



Avaya Solution & Interoperability Test Lab

Application Notes for Microsoft Exchange Unified Messaging 2010 with Avaya Communication Server 1000 Release 7.5 – Issue 1.1

Abstract

These Application Notes describe a solution comprised of SIP Trunk interoperability between Microsoft Exchange Unified Messaging 2010 System and Avaya Communication Server 1000 Release 7.5.

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 configuration steps required to integrate Microsoft Exchange Server 2010 Unified Messaging (UM) with Avaya Communication Server 1000 (CS 1000). Exchange UM is a voice mail system that combines voice messaging, fax, and e-mail into one inbox, which can be accessed from a telephone or computer. UM subscribers can have their calls cover to voicemail and can retrieve their messages from a telephone by calling into a voice mailbox, or from a PC via the Play-on-Phone feature available with Outlook Web Access (OWA). In addition, Exchange UM can control the Message Waiting Indicator (MWI) on a user's telephone to notify the user of new voicemail messages. The focus of these Application Notes is on the Exchange UM component of Microsoft Exchange Server 2010.

2. General Test Approach and Test Results

The general test approach was to exercise the features of Exchange UM and verifying the appropriate behavior. All test cases were performed manually.

2.1. Interoperability Compliance Testing

The interoperability compliance test covered the following features:

- Calls to Exchange UM from subscribers and non-subscribers.
- Calls to UM subscribers covered to Exchange UM on no-answer and the appropriate greeting was played to the caller. Voicemail was left for the UM subscriber.
- Subscribers logging into Exchange UM.
- MWI lamp of a subscriber's phone was turned on when a new voicemail message existed.
- UM subscriber was able to retrieve voicemail messages from a phone, which would extinguish the MWI.
- UM subscriber was able to use Play-on-Phone via OWA to listen to voicemail messages.
- UM subscriber was able to navigate Exchange UM using the Voice User Interface or Telephony User Interface.
- Call transfer from Exchange UM to another subscriber.
- Calls to the UM Auto Attendant.
- G.711 and G.723 codec support.
- Call answering rules to do a "Find Me" or "Transfer" to another number.
- Calls to Exchange UM with SIP TLS.
- Calls to Exchange UM with SIP TLS and secure media.

2.2. Test Results

All test cases were successful, except for the following observations:

- Unlike Exchange 2007 UM, Exchange 2010 UM requires an external fax server, which wasn't available during testing. The T.38 negotiation would have been between SIP Gateway and a 3rd party fax server. The scope of Fax T.38 testing was to verify that

Exchange UM returns the correct URL of the external fax server in the REFER message when it detects a fax tone, which was verified successfully.

- Call Transfer from Exchange UM back to CS 1000 phone gets disconnected. This issue was reported to the CS 1000 development team and is under investigation.

2.3. Support

Technical support of Microsoft Exchange Server 2010 Unified Messaging is available at Microsoft TechNet at <http://technet.microsoft.com/en-us/library/bb125141.aspx>. Additional support options are also covered on this webpage.

3. Reference Configuration

Figure 1 illustrates the network diagram configuration used during the compliance testing between the Avaya Communication Server 1000 and Microsoft Exchange Unified Messaging 2010.

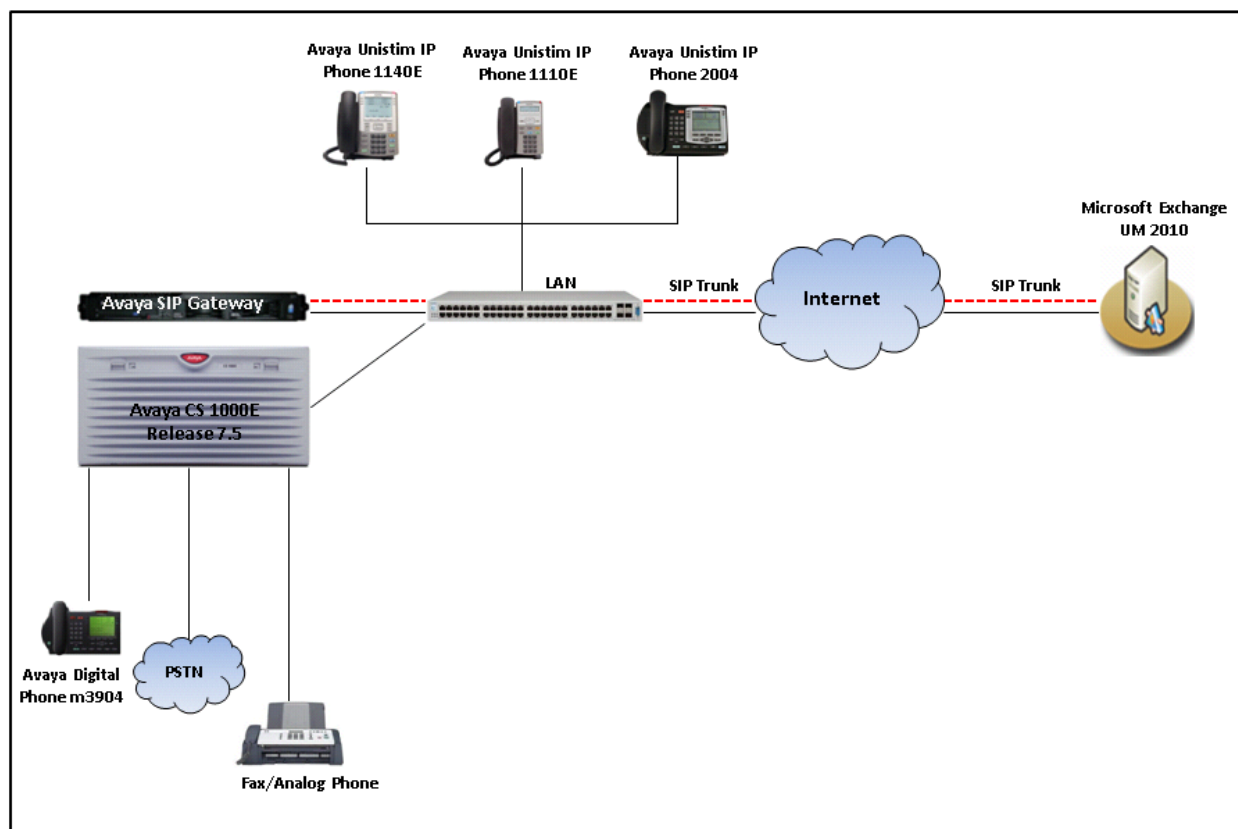


Figure 1: Reference Network Configuration

4. Equipment and Software Validated

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

Equipment	Software
Avaya Communication Server 1000E CPPM	SW Version 7.50Q With DepList 1
Avaya IP Unistim Phone 2004P1	0602B76
Avaya IP Unistim Phone 1110	0623C8A
Avaya IP Unistim Phone 1140E	0625C8A
Microsoft Exchange 2010	Version 14.01.0359.00
Microsoft Exchange Server Operating System	Windows Server 2008 64-bit Service Pack 2

5. Configure Avaya Communication Server 1000

This document assumes that the Avaya Communication Sever 1000 system was properly installed and configured as per the product documents. This section provides the steps on how to provision the CS1000 to work with Exchange UM. For more information about how to install and configure Communication Sever 1000, please refer to **Section 11**.

The following summarizes the tasks which need to be done on the CS1000 System:

- Configure SIP Trunk between CS 1000 SIP GW and Exchange UM server.
- Configure D-Channel for SIP Trunk.
- Configure Zone for Route and Trunk.
- Configure SIP Route.
- Configure IP Trunks.
- Configure CDP Dialing plan.

5.1. Configure SIP Trunk between CS1000 SIP Gateway and Exchange UM Server

To configure SIP Trunk between CS1000 SIP GW and Exchange UM, follow the procedures below:

Launch the Unified Communication Management (UCM) managing the CS1000 system that needs to be configured. Enter the username “admin” and its password in the **User ID** and **Password** boxes and click on the **Login** button.

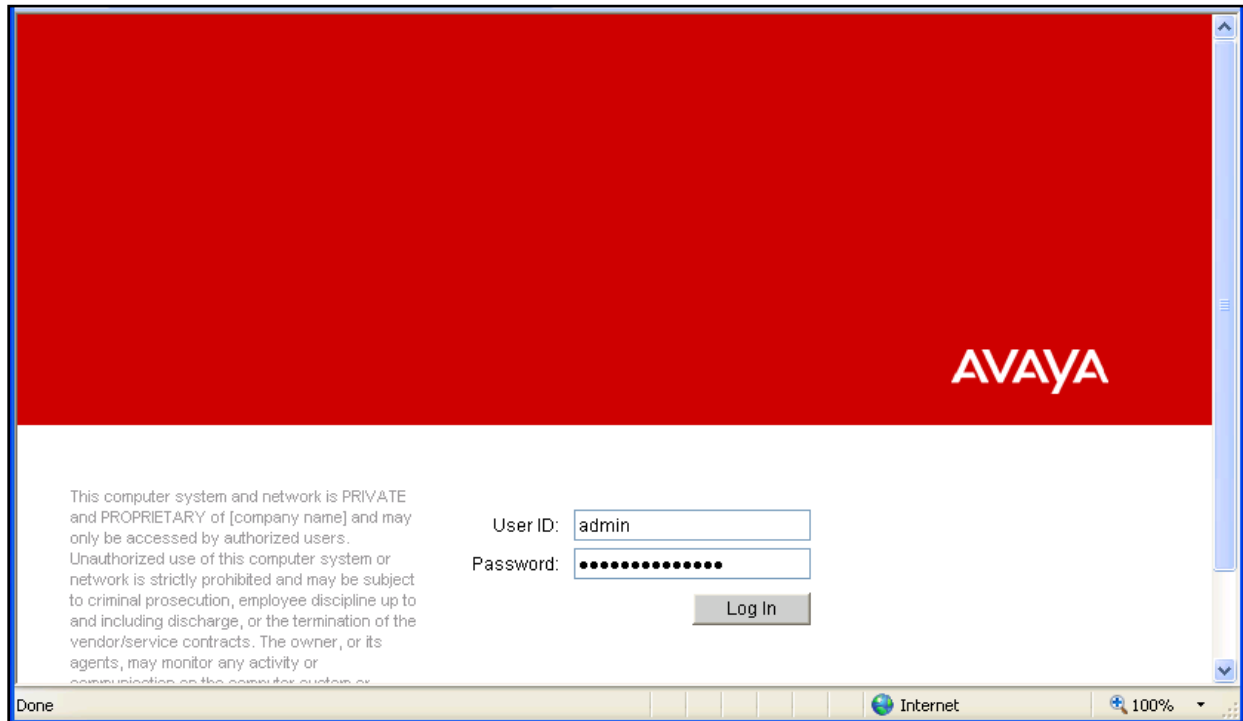


Figure 2: UCM Login window

On right-hand side of UCM homepage, click on Element Name “*EM_on_cpppm3*” link that manages the SIP Gateway used to connect to Exchange UM.

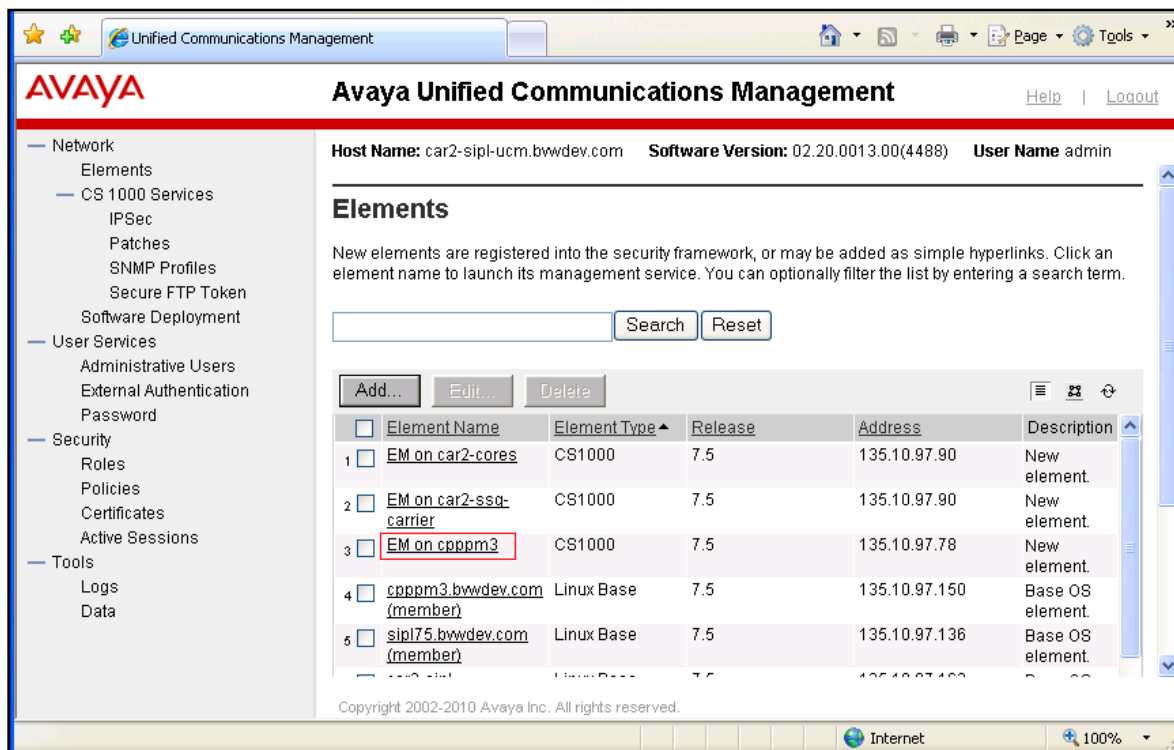


Figure 3: UCM Home Page

Figure 4 displays homepage of CS1000 Element Manager.

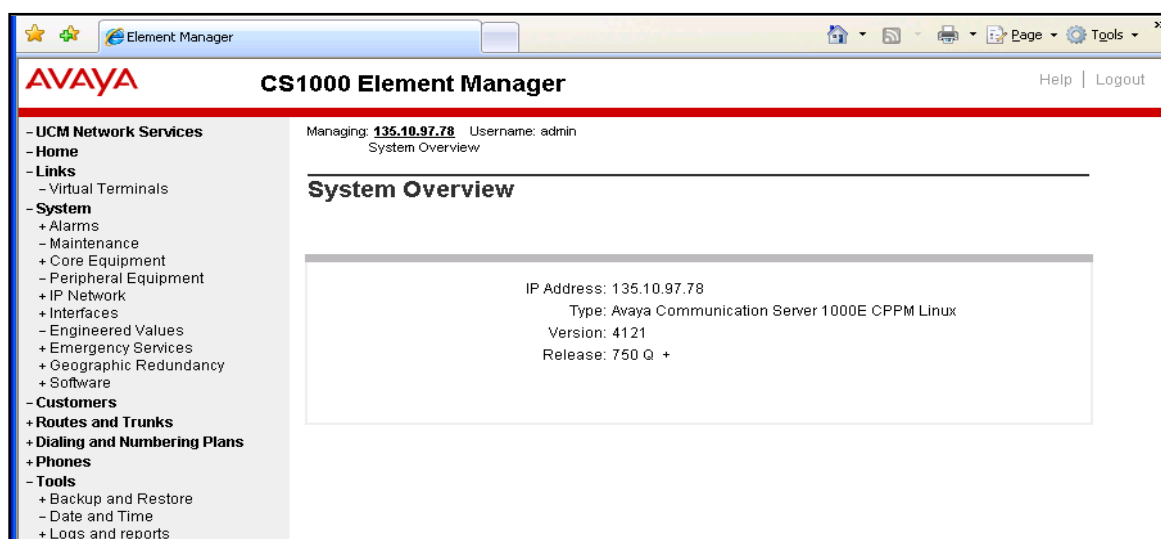


Figure 4: CS1000 Element Manager Home Page

On left-hand side tree menu of the Element Manager window, navigate to **System > IP Network > Nodes: Servers and Media Cards, IP Telephony Nodes** displays in the right-hand side of the window.

Click on Node ID “511” which has the **SIPGw** application enabled and used to connect to Exchange UM.

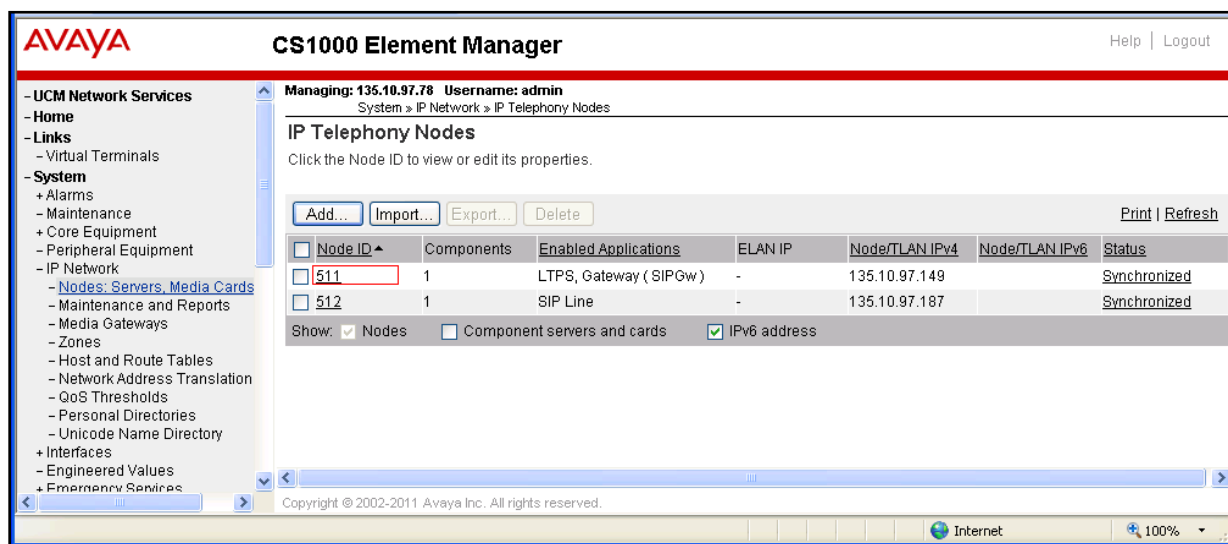


Figure 5: IP Telephony Nodes Page

Node Details (ID: 511 - LTPS, Gateway (SIPGw)) page displays.

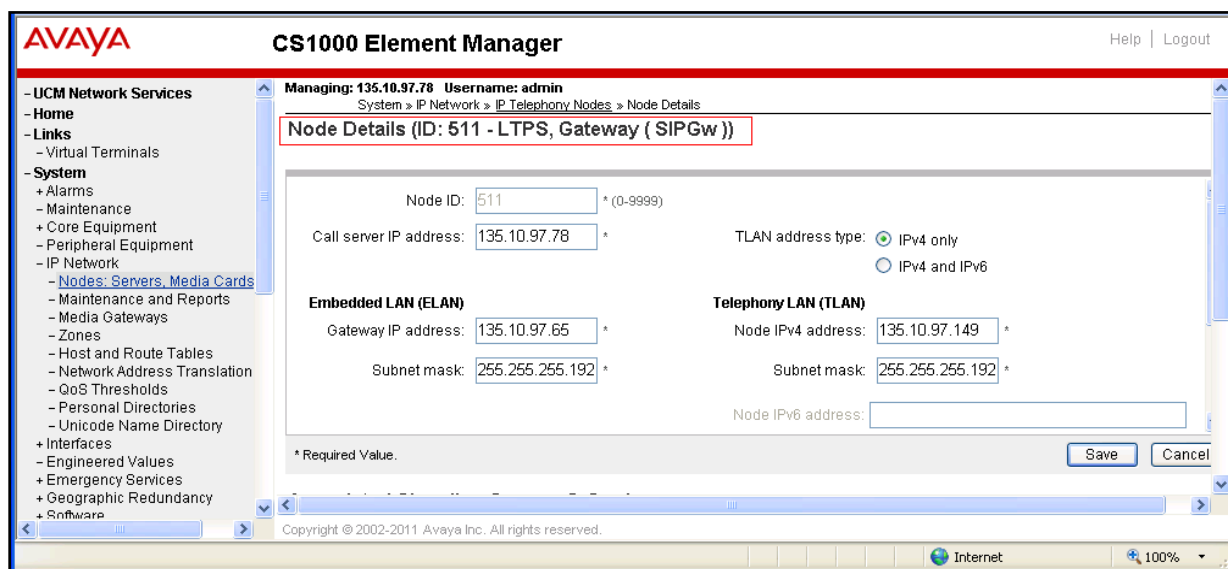


Figure 6: Node Details (ID: 511 - LTPS, Gateway (SIPGw)) Page

Scroll down to **Applications** section and click on **Gateway (SIPGw)** link.

