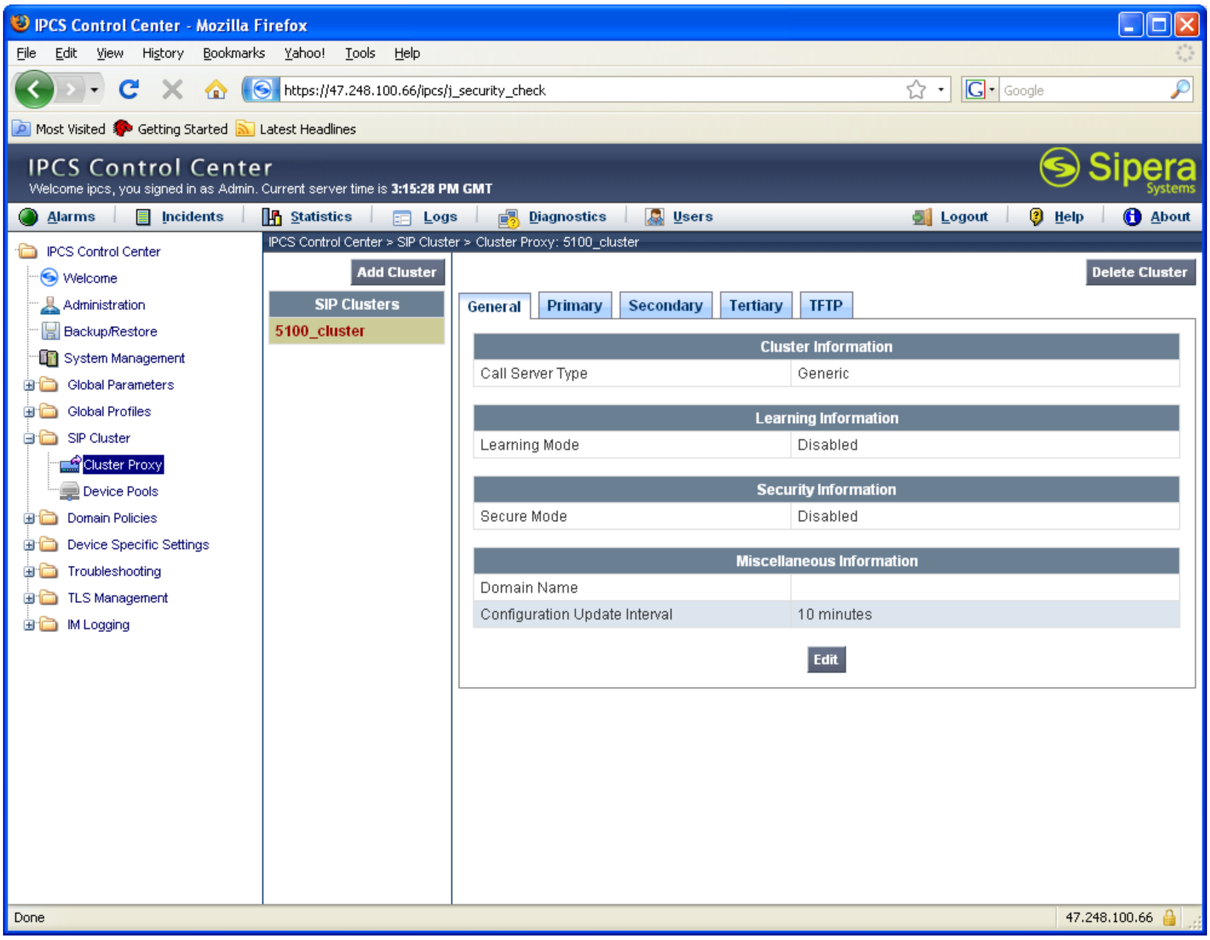
Server Configuration: MCS 5100

Priority	Flow Name	From URI Group	To URI Group	Media Interface	Signaling Interface	End Point Policy Group	File Transfer Profile
1	MCS Server	*	*	Internal Media	Internal Sig	default-low	None