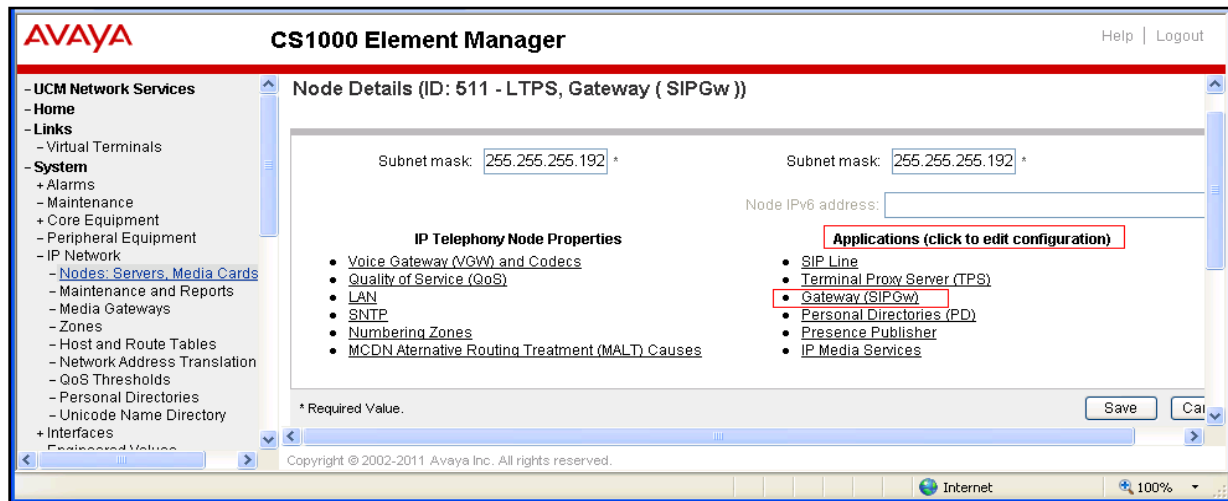


Figure 7: List of Applications in Node Details

Node ID: 511 – Virtual Trunk Gateway Configuration Details page displays. Enter information for **General** section:

- **SIP domain name:** enter IP address of Exchange UM “131.107.5.62”.
- **Local SIP port:** “5060”.
- **Gateway Endpoint Name:** “cippm3”.
- **Gateway password:** Leave it blank.
- **Application Node ID:** “511”.

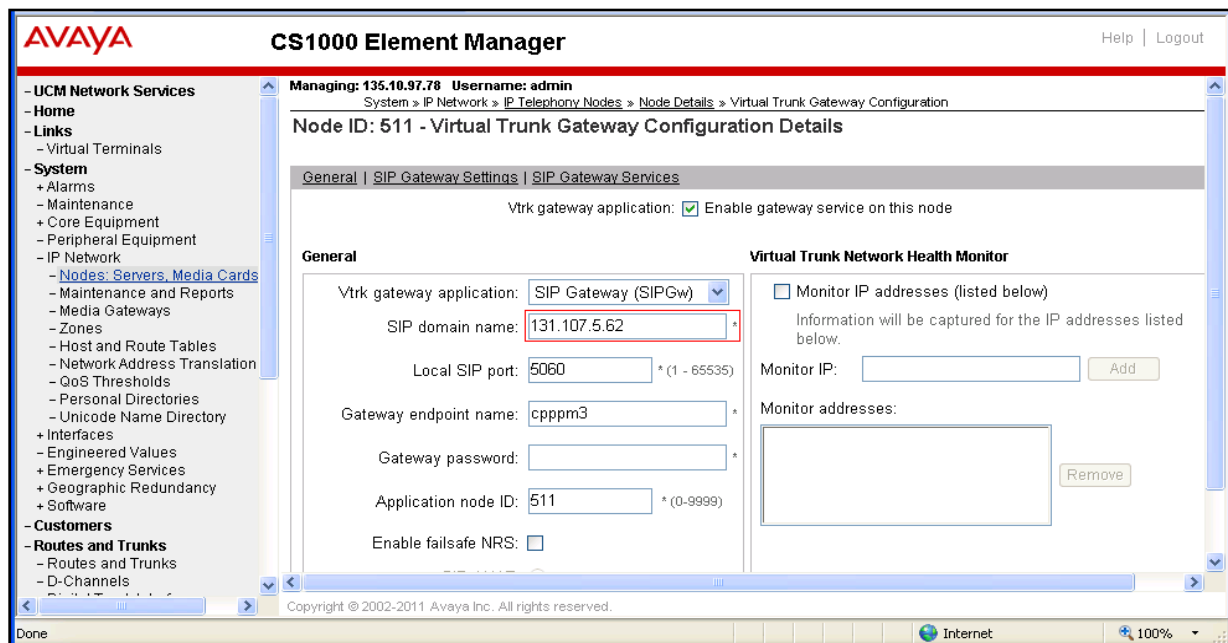


Figure 8: Node ID: 511 – Virtual Trunk Gateway Configuration Details Page

Scroll down to section **SIP Gateway Settings** (not shown), in **Proxy Or Redirect Server** subsection of this section, enter information for this section:

- **Primary TLAN IP address:** enter IP address of Exchange UM “131.107.5.62”.
- **Port:** “5060”.
- **Transport protocol:** “TCP”.

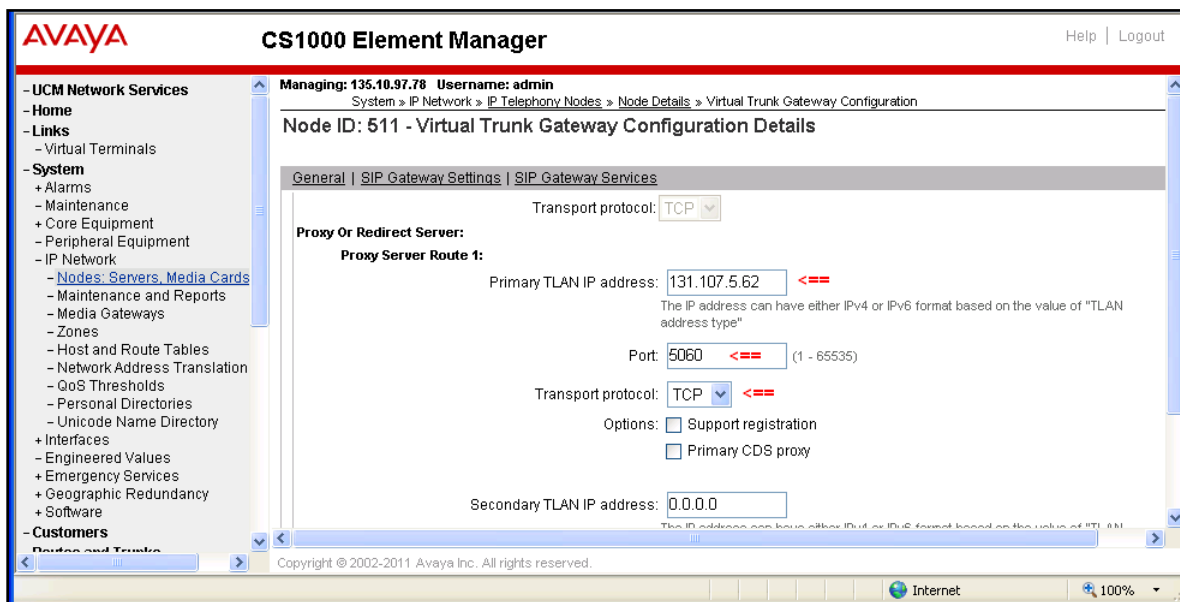


Figure 9: The SIP Gateway Setting of Telephony Node

Scroll down to **SIP URI Map** of **SIP Gateway Settings** section, in **Private domain names**, leave CDP field as blank. If there is any text presented in the CDP field, delete it.

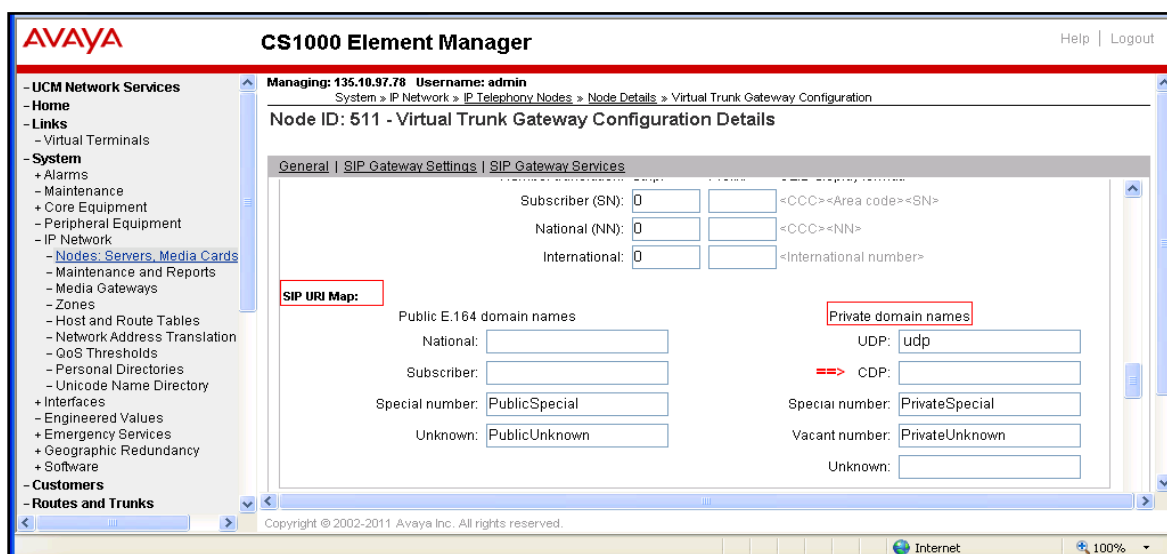


Figure 10: SIP URI Map Configuration Page

Scroll down to **SIP Gateway Services** section of **Node ID: 511 - Virtual Trunk Gateway Configuration Details** page.

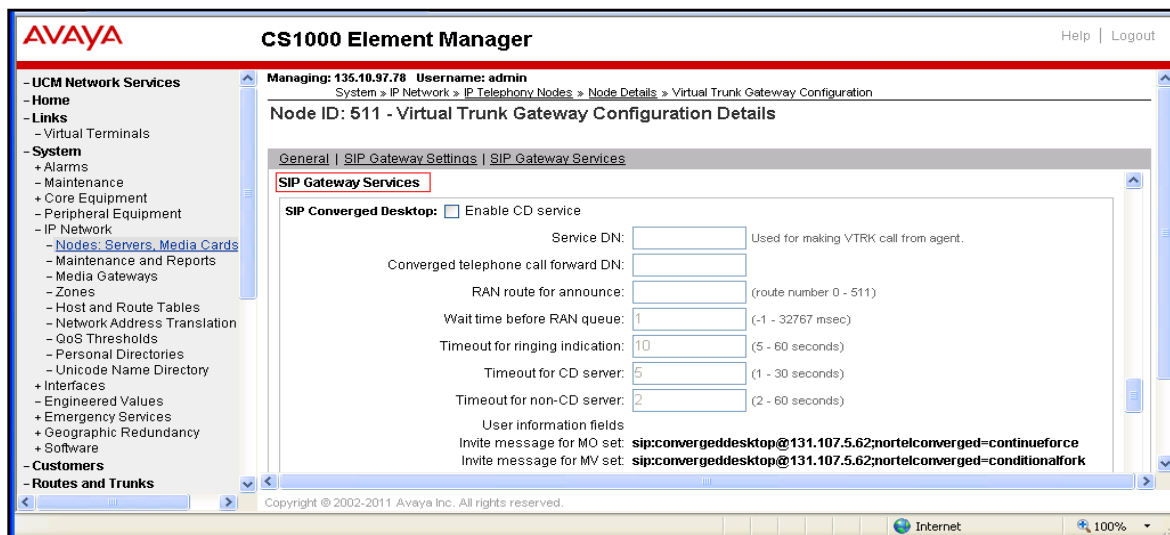


Figure 11: SIP Gateway Services Section

In the **SIP Gateway Services** section, scroll down to **Microsoft Unified Messaging** subsection and enter information:

- **MWI Application DN:** enter number “73100” which is defined in **Section 5.6.2**
- **MWI dialing plan:** select “CDP” in dropdown menu.

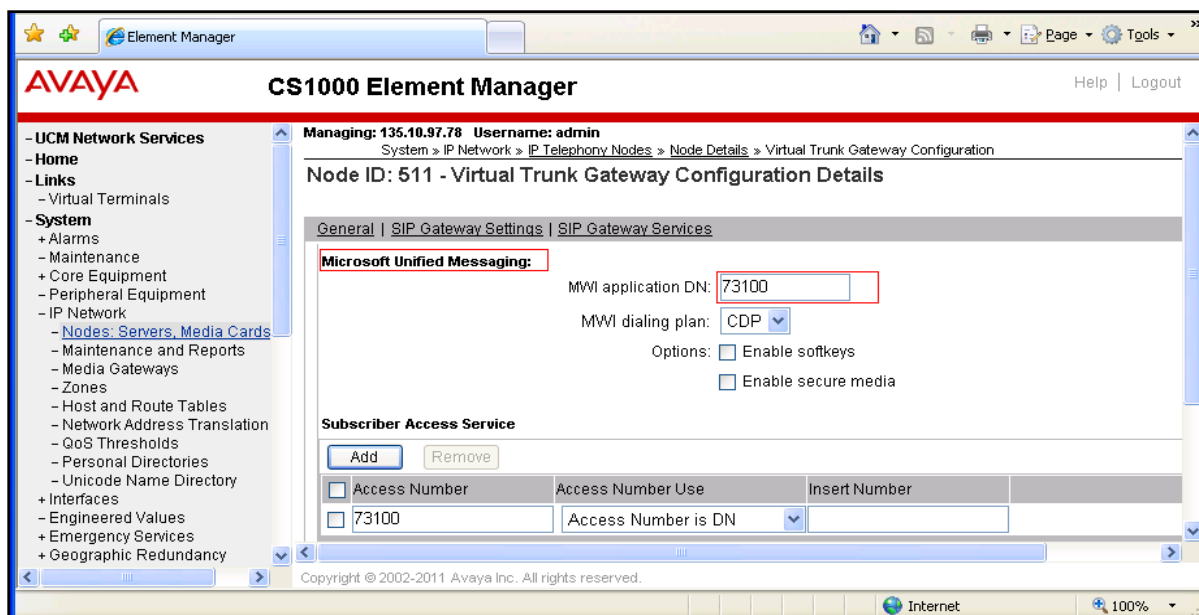


Figure 12: Microsoft Unified Messaging

Scroll down to **Subscriber Access Service** and **Auto Attendant Service** of **SIP Gateway Services** section, click on **Add** button in each service to add number “73100” for subscriber access and number “73200” for auto attendant. Note: The number “73100” and “73200” will be defined in **Section 5.6.2**.

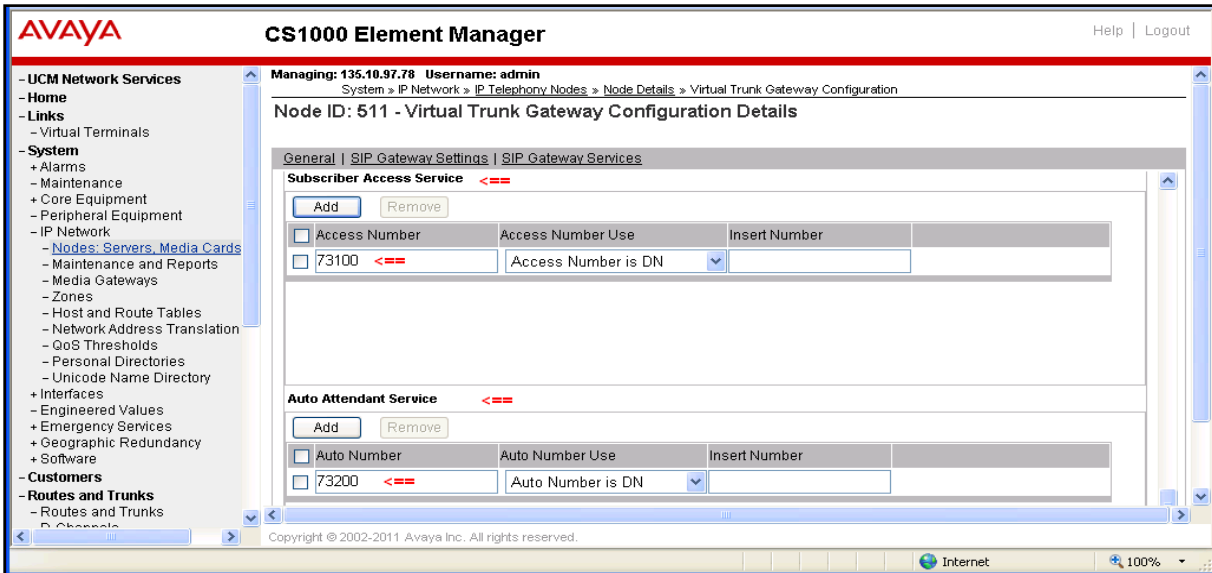


Figure 13: Subscriber Access Service and Auto Attendant Service

Click on the **Save** button at the bottom of **Node ID: 511 - Virtual Trunk Gateway Configuration Details** page (not shown) to save the changes in the **Node ID: 511**, the **Node ID 511 - Virtual Trunk Gateway Configuration Detail** page, which will be closed and returned back to the **Node Details (ID: 511 - LTPS, Gateway (SIPGw))** page. Click on **Save** button in this page and the **Node Saved** window displays as shown in **Figure 14**.

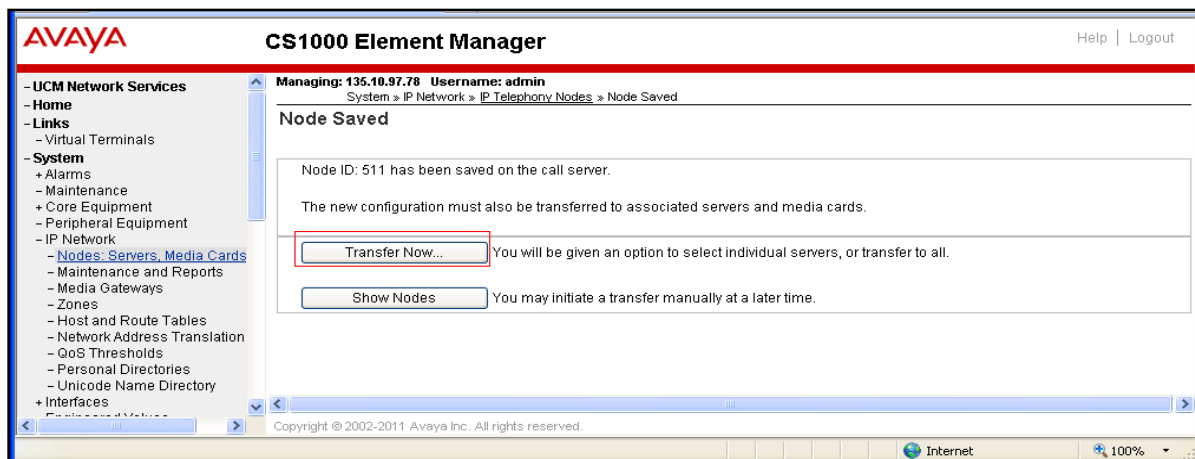


Figure 14: Node Saved Page

Click on the **Transfer Now...** button in **Figure 14** to display the **Synchronize Configuration Files (Node ID)** page. Click on associated signaling server “*cpppm3*” that the new configurations need to be transferred to and click on the **Start Sync** button to start transferring the changes to Call Server.

Note: The process of saving, transferring and synchronizing need to be applied if any change is made in the **Node ID - Virtual Trunk Gateway Configuration Detail** page.

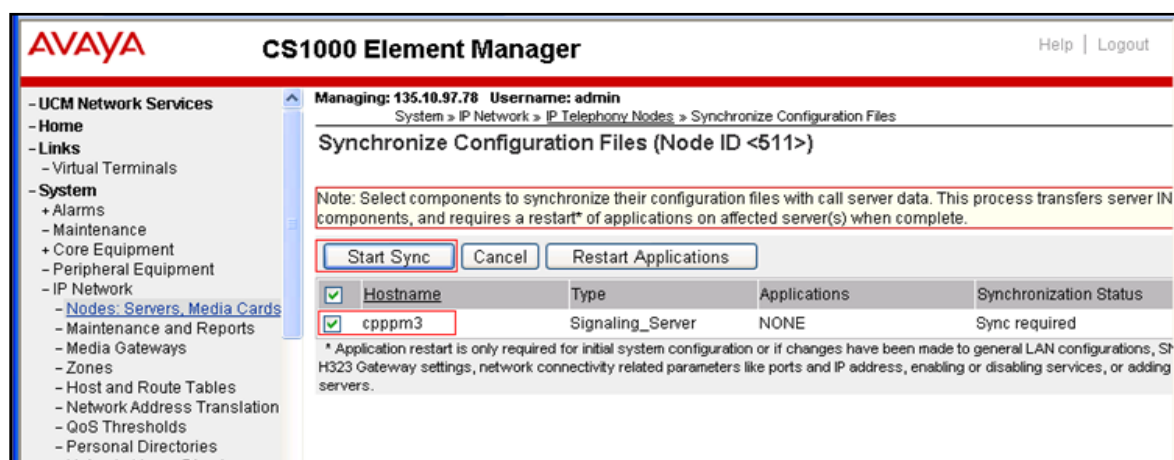


Figure 15: Synchronize Configuration Files (Node ID <551>) page

5.2. Configure D-Channel for SIP Trunk

Configure a D-Channel for SIP Trunk. From the Element Manager homepage, navigate to **Routes and Trunks > D-Channels** and select the **D-Channels** tab. The **D-Channels** page displays in the right-hand side of the page.

In the **Configuration** section of this page, select D-Channel number “4” which is available in the **Choose a D-Channels Number** dropdown list, select the type of D-Channel as **DCH** and click on the **to Add** button.

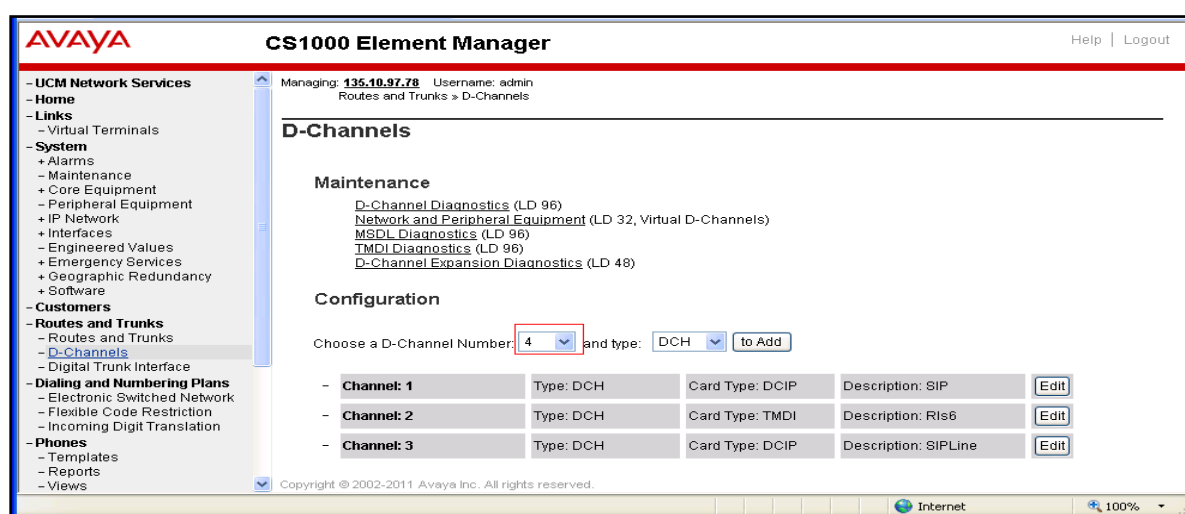


Figure 16: D-Channels Page

D-Channels 4 Property Configuration page displays. Enter information for **Basic Configuration** section:

- **D channel Card Type:** select “*D-Channel is over IP (DCIP)*”.
- **Designator:** type “SIP”.
- **Interface type for D-channel:** select “*Meridian Meridian 1 (SL1)*”.
- And keep other value of this section at default.

AVAYA CS1000 Element Manager

Routes and Trunks » D-Channels » D-Channels 4 Property Configuration

D-Channels 4 Property Configuration

- Basic Configuration <==

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type:	D-Channel is over IP (DCIP) *
Designator:	SIP
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User:	Integrated Services Signaling Link Dedicated (ISLD) *
Interface type for D-channel:	Meridian Meridian1 (SL1) *
Country:	ETS 300=102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	<input type="text"/> more PRI
Secondary PRI2 loops:	<input type="text"/>
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 Range: 1 - 4000
Signalling server resource capacity:	3700 Range: 0 - 3700

Copyright © 2002-2011 Avaya Inc. All rights reserved.

Figure 17: Basic Configuration Section of D-Channel

Scroll down and expand **Basic options (BSCOPT)** subsection of the **Basic Configuration** Section. Click on **Edit** button in the **Remote Capabilities** field.

AVAYA CS1000 Element Manager

Release ID of the switch at the far end: 25

Central Office switch type: 100% compatible with Bellcore standard (STD)

Integrated Services Signaling Link Maximum: 4000 Range: 1 - 4000

Signalling server resource capacity: 3700 Range: 0 - 3700

- Basic options (BSCOPT)

Primary D-channel for a backup DCH: Range: 0 - 254

- PINX customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffers: 32

- D-channel transmission Rate: 56 kb/s when LCMT is AMI (56K)

- Channel Negotiation option: No alternative acceptable, exclusive. (1)

- Remote Capabilities: **Edit** <==

+ - Change protocol timer value (TIMR)

Copyright © 2002-2011 Avaya Inc. All rights reserved.

Figure 18: Basic Options (BSCOPT) Page

The **Remote Capability Configuration** page is displayed. Select “*Network name display method 2 (ND2)*” and keep other values unchecked. Click on **Return-Remote Capability** button at the bottom to return back to the **D-Channel 4 Property Configuration** page.

AVAYA CS1000 Element Manager

Help | Logout

- UCM Network Services
 - Home
 - Links
 - Virtual Terminals
 - System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - + IP Network
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Geographic Redundancy
 - + Software
 - Customers
 - Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
 - Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation
 - Phones
 - Templates
 - Reports
 - Views
 - Lists
 - Properties
 - Migration
 - Tools
 - + Backup and Restore
 - Date and Time
 - + Logs and reports

Remote D-channel is on a MSXL card (MSL) ☐

Message waiting interworking with DMS-100 (MWM) ☐

Network access data (NAC) ☐

Network call trace supported (NCT) ☐

Network name display method 1 (ND1) ☐

Network name display method 2 (ND2) ☒

Network name display method 3 (ND3) ☐

Name display - integer ID coding (NDI) ☐

Name display - object ID coding (NDO) ☐

Path replacement uses integer values (PRI) ☐

Path replacement uses object identifier (PRO) ☐

Release Link Trunks over IP (RLTI) ☐

Remote virtual queuing (RVQ) ☐

Trunk anti-tromboning operation (TAT) ☐

User to user service 1 (UUS1) ☐

NI-2 name display option. (NDS) ☐

Message waiting indication using integer values (QMWI) ☐

Message waiting indication using object identifier (QMWVO) ☐

User to user signalling (UUI) ☐

Return - Remote Capabilities Cancel

Copyright © 2002-2011 Avaya Inc. All rights reserved.

Figure 18: Remote Capabilities Configuration Page of D-Channel

Keep other sections of **D-Channel 4 Property Configuration** page at default and click on **Submit** button to complete creation for D-Channel “4”.

AVAYA CS1000 Element Manager

Help | Logout

- UCM Network Services
 - Home
 - Links
 - Virtual Terminals
 - System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - + IP Network
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Geographic Redundancy
 - + Software
 - Customers
 - Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
 - Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation

D-Channel PRI loop number:

Primary Rate Interface: more PRI

Secondary PRI2 loops:

Meridian 1 node type: Slave to the controller (USR)

Release ID of the switch at the far end: 25

Central Office switch type: 100% compatible with Bellcore standard (STD)

Integrated Services Signaling Link Maximum: 200 Range: 1 - 4000

Signalling server resource capacity: 3700 Range: 0 - 3700

+ Basic options (BSCOPT)

+ Advanced options (ADVOPT)

+ Feature Packages

Submit Refresh Delete Cancel

Copyright © 2002-2011 Avaya Inc. All rights reserved.

Figure 19: D-Channel 4 Property Configuration Page

5.3. Configure Bandwidth Zone

Configure a bandwidth zone. From the Element Manager homepage, navigate to menu **System** > **IP Network** > **Zones** and select the **Zones** tab. The **Zones** page displays in the right-hand side. Click on the **Bandwidth Zones** link.

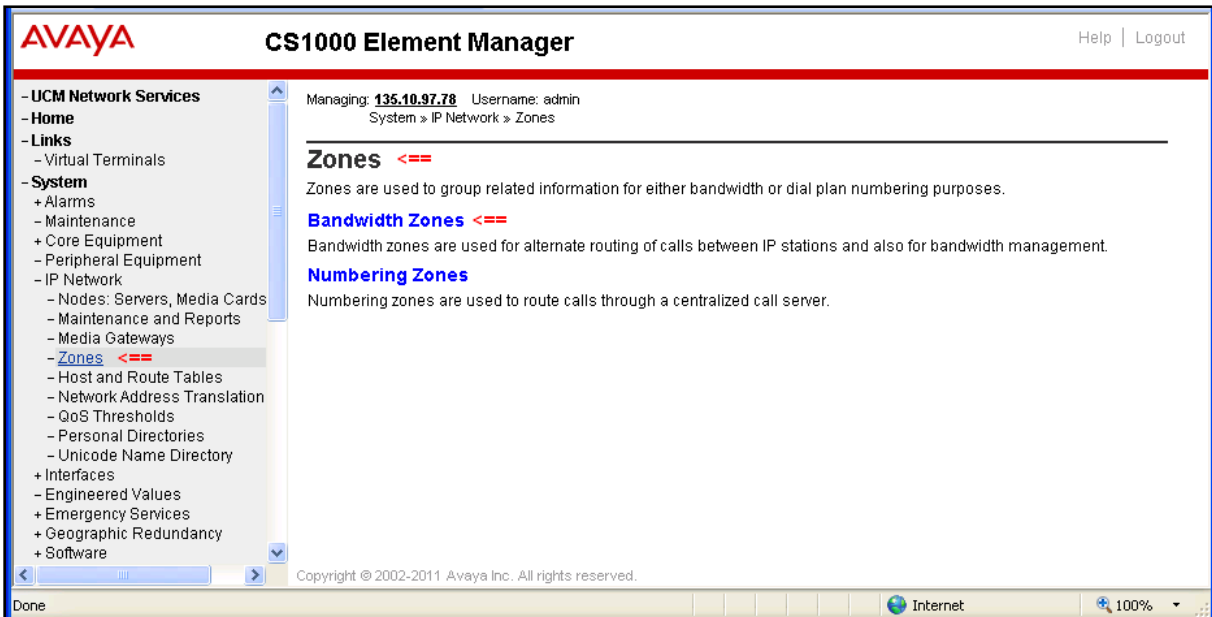


Figure 20: Zones Page

The **Bandwidth Zones** page displays. Click on **Add** button to create a new zone.

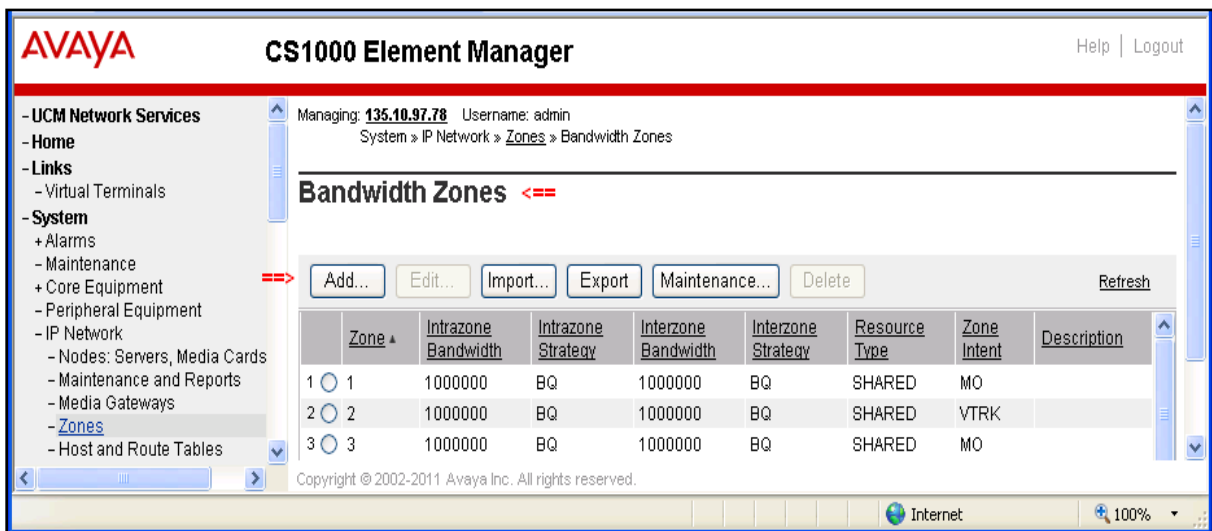


Figure 21: Bandwidth Zones Page

The **Zone Basic Property and Bandwidth Management** page is displayed. Enter information as below:

- **Zone Number (ZONE):** enter “4”.
- **Zone Intent (ZBRN):** select “VTRK (VTRK)”. Due to this zone is for virtual trunk.
- **Description (ZDES):** enter “VTRK”.
- And keep other fields at default.

Click on **Save** button to complete.

AVAYA CS1000 Element Manager Help | Logout

Managing: **135.10.97.78** Username: admin
System » IP Network » Zones » Bandwidth Zones » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management <==

Input Description	Input Value
Zone Number (ZONE):	4 <== * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ) <==
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ) <==
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	VTRK (VTRK) <==
Description (ZDES):	VTRK

* Required value. Save Cancel

Copyright © 2002-2011 Avaya Inc. All rights reserved.

Figure 22: Zone Basic Property and Bandwidth Management

5.4. Configure SIP Route

Configure a SIP Route. From the Element Manager homepage, navigate to **Routes and Trunks** > **Routes and Trunks**. The **Routes and Trunks** page is displayed in the right-hand side.

Identify customer to which the new route is going to be added (for this test there is just one customer, Customer 0, in the CS 1000 system) and click on the **Add route** button.

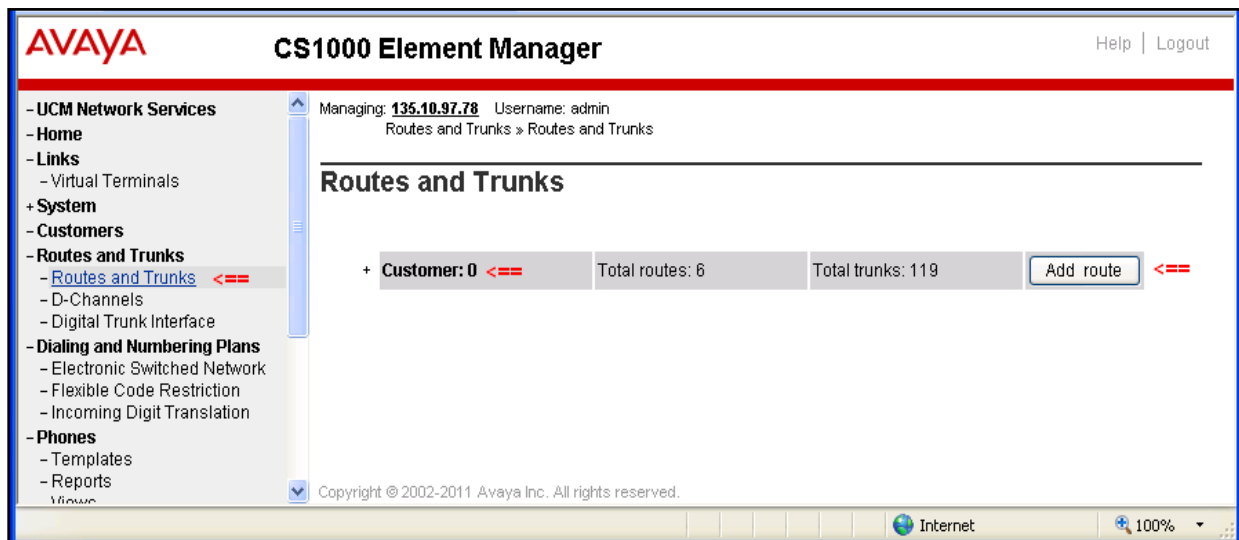


Figure 23: Routes and Trunks Page

The **Customer 0, New Route Configuration** page displays with 5 sections: **Basic Configuration**, **Basic Route Options**, **Network Options**, **General Options**, and **Advanced Configurations**.

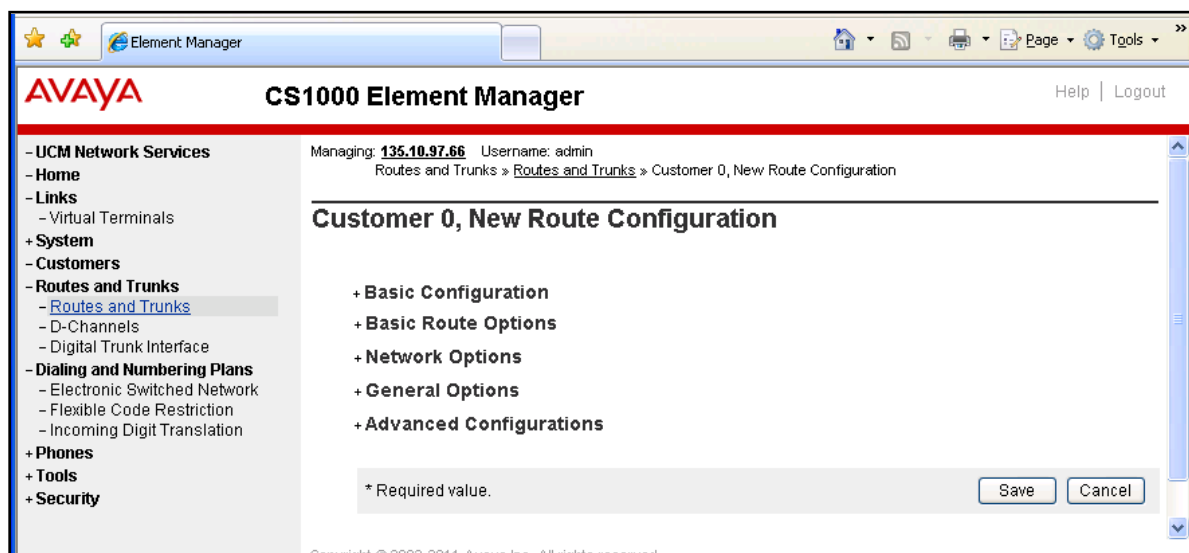


Figure 24: New Route Configuration Page

Expand the **Basic Configuration** section and enter information for this section as below:

- **Route number (ROUT):** select available rout number “1” in dropdown menu.
- **Designator field for trunk (DES):** type “SIP”.
- **Trunks type (TKTP):** select “TIE trunk data block (TIE)”.
- **Incoming and outgoing trunk (ICOG):** select “Incoming and Outgoing (IAO)”.
- **Access code for the trunk route (ACOD):** type “8001”. Note: This number belongs to the directory number in CS 1000 system; it can be any number but must be unique and followed by dialing plan.
- **The route if for a virtual trunk route (VTRK):** Checked
- **Zone ID for codec selection and bandwidth management (ZONE):** type “4” as defined in Section 5.3.
- **Node ID of signaling server of this route (NODE):** type “511”. This is Node ID of SIP Gateway.
- **Integrated services digital network option (ISDN):** Check on this checkbox, the next figure will display options of this feature.
- **Calling number dialing plan (CPND):** select “Coordinated dialing plan (CDP)” as CDP dialing plan is used for this route.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The left sidebar contains a navigation menu with categories like UCM Network Services, System, Customers, Routes and Trunks, and Tools. The main content area is titled 'Customer 0, New Route Configuration' and shows the 'Basic Configuration' section expanded. The configuration fields are as follows:

- Route data block (RDB) (TYPE): RDB
- Customer number (CUST): 0
- Route number (ROUT): 1
- Designator field for trunk (DES): SIP
- Trunk type (TKTP): TIE trunk data block (TIE)
- Incoming and outgoing trunk (ICOG): Incoming and Outgoing (IAO)
- Access code for the trunk route (ACOD): 8001
- Trunk type M911P (M911P): ☐
- The route is for a virtual trunk route (VTRK): ☒
- Zone for codec selection and bandwidth management (ZONE): 4 (0 - 8000)
- Node ID of signaling server of this route (NODE): 511 (0 - 9999)
- Protocol ID for the route (PCID): SIP (SIP)
- Print correlation ID in CDR for the route (CRID): ☐
- Integrated services digital network option (ISDN): ☒ (indicated by a red triple equals sign)
- Calling number dialing plan (CNDP): Coordinated dialing plan (CDP)

Below the configuration fields is the '+ Basic Route Options' section. The footer of the interface shows the copyright notice 'Copyright © 2002-2011 Avaya Inc. All rights reserved.' and a status bar with 'Internet' and '100%' zoom level.

Figure 25: Basic Configuration Section of New Route

The **Integrated services digital network option (ISDN)** subsection displays. Enter information as below:

- **Mode of Operation (MODE):** select “*Route uses ISDN Signaling Link (ISLD)*”.
- **D Channel number (DCH):** select “*4*” as defined in **Section 6.2**.
- **Interface Time For Route (IFC):** select “*Meridian 1 (SL1)*”.
- **Private Network Identifier (PNI):** type “*1*”.
- **Network Calling Name Allowed (NCNA):** Checked.
- **Network call redirection (NCRD):** Checked.
- **Call type for outgoing direct dialed TIE route:** select “*Coordinated Dialing Plan (CDP)*”.
- And keep other fields at default.