Figure 21: Server End Point Flow

5.5. SIP Cluster Proxy

A SIP Cluster Proxy was created to allow the remote user clients to obtain the service package from the Avaya Call Server. It proxies the HTTP requests used to obtain the service package such that a remote user requests the service package from the UC-Sec and the UC-Sec retrieves and delivers that service package on behalf of the Avaya Call server.
For the Avaya Call Server, the critical information is found on the Primary tab – the address and port information. The configuration update interval was set to 10 minutes, however the service package is not cached, and it is retrieved each time it is requested. The configuration update interval is mandatory for configuring a Cluster Proxy. There was no configuration provided for the remaining Cluster Proxy tabs.


IPCS Control Center - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://47.248.100.66/ipcs/j_security_check
Google
Most Visited Getting Started Latest Headlines
IPCS Control Center
Sipera Systems
Alarms Incidents Statistics Logs Diagnostics Users Logout Help About
IPCS Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Cluster Proxy
Device Pools
Domain Policies
Device Specific Settings
Troubleshooting
TLS Management
IM Logging
IPCS Control Center > SIP Cluster > Cluster Proxy: 5100_cluster
Add Cluster
Delete Cluster
SIP Clusters
5100_cluster
General Primary Secondary Tertiary TFTP
Edit
Done
47.248.100.66

Welcome ipcs, you signed in as Admin. Current server time is **3:15:28 PM GMT**

Cluster Information	
Call Server Type	Generic

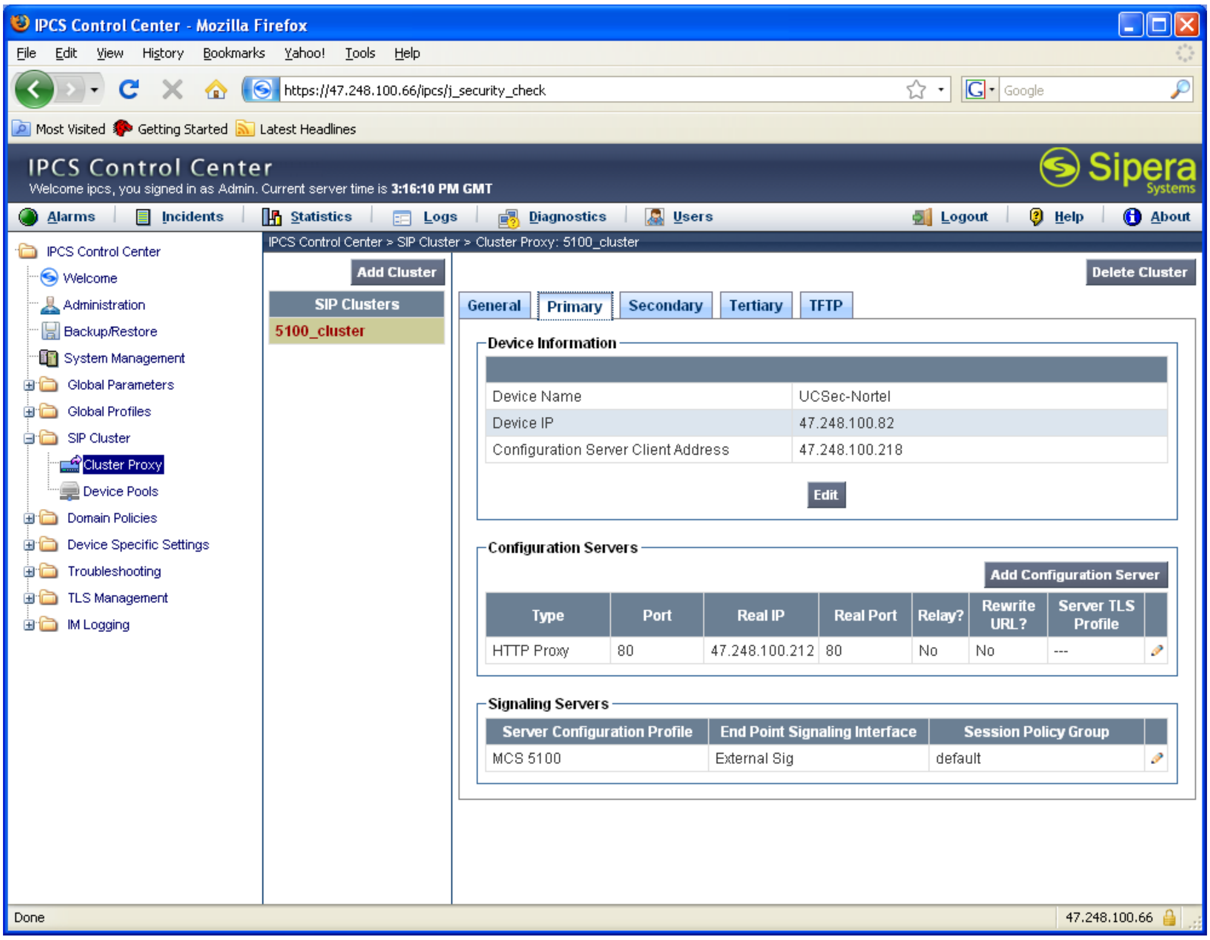
Learning Information	
Learning Mode	Disabled

Security Information	
Secure Mode	Disabled

Miscellaneous Information	
Domain Name	
Configuration Update Interval	10 minutes

Figure 22: Cluster Proxy General Tab

The information provided for the Primary tab of the Cluster Proxy directs HTTP requests from the UC-Sec remote user interface (*Device IP*) to the UC-Sec interface facing the client configuration server (*Configuration Server Client Address*). The *Real IP* provided is the address of the Call server that contains the real client configuration.


IPCS Control Center - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
https://47.248.100.66/ipcs/j_security_check
Most Visited Getting Started Latest Headlines
IPCS Control Center
Welcome ipcs, you signed in as Admin. Current server time is 3:16:10 PM GMT
Sipera Systems
Alarms Incidents Statistics Logs Diagnostics Users Logout Help About
IPCS Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Cluster Proxy
Device Pools
Domain Policies
Device Specific Settings
Troubleshooting
TLS Management
IM Logging
IPCS Control Center > SIP Cluster > Cluster Proxy: 5100_cluster
Add Cluster
SIP Clusters
5100_cluster
Delete Cluster
General Primary Secondary Tertiary TFTP
Edit
Add Configuration Server
Done
47.248.100.66

Device Information

Device Name	UCSec-Nortel
Device IP	47.248.100.82
Configuration Server Client Address	47.248.100.218

Configuration Servers

Type	Port	Real IP	Real Port	Relay?	Rewrite URL?	Server TLS Profile
HTTP Proxy	80	47.248.100.212	80	No	No	---