The screenshot displays the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories like UCM Network Services, System, Customers, Routes and Trunks, and Phones. The 'Routes and Trunks' section is expanded, showing 'Routes and Trunks' as the selected item. The main content area is titled 'Integrated services digital network option (ISDN)' and contains various configuration fields. A red bar at the top of the main area contains the text 'Print correlation ID in CDR for the route (CRID)'. The configuration fields include: 'Mode of operation (MODE)' set to 'Route uses ISDN Signaling Link (ISLD)', 'D channel number (DCH)' set to '4', 'Interface type for route (IFC)' set to 'Meridian M1 (SL1)', 'Private network identifier (PNI)' set to '1', 'Network calling name allowed (NCNA)' checked, 'Network call redirection (NCRD)' checked, 'Trunk route optimization (TRO)' unchecked, 'Recognition of DTI2 ABCD FALT signal for ISL (FALT)' unchecked, 'Channel type (CHTY)' set to 'B-channel (BCH)', 'Call type for outgoing direct dialed TIE route (CTYP)' set to 'Coordinated Dialing Plan (CDP)', 'Insert ESN access code (INAC)' unchecked, 'Integrated service access route (ISAR)' unchecked, 'Display of access prefix on CLID (DAPC)' unchecked, 'Mobile extension route (MBXR)' unchecked, 'Mobile extension outgoing type (MBXOT)' set to 'National number (NPA)', 'Mobile extension timer (MBXT)' set to '0', and 'Calling number dialing plan (CNDP)' set to 'Coordinated dialing plan (CDP)'. At the bottom of the main area is a section for '+ Basic Route Options'. The footer of the page shows 'Copyright © 2002-2011 Avaya Inc. All rights reserved.' and a status bar with 'Internet' and '100%'.

Figure 26: ISDN Option Page

Scroll down and expand the **Basic Route Options** section and keep all fields at default.

The screenshot shows the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories like UCM Network Services, System, Customers, Routes and Trunks, and Phones. The 'Routes and Trunks' section is expanded, and 'Routes and Trunks' is selected. The main content area is titled '- Basic Route Options <=='. It contains several configuration fields: 'Attendant announcement (ATAN)' is a dropdown menu set to 'No Attendant Announcement. (NO)'; 'Billing number required (BILN)' is a checkbox; 'Call detail recording (CDR)' is a checkbox; 'North American toll scheme (NATL)' is a checkbox checked with a green checkmark; 'Controls or timers (CNTL)' is a checkbox; 'Conventional (Tie trunk only) (CNVT)' is a checkbox; 'Incoming DID digit conversion on this route (IDC)' is a checkbox; 'Multifrequency compelled or MFC signaling (MFC)' is a dropdown menu; and 'Process notification networked calls (PNNC)' is a checkbox. Below these are sections for '+ Network Options', '+ General Options', and '+ Advanced Configurations'. The footer shows 'Copyright © 2002-2011 Avaya Inc. All rights reserved.' and a status bar with 'Internet' and '100%' zoom.

Figure 27: Basic Route Options of New Route

Expand the **Network Options** section and keep all fields at default.

The screenshot shows the AVAYA CS1000 Element Manager web interface with the 'Network Options' section expanded. The navigation tree on the left is the same as in Figure 27. The main content area is titled '- Network Options <=='. It contains several configuration fields: 'Electronic switched network pad control (ESN)' is a checkbox; 'Signaling arrangement (SIGO)' is a dropdown menu set to 'Standard (STD)'; 'Route class (RCLS)' is a dropdown menu set to 'Route Class marked as external (EXT)'; 'Off-hook queuing (OHQ)' is a checkbox; 'Off-hook queue threshold (OHQT)' is a dropdown menu set to '0'; 'Call back queuing (CBQ)' is a checkbox; 'Number of digits (NDIG)' is a dropdown menu set to '2'; and 'Authcode (AUTH)' is a checkbox. Below these are sections for '+ General Options' and '+ Advanced Configurations'. At the bottom, there is a note '* Required value.' and 'Save' and 'Cancel' buttons. The footer shows 'Copyright © 2002-2011 Avaya Inc. All rights reserved.' and a status bar with 'Internet' and '100%' zoom.

Figure 28: Network Options of New Route

Expand the **General Options** section and keep all fields at default.

The screenshot shows the AVAYA CS1000 Element Manager web interface. The left sidebar contains a navigation tree with categories: UCM Network Services, Home, Links, System, Customers, Routes and Trunks (selected), and Phones. Under 'Routes and Trunks', 'Routes and Trunks' is selected. The main content area is titled '- General Options <=='. It contains several configuration fields: 'M1 is the only controlling party on incoming calls (CPDC):' with a checkbox; 'Dial tone on originating calls (DLTN):' with a checkbox; 'Hold failure threshold (HOLD):' with a text input field; 'Trunk access restriction group (TARG):' with a text input field; 'Alternate trunk route for outgoing trunks (STEP):' with a text input field and '(0 - 511)' to its right; 'Actual outgoing toll digits to be ignored for code restriction (OABS):' with a text input field; 'Display IDC name (DNAM):' with a checkbox; 'Enable equal access restrictions (EQAR):' with a checkbox; 'ACD DNIS route (DNIS):' with a checkbox; and 'Include DNIS number in CDR records (DCDR):' with a checkbox. Below these is a section titled '+ Advanced Configurations'. At the bottom, there is a copyright notice: 'Copyright © 2002-2011 Avaya Inc. All rights reserved.' and a status bar showing 'Internet' and '100%' zoom.

Figure 29: General Options of New Route

Keep all fields at default in the **Advanced Configurations** section.

Click on **Save** button to complete creating the SIP route “1”.

The screenshot shows the AVAYA CS1000 Element Manager web interface. The left sidebar is the same as in Figure 29. The main content area is titled '+ Basic Route Options'. It contains a list of expandable sections: '+ Network Options', '+ General Options', and '+ Advanced Configurations <=='. Below these is a grey box with the text '* Required value.' followed by a red double arrow icon '==>'. To the right of this box are two buttons: 'Save' and 'Cancel'. At the bottom, there is a copyright notice: 'Copyright © 2002-2011 Avaya Inc. All rights reserved.' and a status bar showing 'Internet' and '100%' zoom.

Figure 30: Advanced Configuration Section

5.5. Configure IP Trunks

Configure IP Trunks, from the Element Manager homepage, navigate to **Routes and Trunks > Routes and Trunks**. The **Routes and Trunks** page displays in the right-hand side. Expand Customer number (Customer 0) and click on **Add trunk** button on the left of **Route 1** which is created in **Section 5.4** above.

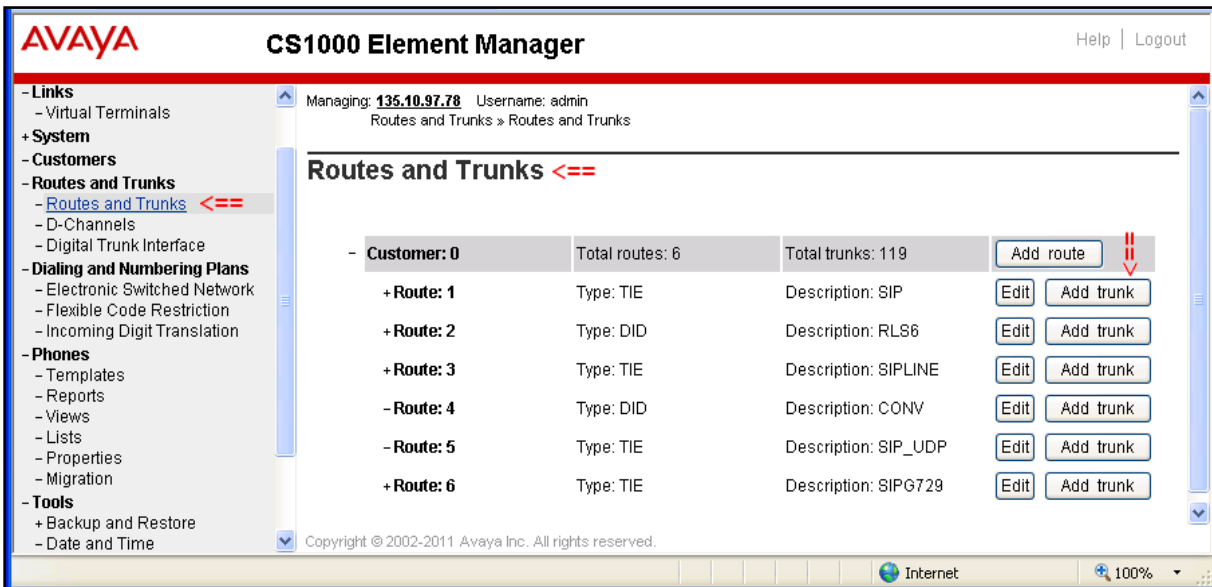


Figure 31: Routes and Trunks Page

The **Customer 0, Route 1, Trunk type TIE trunk data block** page displays with two sections: **Basic Configuration** and **Advanced Trunk Configuration**.

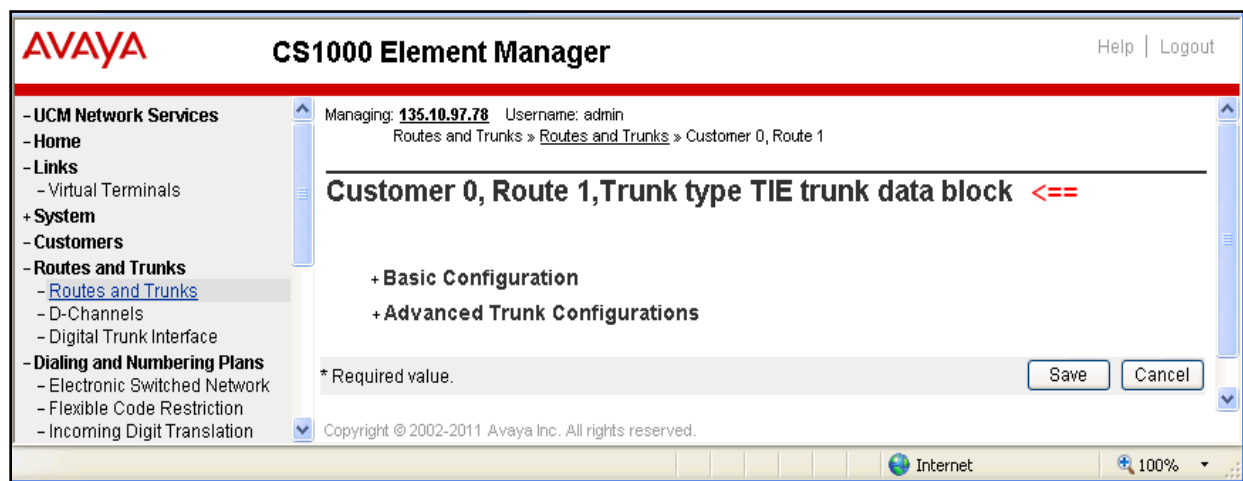


Figure 32: Trunk Type TIE Trunk Data Block Page

Expand the **Basic Configuration** section, enter information as below:

- **Trunk data block:** select “*IP Trunk (IPTI)*”.
- **Multiple trunk input number:** type “32”. 32 IP Trunks will be created.
- **Terminal number:** type “100 0 0 0”. Note: This is virtual terminal card, make sure virtual super loop 100 is already configured in your system and it is available for creating these IP Trunks.
- **Designator field for trunk:** type “SIP”.
- **Member number:** enter “1”. Input as “1” if this is first trunk in this route, in case there are existent trunks in the route, this number should be next number of last trunk. This number is automatically incremented from 1 to 32 as 32 multiple trunks entered in the **Multiple trunk input number** field.
- **Start arrangement Incoming:** select “*Immediate (IMM)*”.
- **Start arrangement Outgoing:** select “*Immediate (IMM)*”.
- **Trunk group access restriction:** enter “1”.
- **Channel ID for this trunk:** enter “1”. This channel ID should be unique for IP trunks located in same route. This number is also automatically incremented from 1 to 32.
- Click on **Edit** button in **Class of Service** field. The next figure will show detailed class of service for IP trunk.

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with categories like UCM Network Services, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The 'Routes and Trunks' section is expanded, showing 'Routes and Trunks' as the selected item. The main area is titled '- Basic Configuration <=='. It contains several fields: 'Multiple trunk input number' (32, Range: 2 - 3700), 'Auto increment member number' (checked), 'Trunk data block' (IP Trunk (IPTI)), 'Terminal number' (100 0 0 0), 'Designator field for trunk' (SIP), 'Extended trunk' (VTRK), 'Member number' (1), 'Level 3 Signaling' (dropdown), 'Card density' (dropdown), 'Start arrangement Incoming' (Immediate (IMM)), 'Start arrangement Outgoing' (Immediate (IMM)), 'Trunk group access restriction' (1), 'Channel ID for this trunk' (1), and 'Class of Service' (Edit button). There are red double equals signs next to several fields. At the bottom, there is a '+ Advanced Trunk Configurations' section, a '* Required value.' note, and 'Save' and 'Cancel' buttons. The footer shows 'Copyright © 2002-2011 Avaya Inc. All rights reserved.' and a browser status bar with 'Internet' and '100%' zoom.

Figure 33: Basic Configuration of New Trunk

The **Class of Service Configuration** page displays.

- **Media Security:** select “*Media Security Never (MSNV)*”. This field will be changed to “Media Security Best Try (MSBT)” when SIP TLS and secure media are tested.
- **Restriction level:** “*Unrestricted (UNR)*”.
- Keep other fields at default and click on **Return Class of Service** button to go back to the **Customer 0, Route 1, Trunk type TIE trunk data block** page.

Figure 34: Class of Service of New Trunk

Keep all fields at default in the **Advanced Trunks Configurations** section. And then click on **Save** button to complete creating these IP virtual trunks.

Figure 35: Class of Service of New Trunk (cont)

Figure 36 below displays 32 new IP trunks are created in the **Route 1**.

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with categories like UCM Network Services, Links, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The 'Routes and Trunks' section is expanded, showing 'Routes and Trunks' and 'D-Channels'. The main area displays a table for 'Customer: 0' with 'Total routes: 6' and 'Total trunks: 119'. A red box highlights the 'Route: 1' section, which shows 'Type: TIE', 'Description: SIP', and a list of 32 trunks. Each trunk has a 'TN' (Trunk Number) and a 'Description: SIP'. Buttons for 'Edit' and 'Multi - Del' are visible next to each trunk entry.

Customer	Total routes	Total trunks
Customer: 0	6	119

Route	Type	Description
Route: 1	TIE	SIP
Trunk: 1 - 32	Total trunks: 32	
Trunk: 1	TN: 100 0 00 00	Description: SIP
Trunk: 2	TN: 100 0 00 01	Description: SIP
Trunk: 3	TN: 100 0 00 02	Description: SIP
Trunk: 4	TN: 100 0 00 03	Description: SIP
Trunk: 5	TN: 100 0 00 04	Description: SIP
Trunk: 6	TN: 100 0 00 05	Description: SIP
Trunk: 7	TN: 100 0 00 06	Description: SIP
Trunk: 8	TN: 100 0 00 07	Description: SIP
Trunk: 9	TN: 100 0 00 08	Description: SIP
Trunk: 10	TN: 100 0 00 09	Description: SIP
Trunk: 11	TN: 100 0 00 10	Description: SIP
Trunk: 12	TN: 100 0 00 11	Description: SIP
Trunk: 13	TN: 100 0 00 12	Description: SIP
Trunk: 14	TN: 100 0 00 13	Description: SIP
Trunk: 15	TN: 100 0 00 14	Description: SIP
Trunk: 16	TN: 100 0 00 15	Description: SIP
Trunk: 17	TN: 100 0 00 16	Description: SIP

Figure 36: 32 New IP Trunks Created

5.6. Configure CDP Dialing Plan

This section provides the steps on how to create a new Route List Index (RLI) and new Distant Steering Codes (DSC) for Exchange UM in CS 1000 system.

5.6.1. Configure Route List Block Index (RLI)

Configure a Route List Block Index. From the Element Manger homepage, navigate to **Dialing and Numbering Plan > Electronic Switched Network**. The **Electronic Switched Network (ESN)** page displays.

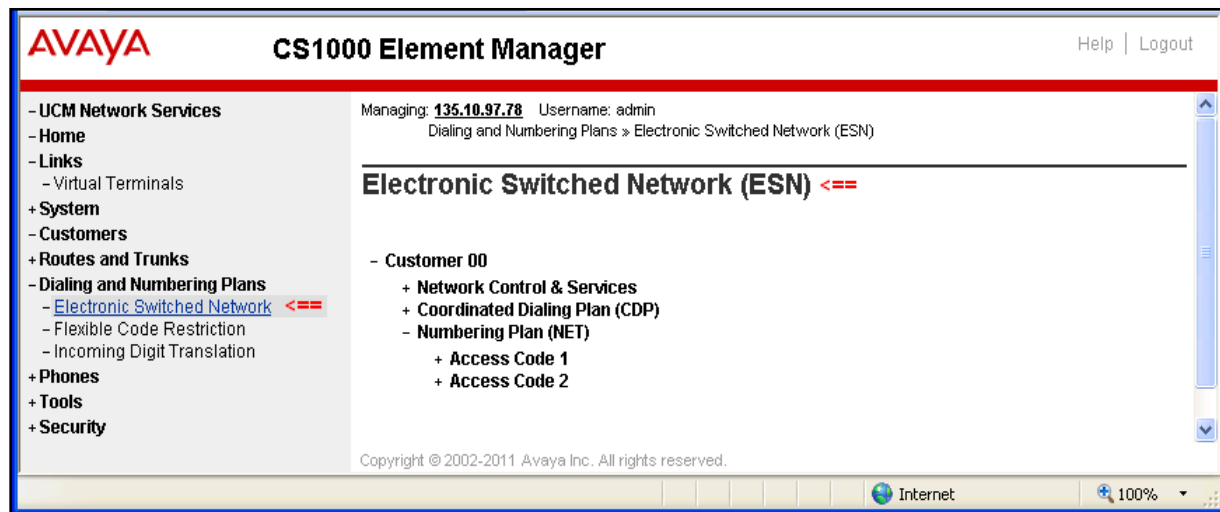


Figure 37: Electronic Switched Network (ESN) Page

Expand **Network Control & Services** and click on **Route List Block (RLB)** link.

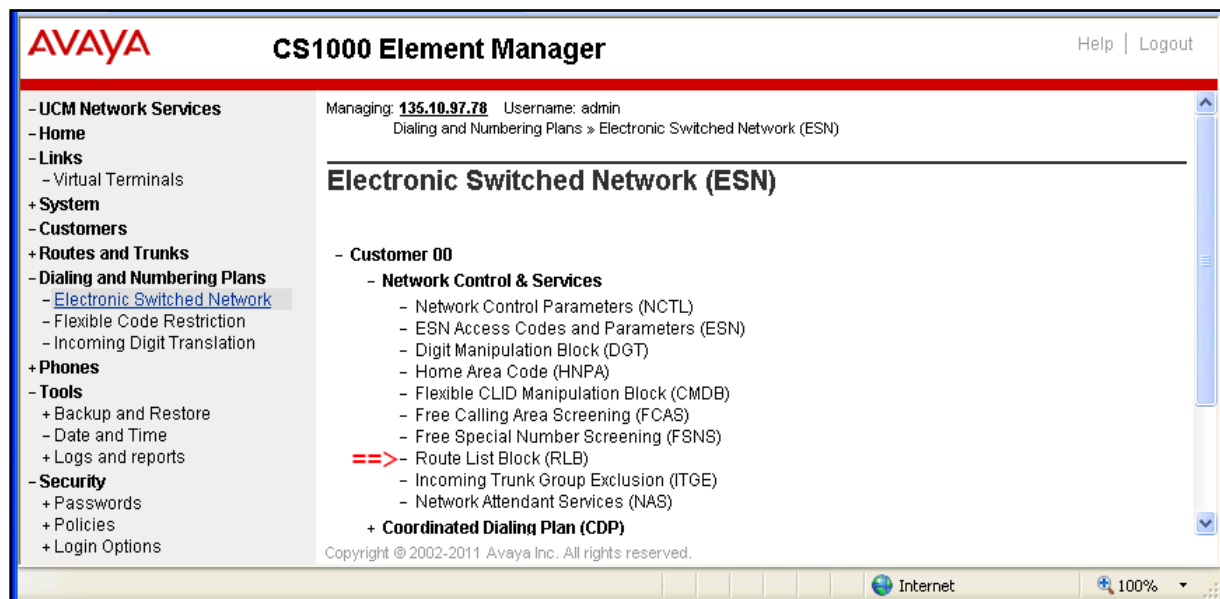


Figure 38: Network Control & Services Section

The **Route List Blocks** page is displayed. Enter “1” which is free number in **Please enter a route list index** box and then click on **Add** button.