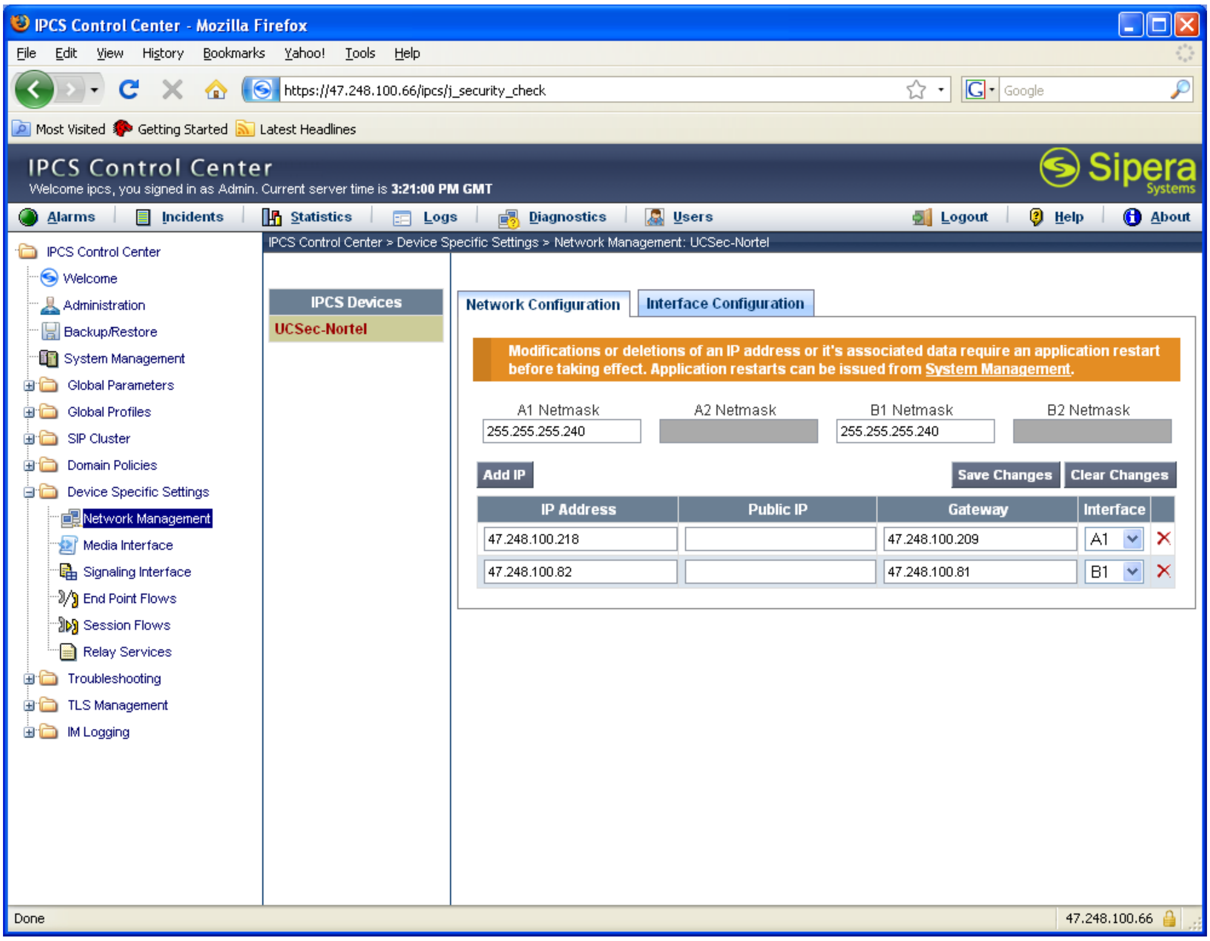
Signaling Servers

Server Configuration Profile	End Point Signaling Interface	Session Policy Group
MCS 5100	External Sig	default

Figure 23: Cluster Proxy Primary Tab

5.6. Interface Configuration

Once all configurations are completed on the UC-Sec, the network interfaces must be enabled to allow traffic for the external network facing the remote users and the internal network facing the call server.
Note: *The configuration of the network addresses is done when the UC-Sec is initially configured, but can be modified later. The Network Configuration tab below is provided for reference and was not changed after initial configuration.*



https://47.248.100.66/ipcs/j_security_check

Welcome ipcs, you signed in as Admin. Current server time is **3:21:00 PM GMT**

IPCS Control Center > Device Specific Settings > Network Management: UCSec-Nortel

Modifications or deletions of an IP address or it's associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.240		255.255.255.240	

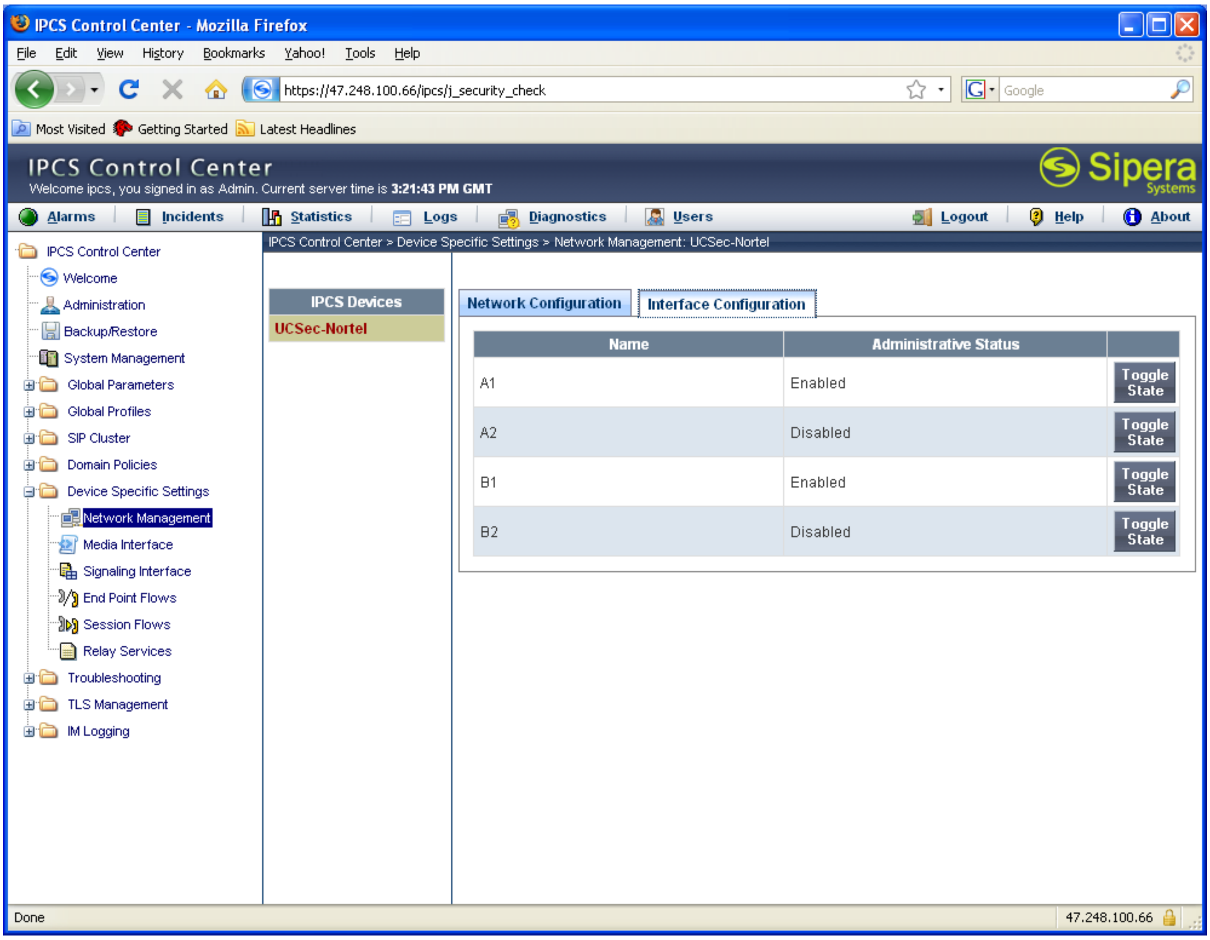
IP Address	Public IP	Gateway	Interface
47.248.100.218		47.248.100.209	A1
47.248.100.82		47.248.100.81	B1

47.248.100.66

Figure 24: Network Management UC-Sec Addresses

The UC-Sec has network interfaces labelled M1, M2, A1, A2, B1 and B2. The M1 interface is used for management and is configured as part of initial installation and commissioning done from a console connected directly to the UC-Sec. This configuration is not shown.