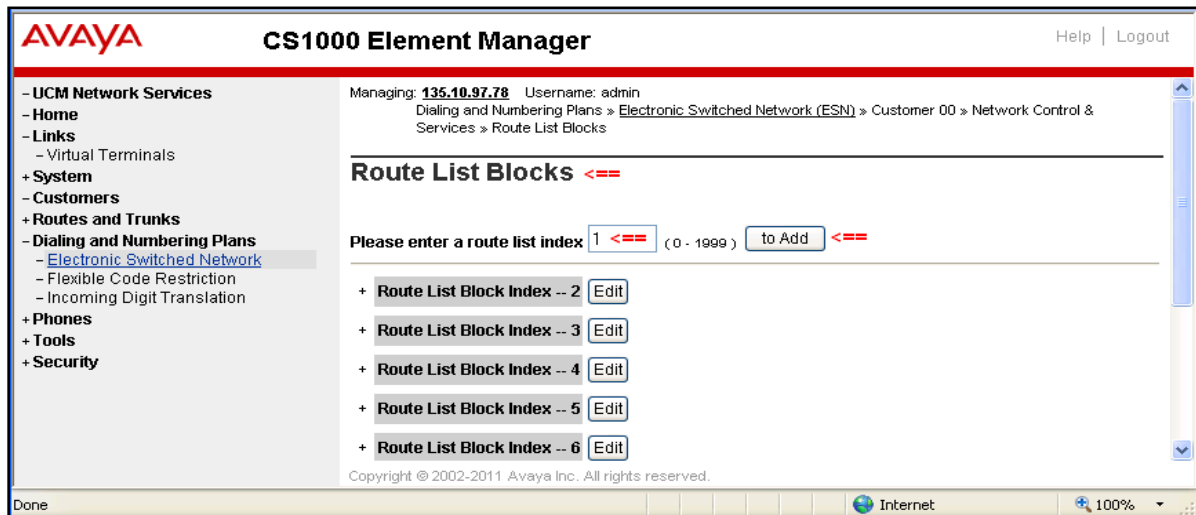


Figure 39: Route List Blocks page

The **Route List Block** page of route list index “1” page displays. In the **Options** section, select route “1” which is the SIP Route created in **Section 5.4** in **Route Number** dropdown menu. Keep other fields at default and click on **Submit** button to complete creating the new route list block index “1”.

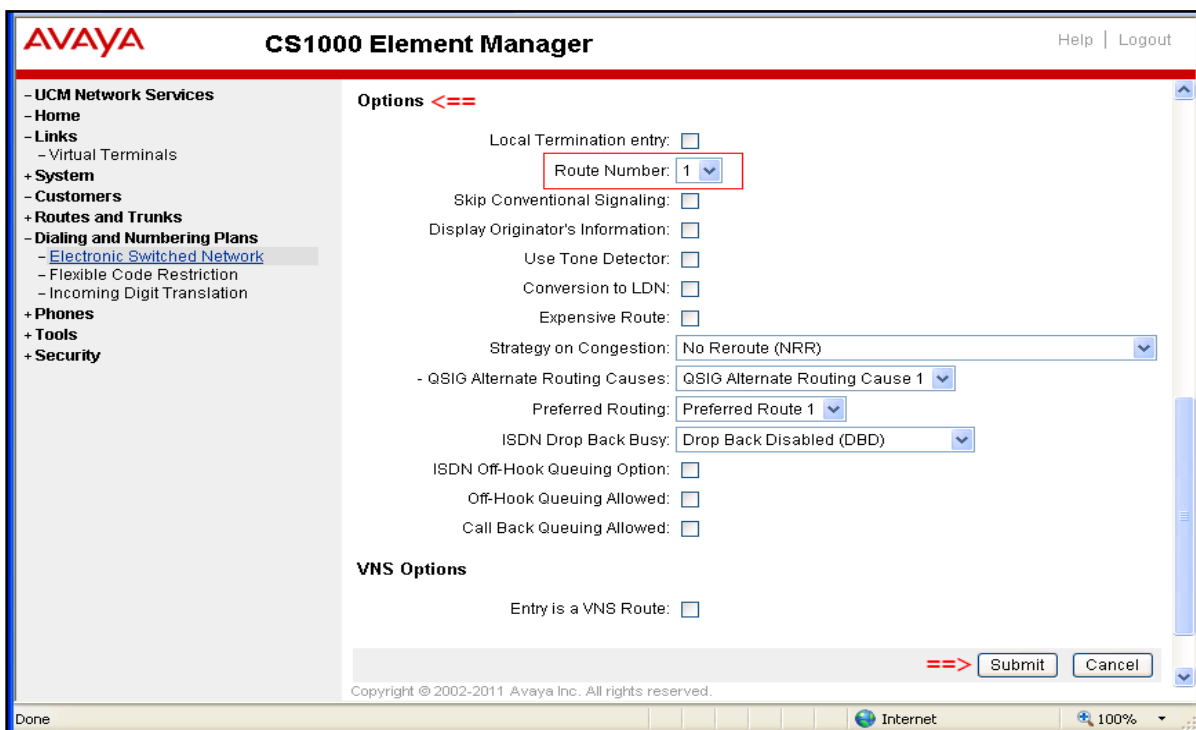


Figure 40: Detail of Route List Block Page

Figure 41 below shows the new route list block index “1” is created.

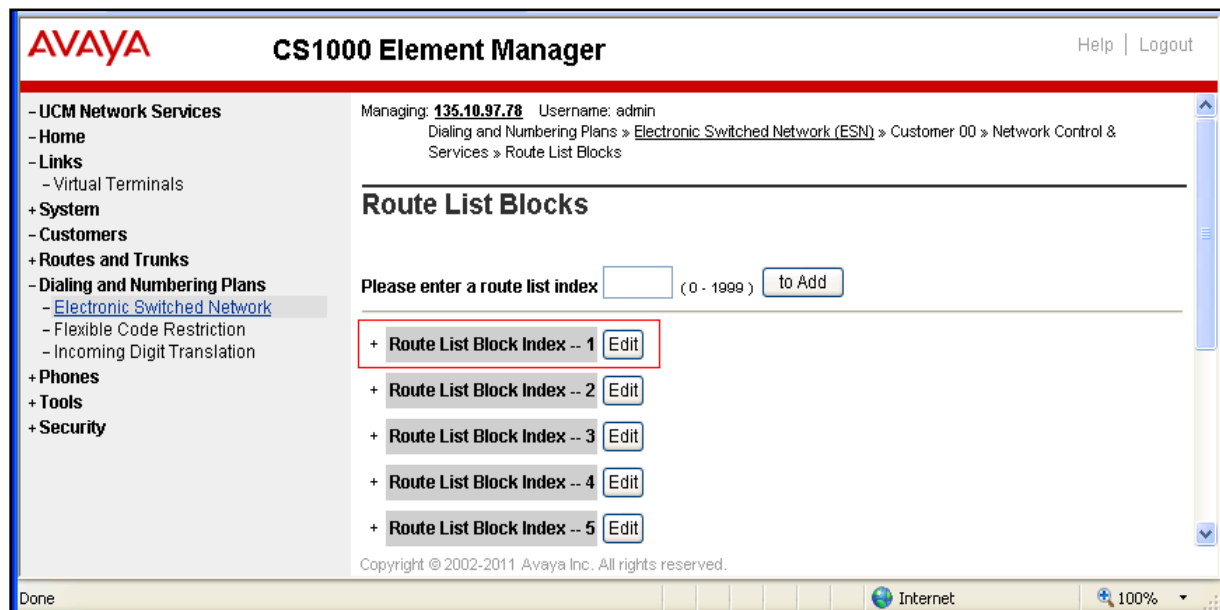


Figure 41: The new route list index “1” created

5.6.2. Configure Distant Steering Code (DSC)

Configure new distant steering code, from the Element Manager homepage, navigate to **Dialing and Numbering Plans > Electronic Switched Network > Coordinated Dialing Plan (CDP)** and select **Distant Steering Code (DSC)**.

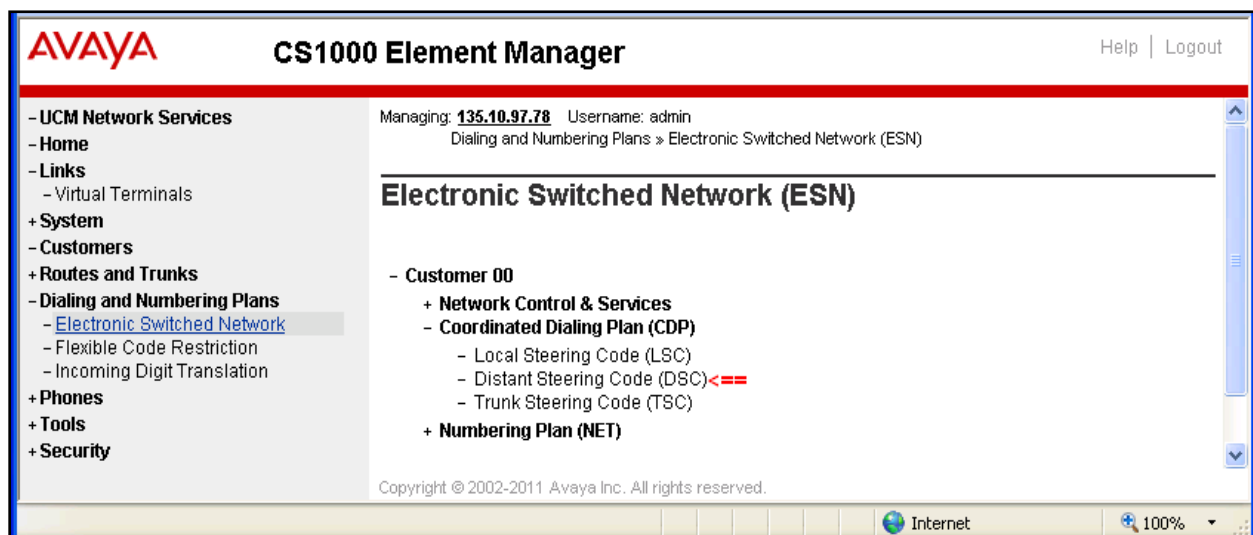


Figure 42: Distant Steering Code List page

The **Distant Steering Code List** page is displayed. Select **Add** in the dropdown menu and enter distant steering code number “73100” which is used as the UM subscriber number in **Please enter a distant steering code** box and click on **Add** button.

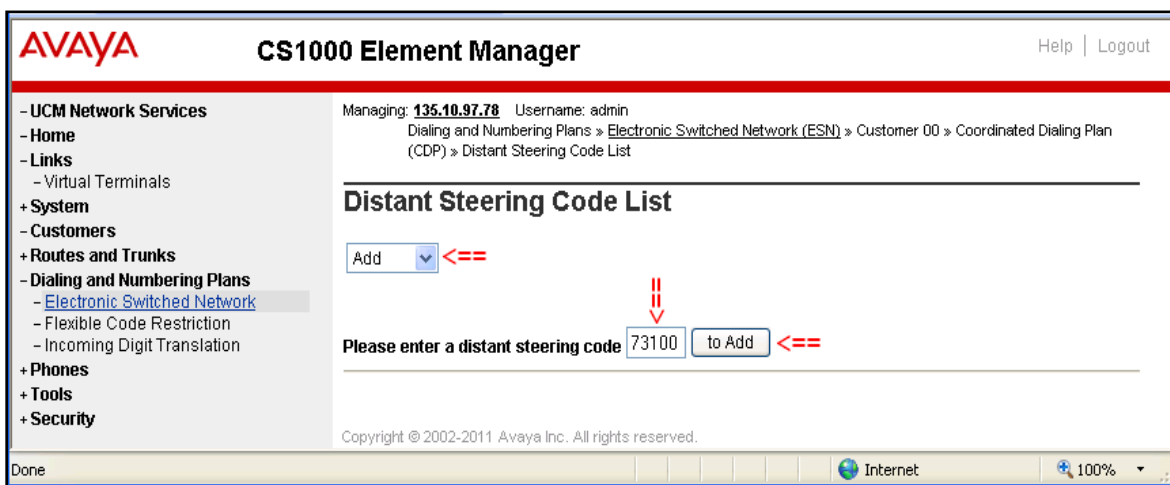


Figure 43: Distant Steering Code List Page

The **Distant Steering Code** of new code “73001” page displays. Enter information as below:

- **Flexible Length number of digits:** enter “5”. Due to 5 digits will be dialled.
- **Route List to be accessed for trunk steering code:** select “1” from dropdown menu list. This is the route list block index “1” created in **Section 5.6.1** above.
- Keep other fields at default and click on **Submit** button complete.

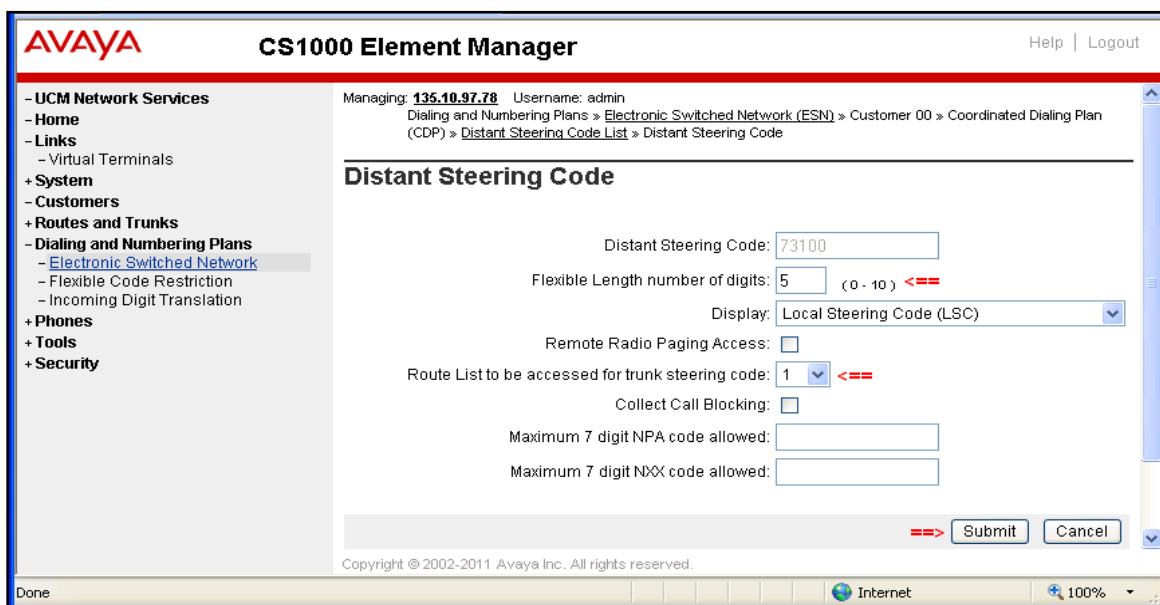


Figure 44: Distant Steering Code page

Repeat the same procedure above to create another distant steering code “73200” which is used as Auto Attendant number.

6. Configure Microsoft Exchange Unified Messaging 2010

This document assumes that the Microsoft Exchange UM 2010 server was properly installed and configured by a Microsoft engineer. This section provides the steps on how to configure Microsoft Exchange UM to work with an Avaya Communication Server 1000 system.

The following summarizes the tasks which need to be done on the Exchange UM:

- Configure a new UM Dial Plan.
- Configure a new UM IP Gateway.
- Configure a new UM IP Mailbox Policy.
- Configure a new UM Auto Attendant.

6.1. Configure a New UM Dial Plan

Configure a new UM dial plan on the Exchange UM, from the Exchange UM server; navigate to the menu **Start > All Programs > Microsoft Exchange Server 2010 > Exchange Management Console**, the **Exchange Management Console** displays.

In the Exchange Management Console, navigate to **Microsoft Exchange > Microsoft Exchange On-Premise > Organization Configuration**, right-click on **Unified Messaging** item and select **New UM Dial Plan**.

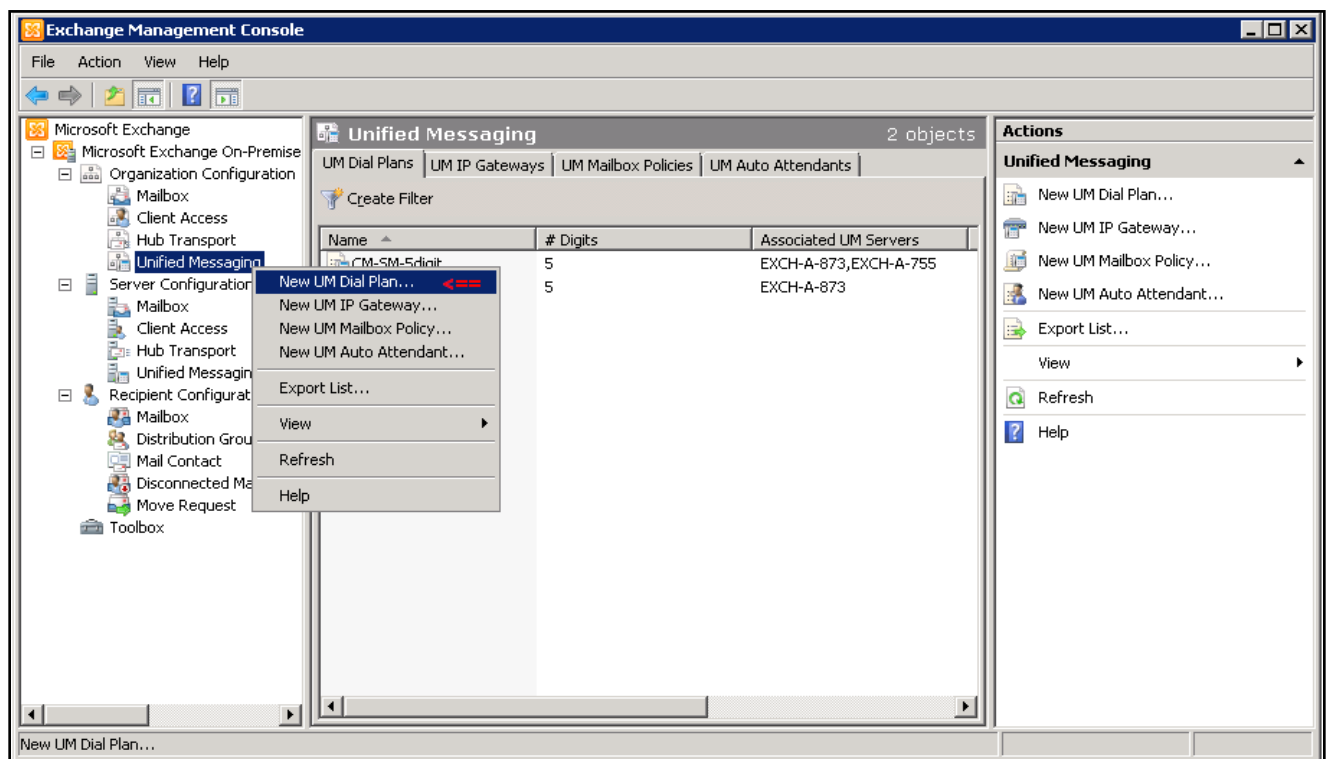


Figure 45: Exchange Management Console Window

The **New UM Dial Plan** window is displayed. Enter information for the new dial plan in the **Introduction** section as below:

- **Name:** type “*CS1K_CDP_5Digit*”.
- **Number of digits in extension numbers:** enter “5”.
- **URI:** select “*Telephone Extension*”.
- **VoIP Security:** select “unsecured”.

Click on the **Next** button to go to **Set UM Servers** section.

New UM Dial Plan

☒ Introduction
☐ Set UM Servers
☐ New UM Dial Plan
☐ Completion

Introduction
This wizard helps you create a UM dial plan for use by Microsoft Exchange Unified Messaging. A dial plan is a grouping of unique telephone extension numbers.

Name:
CS1K_CDP_5Digit

Number of digits in extension numbers:
5

URI type:
Telephone Extension

VoIP security:
Unsecured

Country/Region code:
1

Help < Back Next > Cancel

Figure 46: New UM Dial Plan Window

The **Set UM Servers** section of **New UM Dial Plan** window is displayed, click on **Add** button on right-hand of the window to add a new UM server.