By convention, the internal facing interface is set to A1 and the external facing interface is set to B1. Regardless of what is selected, the physical network connections must match what is configured in order to properly enable network traffic on the separate networks.



Welcome ipcs, you signed in as Admin. Current server time is **3:21:43 PM GMT**

IPCS Control Center > Device Specific Settings > Network Management: UCSec-Nortel

Name	Administrative Status	
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

Figure 25: Network Management Interfaces Enabled

6. General Test Approach and Test Results

The focus of this interoperability compliance testing was to verify the authorize SIP clients (users) of MCS system are be able to communicate with each other through the Sipera UC-Sec securely within the MCS 5100 domain. The testing verified the Sipera UC-Sec was able to allow the SIP signaling and media to pass through. The following features were covered: registration, basic calls, busy, music on hold, mute, transfer, DTMF, MWI, codec negotiation, meet-me conference, ad-hoc conference, instance messaging, chat room, web collaboration, simultaneously ringing, call branding, presence update, file transfer and video SIP calls.

6.1. General test approach

The general test approach was to have one of the MCS clients/users to place a call to another client/user who are registered to the Sipera UC-Sec. The UC-Sec then in turn sends that registration to the MCS 5100 to allow the connection to be established. The main objectives were to verify the Sipera UC-Sec represents the MCS clients/users were able to successfully:

- Register to MCS 5100 domain.
- Perform basic call operation: DTMF transmission, voicemail with MWI notification, busy, hold.
- Redirect calls between users/clients/endpoints: blind/consultative transfers, call forward all calls, busy and no answer.
- Perform codec negotiation
- Perform conferencing: ad-hoc and meet-me conferencing.
- Perform the MCS multi-media functions: music on hold, meet-me conference, instant messaging, web collaboration, sim-ring, branding, present update, file transfer and video SIP calls

6.2. Test Results

The objectives outlined in section 6.1 were verified and met.
The following observations were made during the compliance testing:

- Sipera UC-Sec should be configured as a trusted external node in the MCS 5100 MCP Console. This is to eliminate unnecessary authentication messages going back and forth which may cause unexpected traffic.
- Because Sipera UC-Sec does not support HTTPS proxy, the Default PA URL Properties configured in MCS 5100 Provisioning should have HTTPS disabled (port is set to 0)
- At the start of audit testing, Sigma phone can not retrieve service package from MCS 5100 through UC-Sec. The issue has been fixed by Sipera.
- The second hold used to cause the music to be delayed. From the pcap trace, UC-Sec did not forward the ACK for 200OK from MPCC. The issue has been fixed by Sipera. The issue does not happen without the UC-Sec.