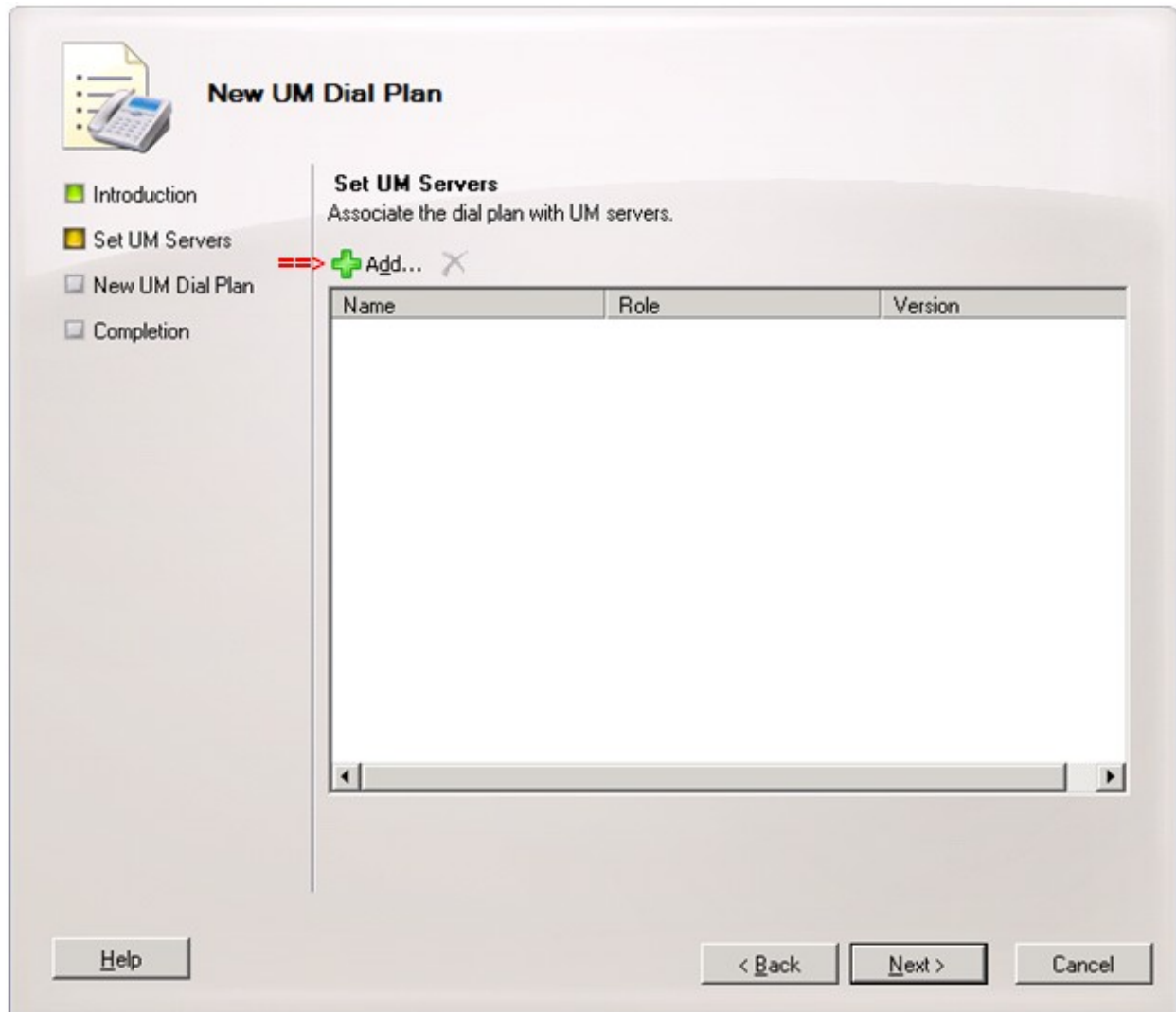


Figure 47: New UM Dial Plan Window (cont)

The **Select UM Server** window displays with two Exchange servers, select “*EXCH-A-873*” is Exchange UM 2010 server, select this server and then click **OK** button to complete and close the **Select UM Server** window.

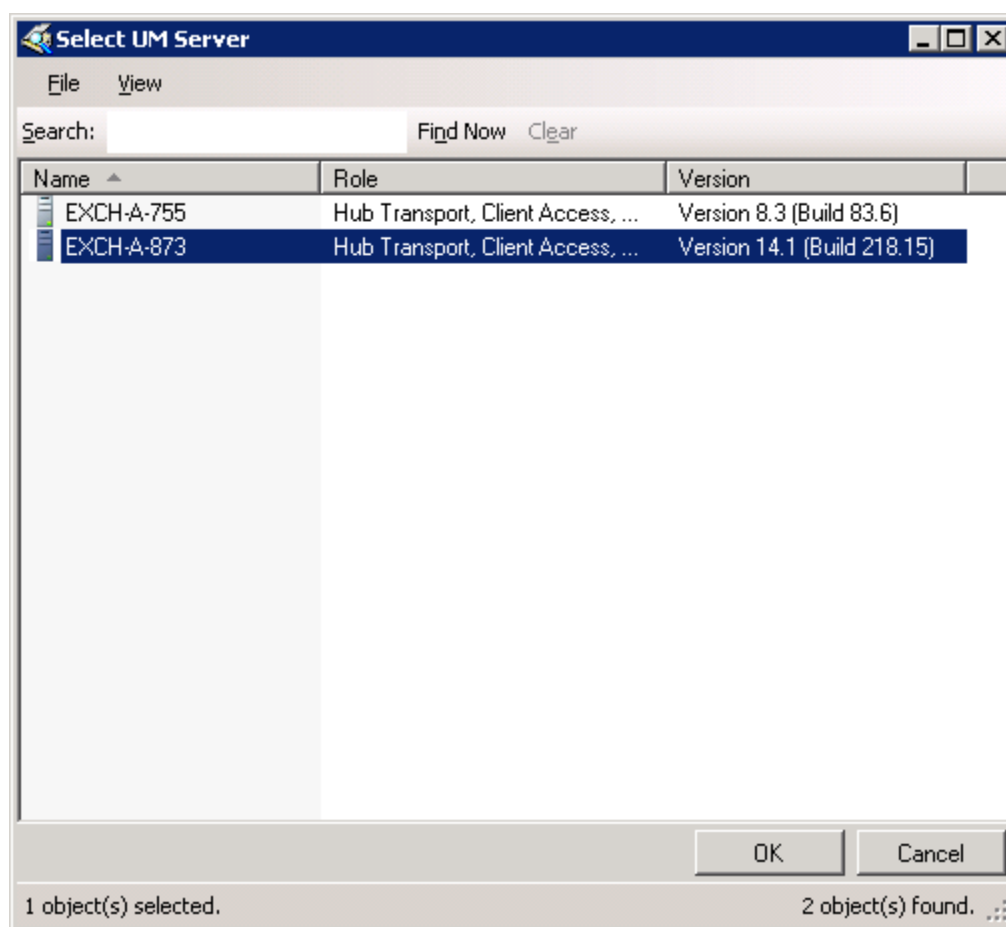


Figure 48: Select UM Server window

Return to the **Set UM Servers** section of **New UM Dial Plan** window with the Exchange UM server selected. Click on **Next** button to continue.

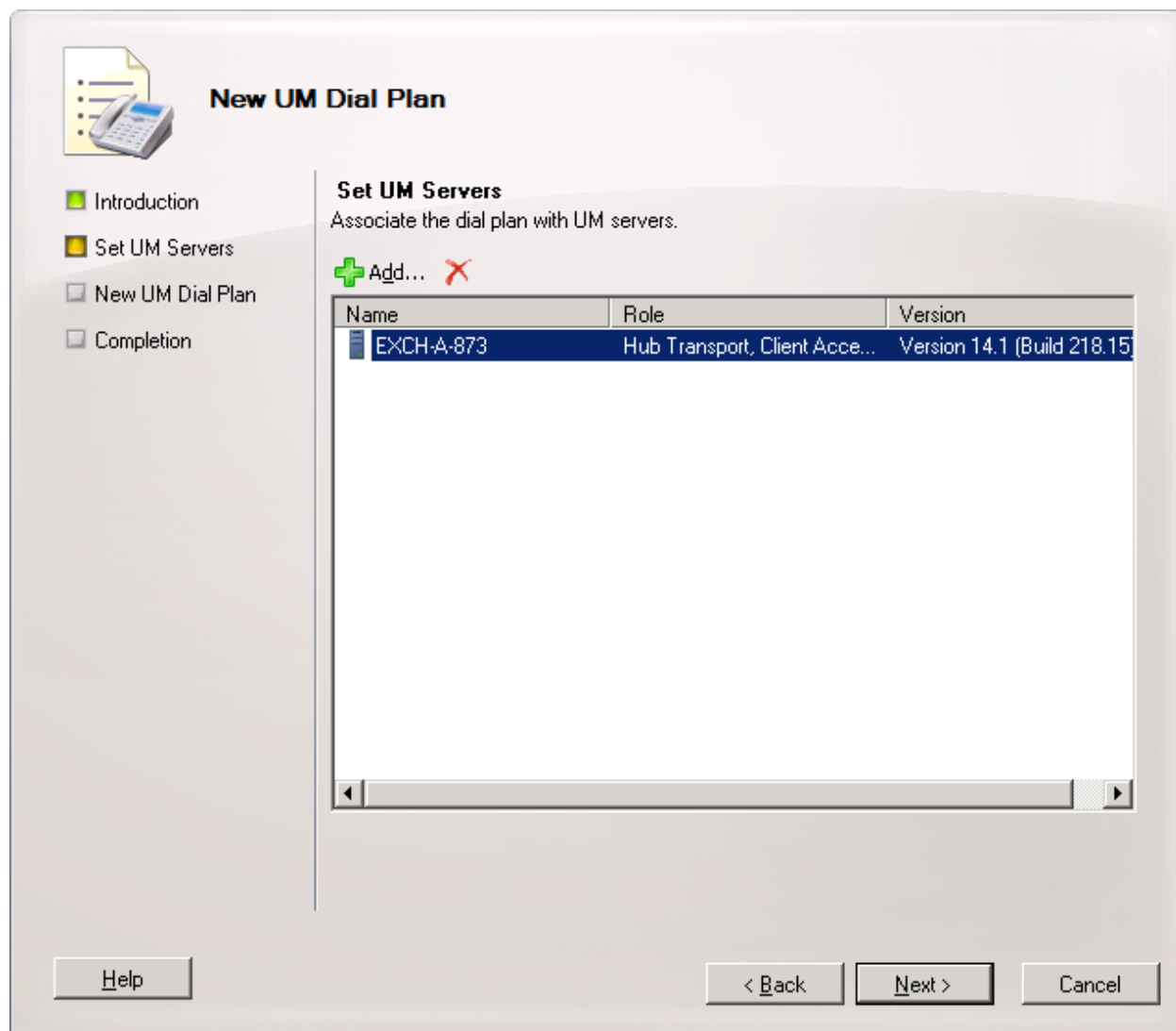


Figure 49: New UM Dial Plan Window (cont)

The **New UM Dial Plan** section of **New UM Dial Plan** window displays configuration summary of the new UM dial plan.

Click on **New** button to go to continue.

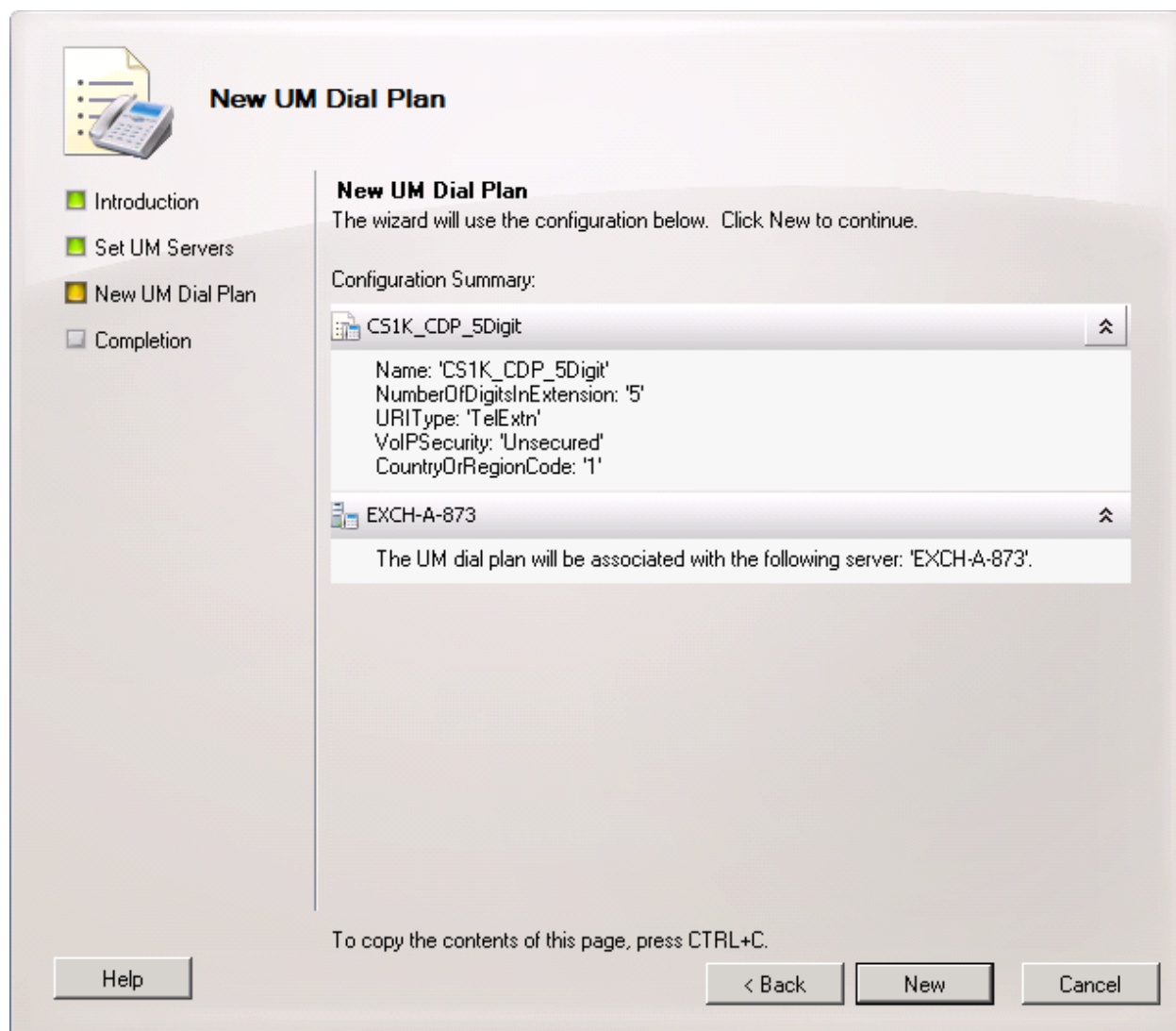


Figure 50: New UM Dial Plan Window (cont)

The **Completion** section displays the new UM dial plan is successfully created. Click on **Finish** button to complete and close the **New UM Dial Plan** window.

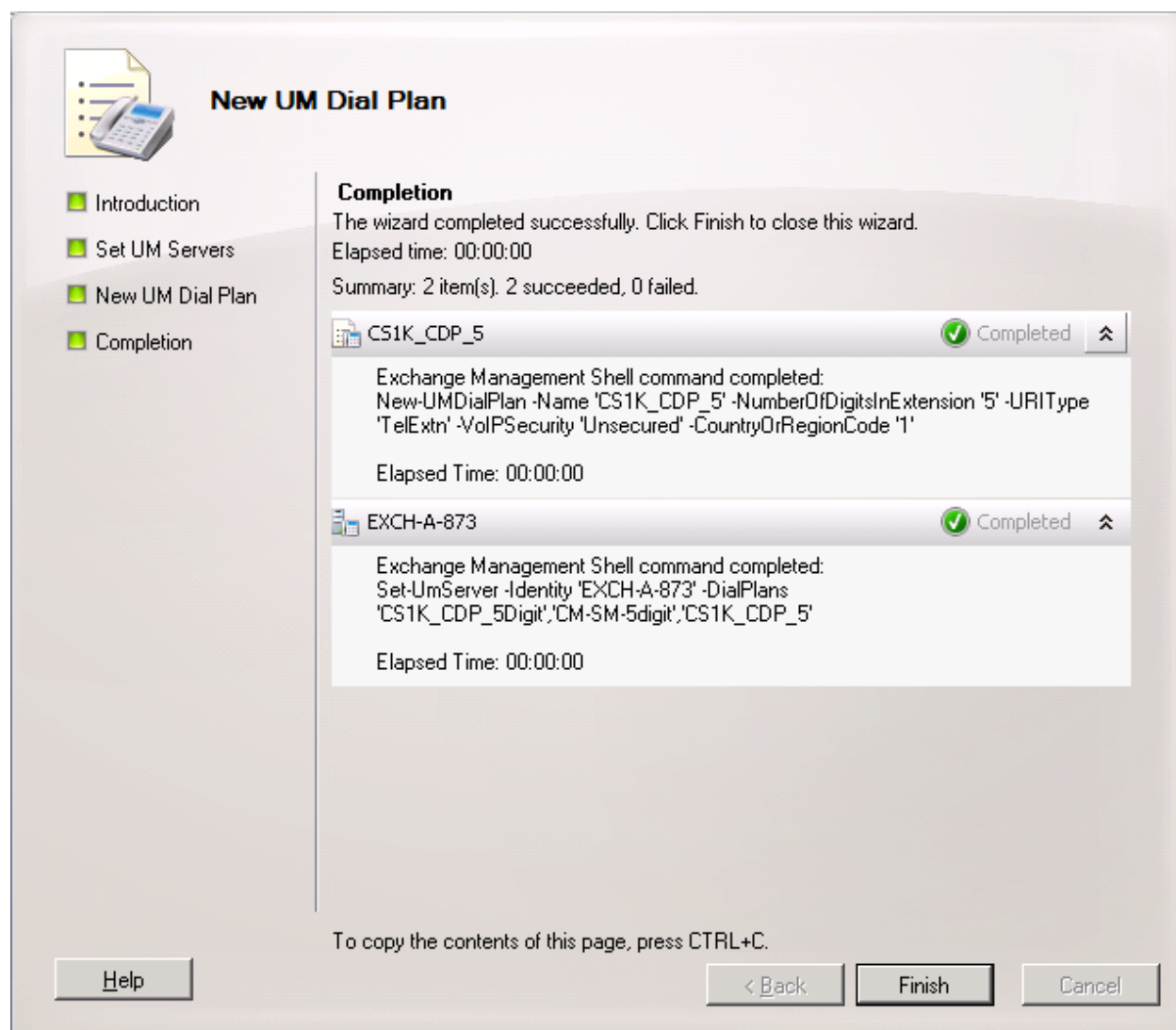


Figure 51: New UM Dial Plan Window (cont)

Figure 52 shows the new “CS1K_CDP_5Digit” UM dial plan is created.

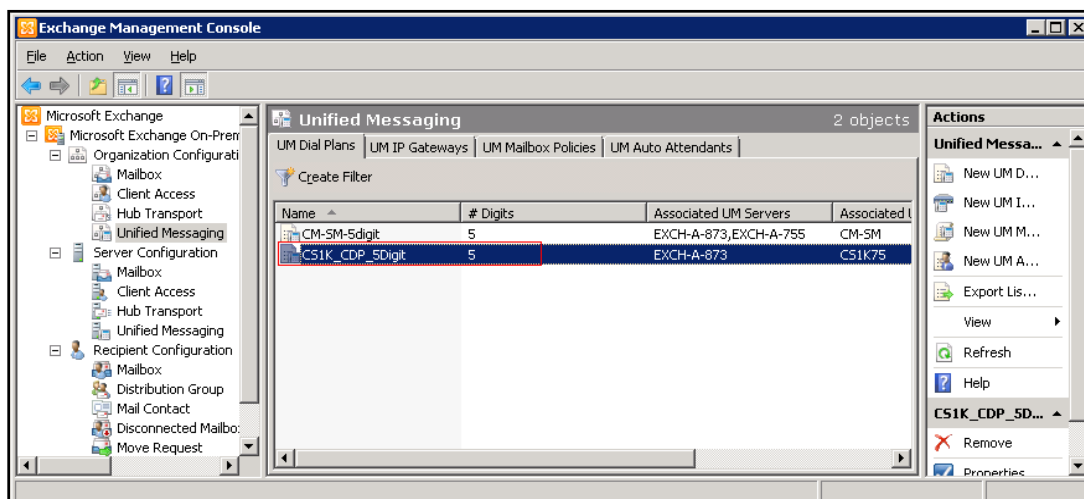


Figure 52: Exchange Management Console with the new UM Dial Plan created

Right-click on the “CS1K_CDP_5Digit” UM dial plan created above as shown in Figure 52, and then select **Properties** (not shown). The **CS1K_CDP_5Digit Properties** window displays.

Select **Subscriber Access** tab, enter number “73100” which is defined in Section 5.1 and 5.6.2 in **Telephone number to associate** box and then click on the **Add** button to add this number to list of telephone number associate.

Click **Apply** button to save the change and click OK to close the **CS1K_CDP_5Digit Properties** window.

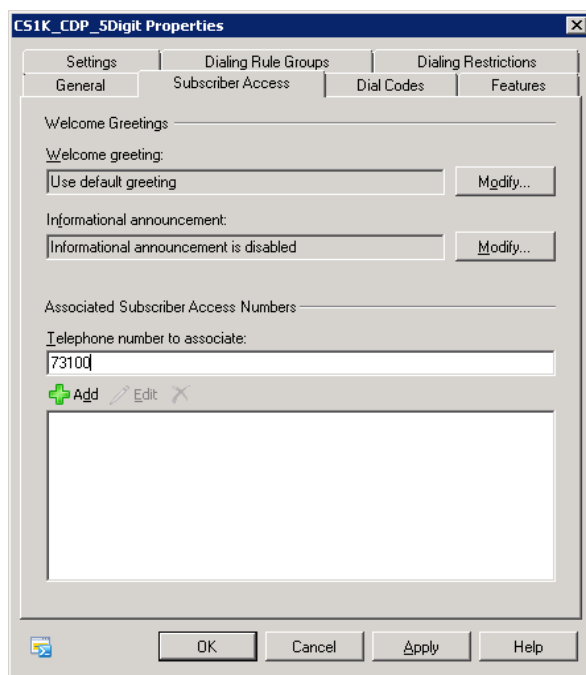


Figure 53: CS1K_CDP_5Digit UM Dial Plan Properties Window

6.2. Configure a New UM IP Gateway

Configure a new UM IP gateway on the Exchange UM, from the Exchange Management Console, navigate to **Microsoft Exchange > Microsoft Exchange On-Premise > Organization Configuration**, right-click on **Unified Messaging** item and select **New UM IP Gateway**.

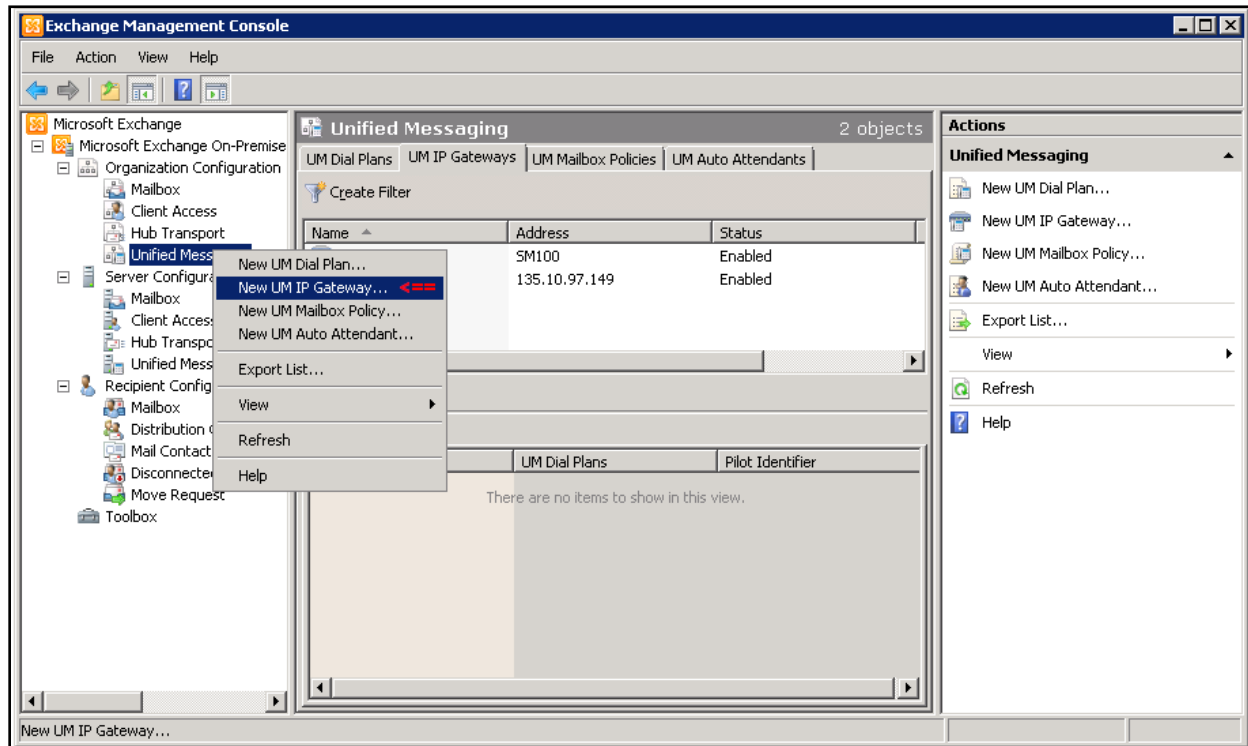


Figure 54: New UM IP Gateway Selected

The **New UM IP Gateway** window displays. Enter information for the new UM IP Gateway as below:

- **Name:** enter “*CS1K75*”
- **IP address:** enter “*135.10.97.149*”. This is Node IP of CS 1000 SIP gateway
- **Dial Plan:** click on **Browser** button and select the dial plan “*CS1K_CDP_5Digit*” created above.

Click on **New** button to continue.

New UM IP Gateway

☒ New UM IP Gateway
☐ Completion

New UM IP Gateway
This wizard helps you create a UM IP gateway for use by Microsoft Exchange Unified Messaging. UM IP gateways represent the connection between a physical gateway or IP PBX and Unified Messaging.

Name:
CS1K75

☒ IP address:
135.10.97.149
Example: 192.168.10.10

☐ Fully qualified domain name (FQDN):
Example: ipgateway1.contoso.com

Dial plan:
CS1K_CDP_5Digit Browse...

If a dial plan is selected, a default hunt group will be created to associate this new UM IP gateway to the specified dial plan. If no dial plan is selected, a hunt group must be created manually.

Help < Back New Cancel

Figure 55: New UM IP Gateway Window

The **Completion** section displays the new UM IP Gateway has been successfully created. Click on **Finish** button to complete and close the window.

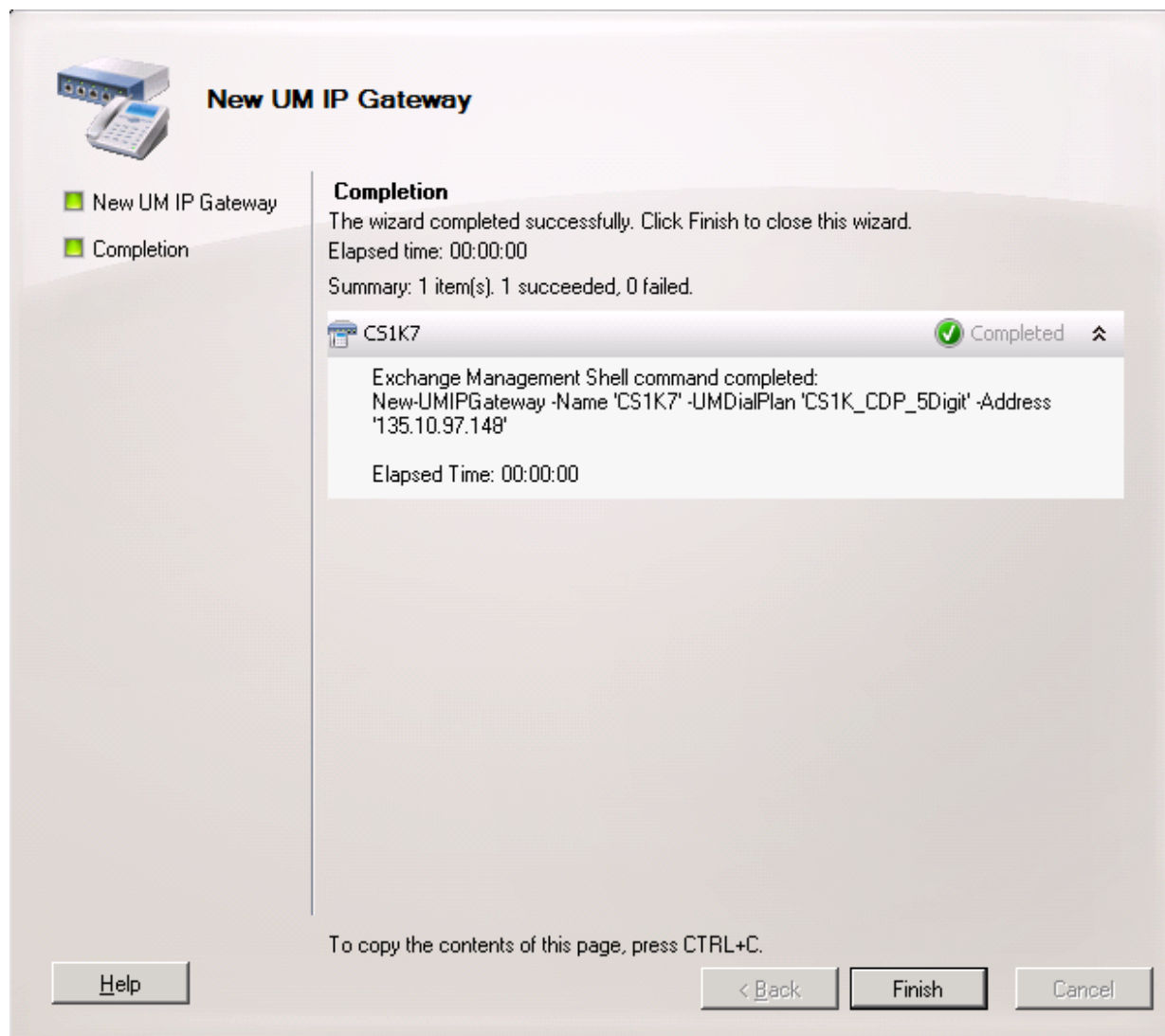


Figure 56: New UM IP Gateway Window (cont)

6.3. Configure a New UM Mailbox Policy

The new default UM Mailbox Policy “*CS1K_CDP_5Digit Default Policy*” is automatically created after the UM Dial Plan “*CS1K_CDP_5Digit*” created. **Figure 57** below displays the new default UM Mailbox Policy.

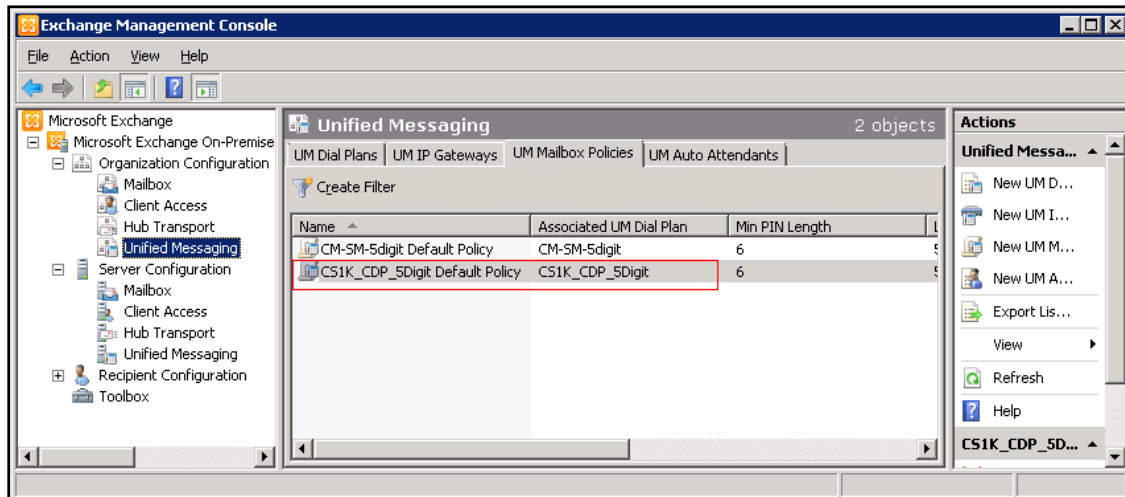


Figure 57: The Default UM Mailbox Policy

Right-click on the “*CS1K_CDP_5Digit Default Policy*” policy and select **Properties** (not shown), the **CS1K_CDP_5Digit Default Policy Properties** window displays. In the **General** tab, features of mailbox can be enabled by checking on individual checkbox.

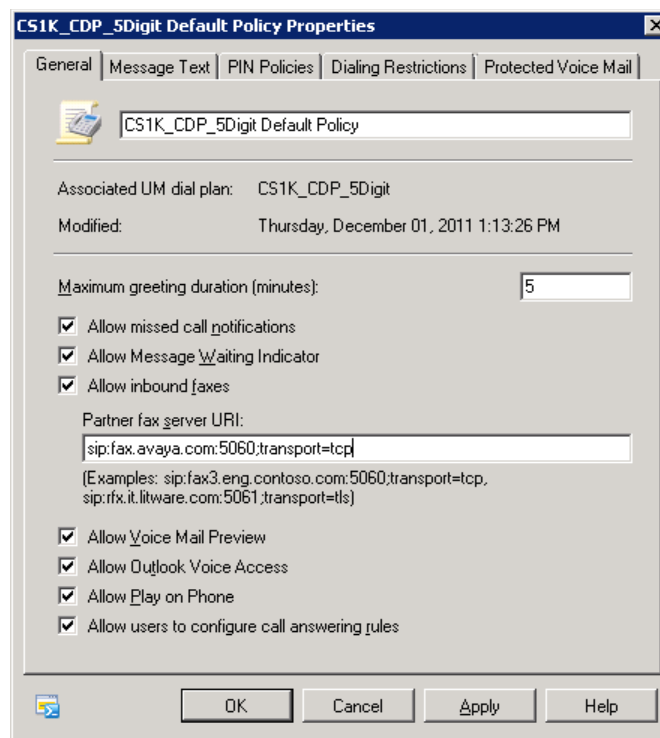


Figure 58: Mailbox Policy Properties Window

6.4. Configure a New Auto Attendant

Configure a new auto attendant on the Exchange UM, from Exchange Management Console window, navigate to **Microsoft Exchange > Microsoft Exchange On-Premise > Organization Configuration**, right-click on **Unified Messaging** item and select **New UM Auto Attendant**.

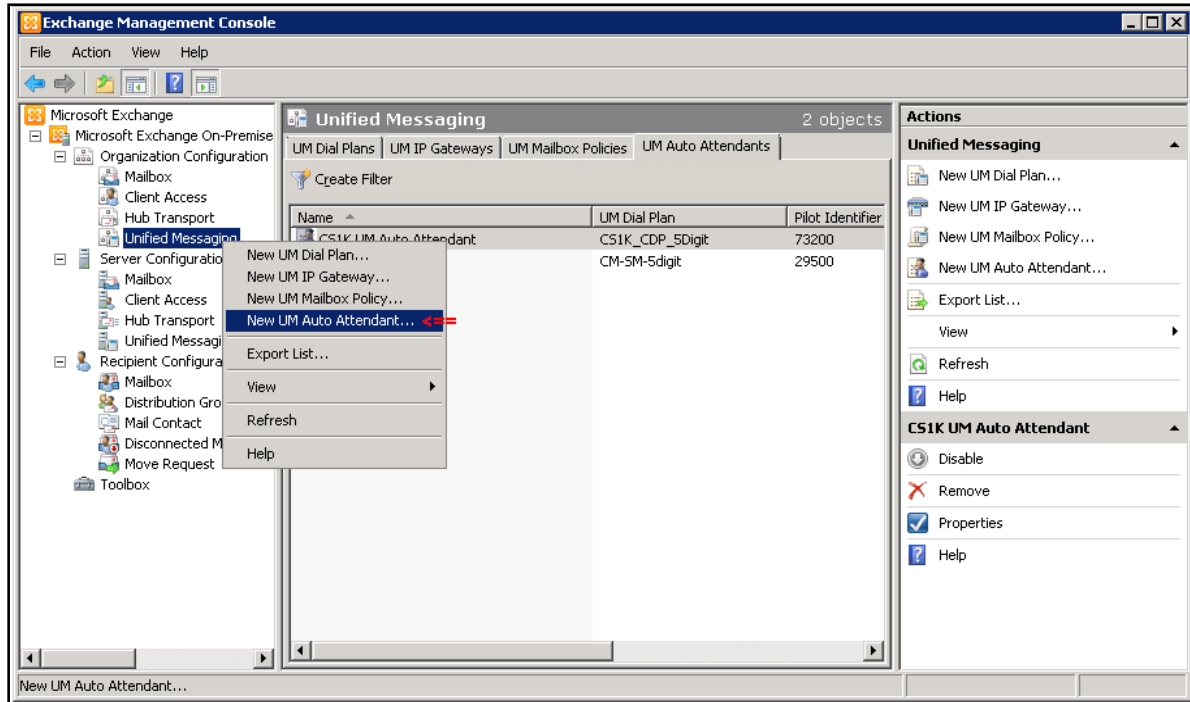


Figure 59: New UM Auto Attendant Option Selected

The **New UM Auto Attendant** window displays. Enter information for this new UM auto attendant as below:

- **Name:** enter “*CS1K Auto Attendant*”.
- **Select associated dial plan:** click on **Browser** button and select the “*CS1K_CDP_5Digit*” dial plan created in **Section 6.1**.
- **Pilot identifier list:** enter number “*73200*” as defined in **Section 5.6.2** and click on **Add** button to add this number to the list.
- **Create auto attendant as enabled:** Checked.
- **Create auto attendant as speech-enabled:** Checked.

Click on **New** button to continue.

New UM Auto Attendant

This wizard helps you create a new UM auto attendant for use by Microsoft Exchange Unified Messaging. You need to enter a name for this auto attendant and associate the auto attendant with a dial plan. You can also enter the extension number or numbers that callers will use to access this auto attendant.

Name:
CS1K Auto Attendant

Select associated dial plan.
CS1K_CDP_5Digit Browse...

Pilot identifier list:
73200

+ Add Edit X

☒ Create auto attendant as enabled
☒ Create auto attendant as speech-enabled

Help < Back New Cancel

Figure 60: New UM Auto Attendant Window

The **Completion** section displays the new UM auto attendant with name “*CS1K Auto Attendant*” has been successfully created.

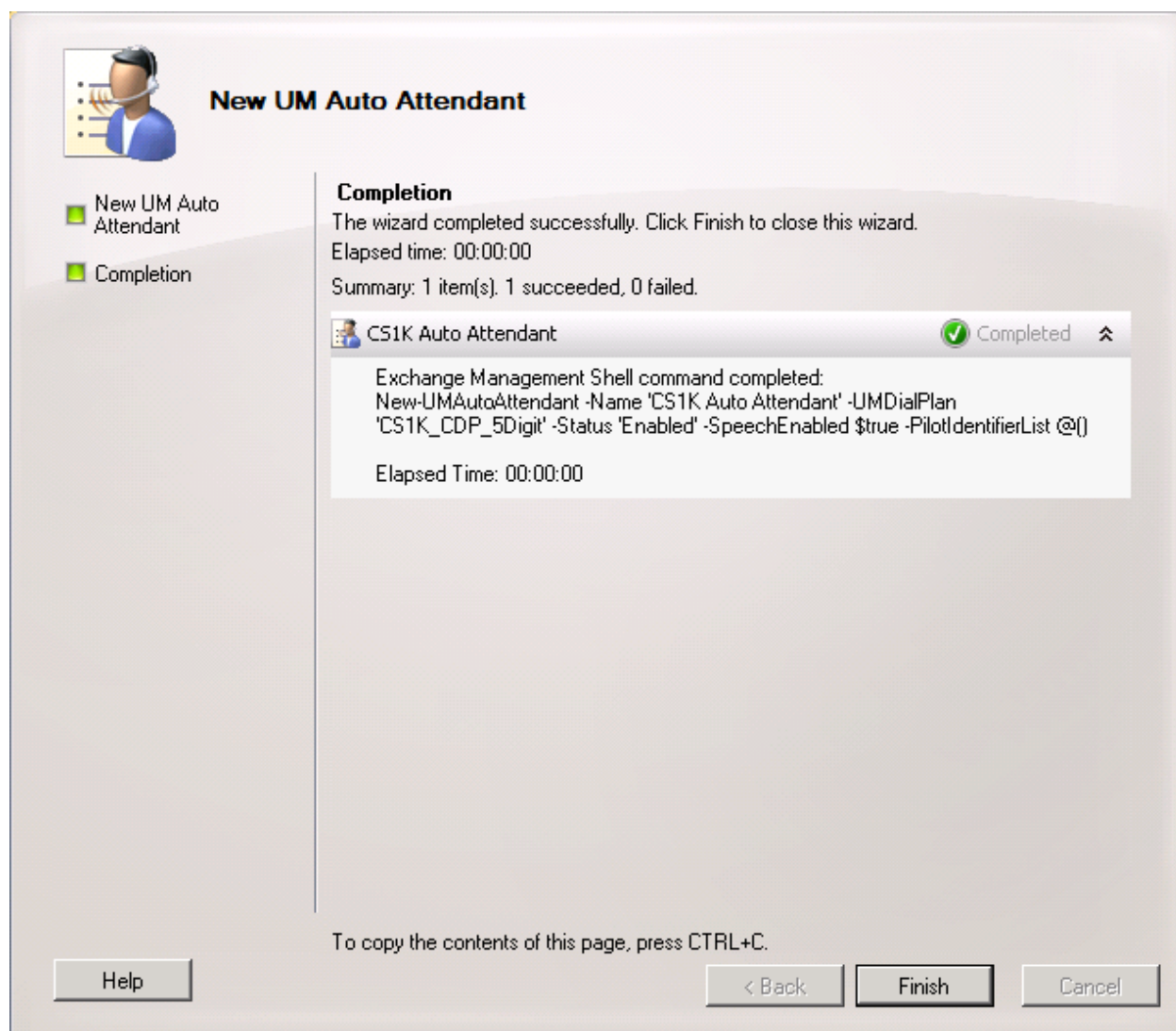


Figure 61: New UM Auto Attendant Window

7. Configure SIP TLS on CS 1000 SIP Gateway

The Communication Server 1000 system might have many SIP Signaling Gateways; these SIP Gateways are managed by a Unified Communication Management (UCM) application. This section provides the procedure for setting up SIP TLS on a specific SIP Gateway that was used to connect to Exchange UM 2010 server:

- Create a self certificate for SIP Gateway.
- Add Exchange UM 2010 Certificate to Certificate Authorities on the CS 1000 Unified Communication Management server.
- Download a certificate from Communication Server 1000 Unified Communication Management (UCM) Private Authority Certificate.
- Enable SIP TLS in SIP Gateway.
- Enable Secure Media in SIP Gateway.
- Add A Host Entry For Exchange UM in SIP Gateway.
- Configure Secure Media in System and Phone Station.