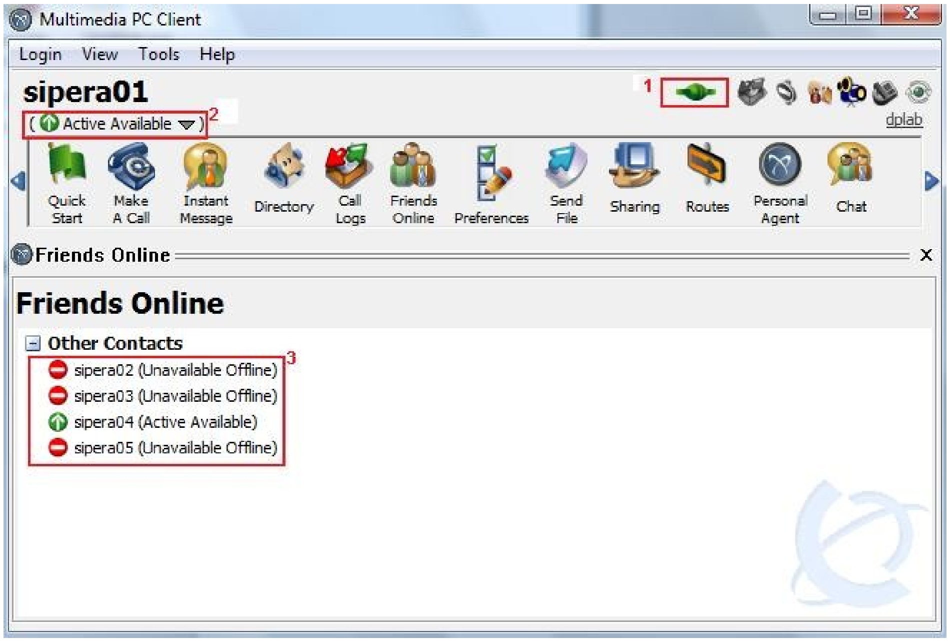
- The chat room feature does not work as expected on UC-Sec. The UC-Sec does not involve the anchoring of the media, i.e., the instant messages do not go through UC-Sec but go directly to MAS server of the MCS system.
- There is no call duration recorded in outbox call log of converged MPCC when a converged desktop user makes a call out. The reason is that The NOTIFY messages have non-identical Call IDs when going through the UC-Sec. So the terminating NOTIFY is not matched to the initial NOTIFY. The issue does not happen without the UC-Sec.

7. Verification Steps

This section includes some steps that can be followed to verify the solution is working.

7.1. Verify that MPCC's and Sigma hard clients successfully register with MCS 5100 Server through Sipera UC-Sec.

- Verify that MPCC's register successfully as show in the following figure. Make sure that:
  1. MPCC is connected.
  2. The current presence is updated accordingly.
  3. Others' presences are observed on the MPCC window.



sipera02 (Unavailable Offline)
sipera03 (Unavailable Offline)
sipera04 (Active Available)
sipera05 (Unavailable Offline)

Figure 26: MPCC window

- On Sigma hard clients, navigate to ***Servcs → 4. Presence*** and observe the current presence of the phone. Then, navigate to ***View → 1. Friends*** and observe the others' presence.
- During the registration, use the pcap tool (ethereal/wireshark) at the MPCC's and Sigma clients to make sure that all SIP registration request/response messages and HTTP requests/responses are going through the Sipera UC-Sec.

7.2. Verify that calls are established with two-way voice and video path when making calls between MPCC's and two-way voice path between Sigma hard clients.

- During the call, use the pcap tool (ethereal/wireshark) at the MPCC's and Sigma clients to make sure that all SIP request/response messages, HTTP requests/responses and RTP streams are going through the Sipera UC-Sec.

8. Conclusion

All of the executed test cases have passed and met the objectives outlined in **Section 6.1**, with some exceptions outlined in **Section 6.2**. The outstanding issues are being investigated by Sipera and Avaya design teams. Some of these issues are considered as exceptions. The Sipera UC-Sec software version 4.0 is considered compliant with MCS 5100 Release 4.0.

9. Additional References

Product documentation for Avaya products may be found at:
http://support.nortel.com/go/main.jsp
[1] *MCS 5100 System Management Console User Guide (MCP Console User Guide), Release 4.0, Standard 01. 05, January 2008, Document Number NN42020-110 01.05*

[2] *Solution Integration Guide for Communication Server 1000 Release 5.0 and Multimedia Communication System 5100 release 4.0, Revision 02.05, Document Number NN49000-301*

[3] *MCS 5100 Provisioning Client User Guide, Release 4.0, Revision 01.10, January 2010, Document Number NN42020-105*

[4] *Multimedia PC Client User Guide, Release 4.0, Revision 01.05, July 2009, Document Number NN42020-102*

Product information for Sipera products can be found at
http://www.sipera.com/index.php?action=products,default

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.