7.1. Create a Self Certificate for CS 1000 SIP Gateway

From the homepage of Communication Server 1000 UCM, navigate to **Security > Certificate**.

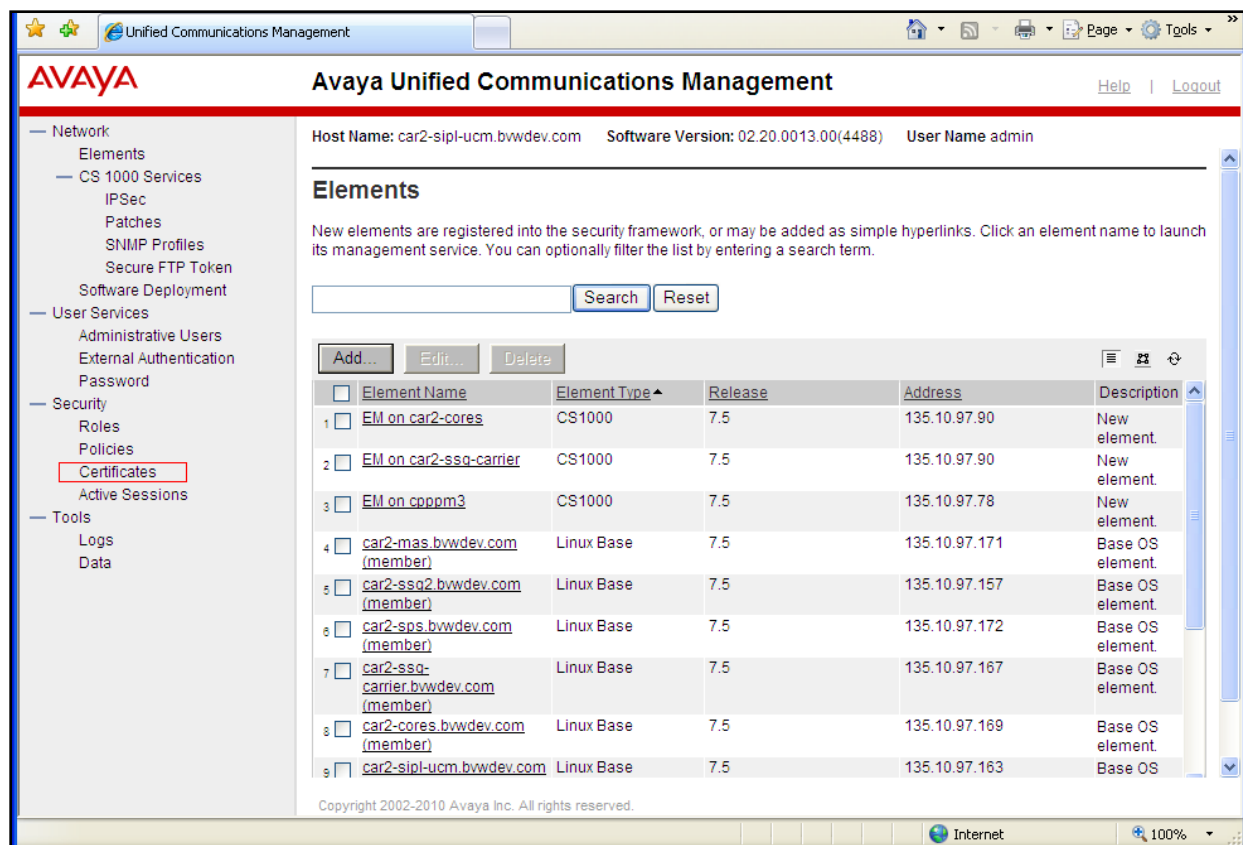


Figure 62: Certificate Section in UCM Home Page

The **Certificate Management** page displays on right-hand side of UCM window, navigate to **Certificate Endpoint** section and select SIP Gateway member that needs to create a self certificate, in this example that is “135.10.97.150” with Element Name “cpppm3.belleville.com”

Avaya Unified Communications Management

Host Name: car2-sipl-ucm.bvwdev.com Software Version: 02.20.0013.00(4488) User Name admin

Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Certificate Endpoints

Private Certificate Authority

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When multiple logical elements reside on a single base server, only the base endpoint is shown.

	Endpoint Address	Element Type	Element Name	Number of Service Profiles
5	135.10.97.169	Linux Base	car2-cores.bvwdev.com (member)	4
6	135.10.97.163	Linux Base	car2-sipl-ucm.bvwdev.com (primary)	4
7	135.10.97.150	Linux Base	cpppm3.bvwdev.com (member)	4
8	135.10.97.136	Linux Base	sipl75.bvwdev.com (member)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	cpppm3	Jan 17, 2021
2	DTLS	none		
3	Web SSL	none		
4	SIP TLS	none		

Copyright 2002-2010 Avaya Inc. All rights reserved.

Figure 63: Certificate Management Page

When the SIP Signaling Gateway “*cpppm3.belleville.com*” member is selected in the **Certificate Endpoints** section, their detailed certificates is displayed in **Endpoint Details** section and under **Certificates** subsection.

Click on **SIP TLS** in **Service Profile** column of the **Certificates** subsection to generate a self certificate for this SIP Gateway.

Avaya Unified Communications Management

Host Name: car2-sipl-ucm.bvwddev.com Software Version: 02.20.0013.00(4488) User Name admin

Endpoint ID	Endpoint Name	Endpoint Type	Endpoint Name	Number of Certificates
5	135.10.97.169	Linux Base	car2-cores.bvwddev.com (member)	4
6	135.10.97.163	Linux Base	car2-sipl-ucm.bvwddev.com (primary)	4
7	135.10.97.150	Linux Base	coppm3.bvwddev.com (member)	4
8	135.10.97.136	Linux Base	sipl75.bvwddev.com (member)	4

Endpoint Details
Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	coppm3	Jan 17, 2021
2	DTLS	none		
3	Web SSL	none		
4	SIP TLS	none		

Certificate Authorities

Add... Enable Trust Disable Trust Delete Update CRL

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1	car2-sipl-ucm.bvwd...	Feb 1, 2035	yes	/O=avaya/ST=ONL=Belleville/...	Nov 17, 2011
2	MSUM	Mar 22, 2016	yes	/DC=com/DC=microsoft/DC=n...	

Copyright 2002-2010 Avaya Inc. All rights reserved.

Figure 64: Certificate of SIP Gateway Member

Server Certificate page pops up, select option “*Create a new certificate, signed by local Certificate Authority*” and Click **Next** button to continue.

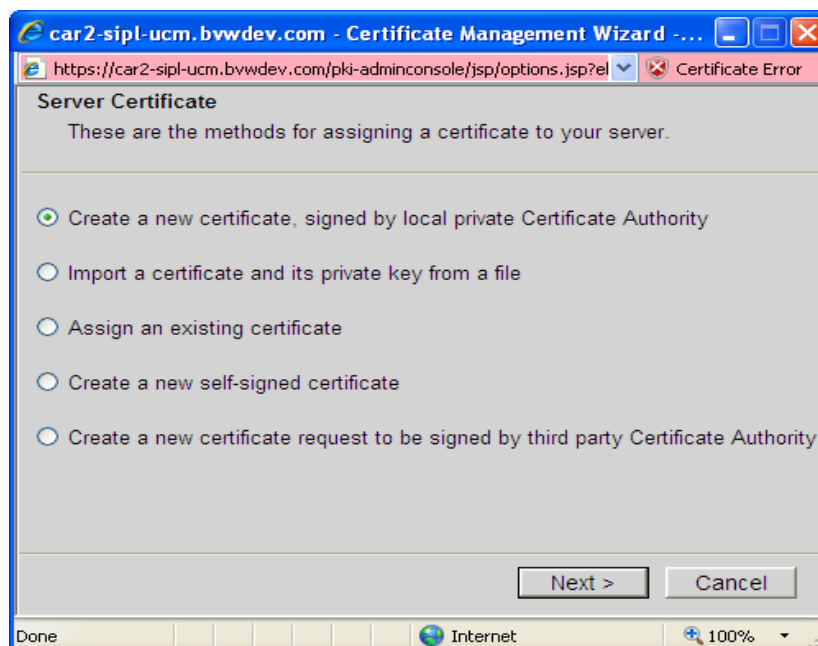


Figure 65: Server Certificate Window

Name and Security Settings section displays. Enter the name “*SIPGW-TLS*” in **Friendly Name** box and select **Bit Length** as “*1024*” (Default value). Click on **Next** button to continue.

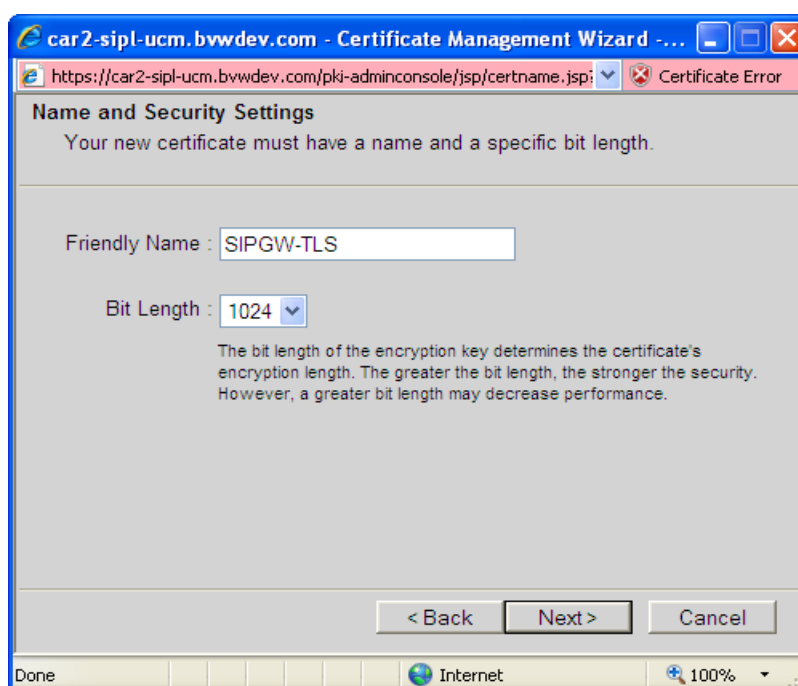


Figure 66: Server Certificate Window (cont)

The **Organization Information** section displays. Enter “*Solution and Interoperability*” in **Organization** box and “*BvwDevConnect*” in **Organization Unit**. Click on **Next** button to continue.

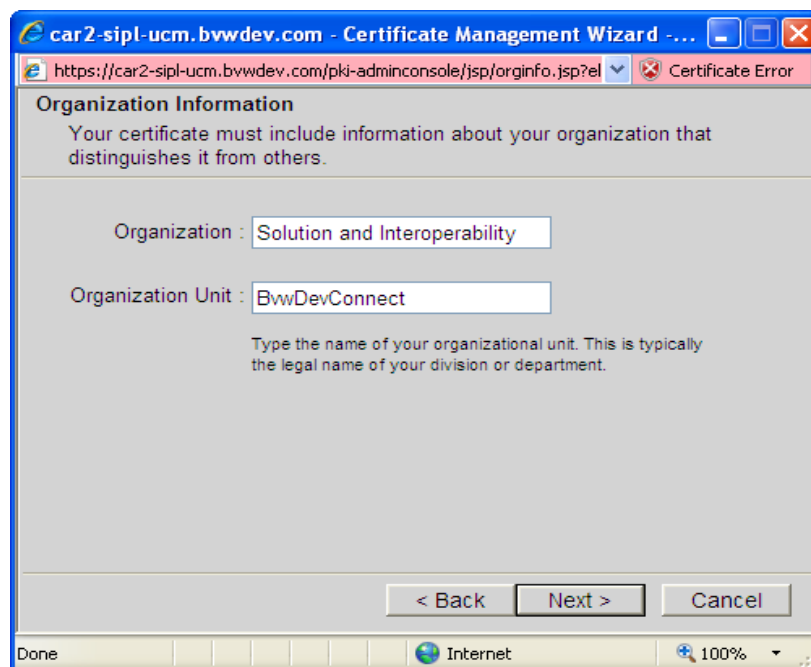
The screenshot shows a web browser window titled "car2-sipl-ucm.bvwdev.com - Certificate Management Wizard". The address bar shows "https://car2-sipl-ucm.bvwdev.com/pki-adminconsole/jsp/orginfo.jsp?el". The main content area is titled "Organization Information" and contains the text: "Your certificate must include information about your organization that distinguishes it from others." Below this, there are two input fields: "Organization" with the value "Solution and Interoperability" and "Organization Unit" with the value "BvwDevConnect". A note below the fields says: "Type the name of your organizational unit. This is typically the legal name of your division or department." At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The status bar at the bottom shows "Done", "Internet", and "100%".

Figure 67: Server Certificate Window (cont)

Your Server's Common Name section displays. Enter “*cpppm3.bvwdev.com*” in **Common Name** box and select “*None*” in **Subject At Name** dropdown menu. Click on **Next** button to continue.

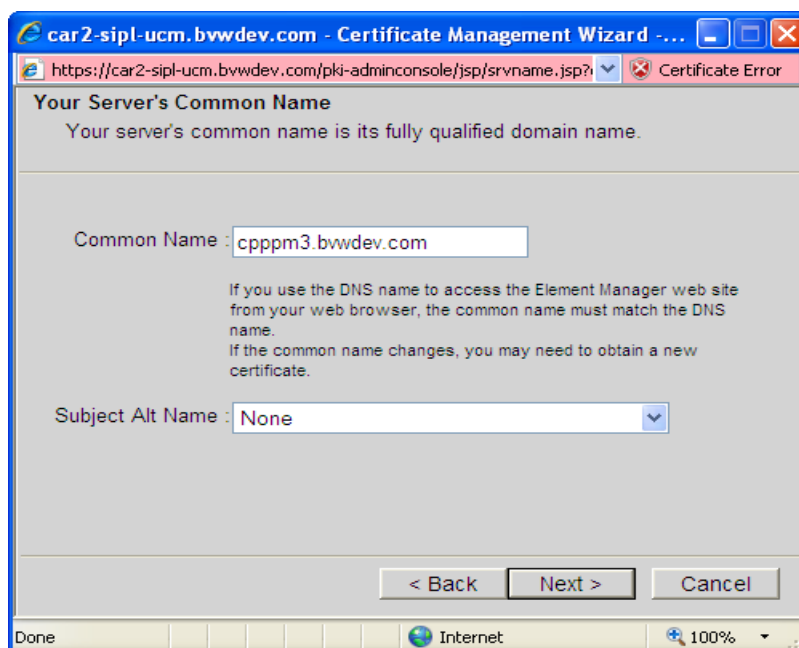
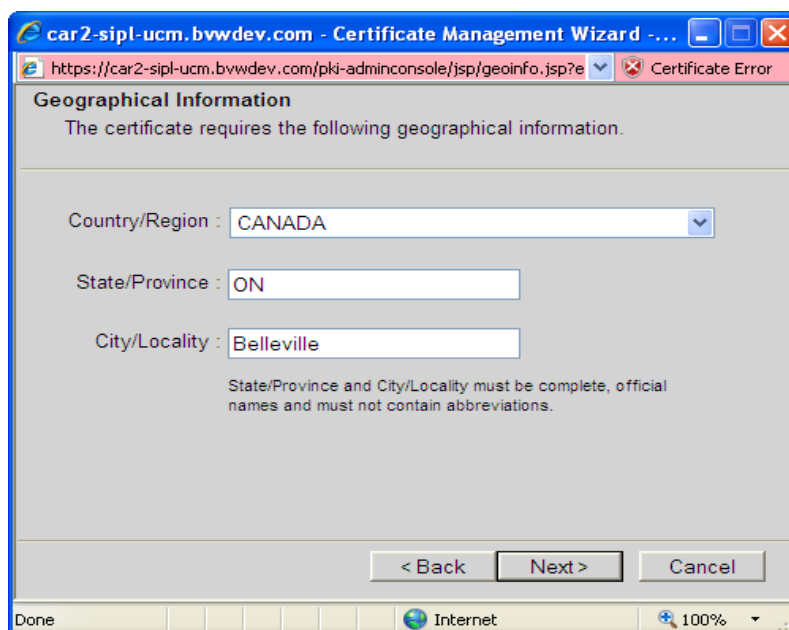
The screenshot shows a web browser window titled "car2-sipl-ucm.bvwdev.com - Certificate Management Wizard". The address bar shows "https://car2-sipl-ucm.bvwdev.com/pki-adminconsole/jsp/srvname.jsp?". The main content area is titled "Your Server's Common Name" and contains the text: "Your server's common name is its fully qualified domain name." Below this, there are two input fields: "Common Name" with the value "cpppm3.bvwdev.com" and "Subject Alt Name" with a dropdown menu set to "None". A note below the fields says: "If you use the DNS name to access the Element Manager web site from your web browser, the common name must match the DNS name. If the common name changes, you may need to obtain a new certificate." At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The status bar at the bottom shows "Done", "Internet", and "100%".

Figure 67: Server Certificate Window (cont)

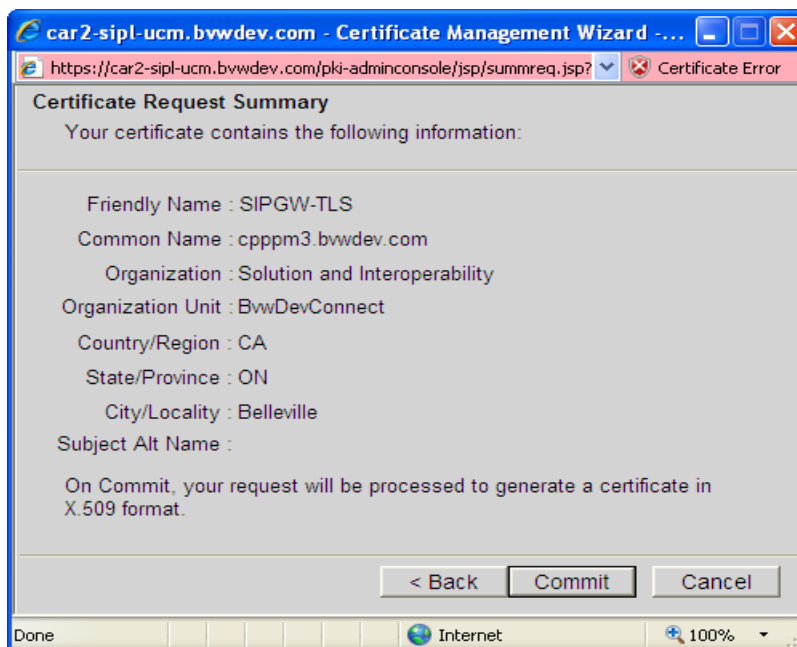
The **Geographic Organization** section displays. Select “*CANADA*” in **Country/Region** dropdown menu, “*ON*” in **State/Province** box, and “*Belleville*” in **City/Locality**. Click on **Next** button to continue.



The screenshot shows a web browser window titled "car2-sipl-ucm.bvwdev.com - Certificate Management Wizard - ...". The address bar shows "https://car2-sipl-ucm.bvwdev.com/pki-adminconsole/jsp/geoinfo.jsp?e". The page has a "Certificate Error" icon in the top right. The main heading is "Geographical Information" with the subtext "The certificate requires the following geographical information." Below this, there are three input fields: "Country/Region" with a dropdown menu showing "CANADA", "State/Province" with a text box containing "ON", and "City/Locality" with a text box containing "Belleville". A note below the fields states: "State/Province and City/Locality must be complete, official names and must not contain abbreviations." At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The browser's status bar at the bottom shows "Done", "Internet", and "100%".

Figure 68: Server Certificate Window (cont)

Certificate Request Summary section displays summary information of the self certificate. Click on **Commit** button to start generating the certificate.



The screenshot shows a web browser window titled "car2-sipl-ucm.bvwdev.com - Certificate Management Wizard - ...". The address bar shows "https://car2-sipl-ucm.bvwdev.com/pki-adminconsole/jsp/summreq.jsp?". The page has a "Certificate Error" icon in the top right. The main heading is "Certificate Request Summary" with the subtext "Your certificate contains the following information:". Below this, the following information is displayed: "Friendly Name : SIPGW-TLS", "Common Name : cpppm3.bvwdev.com", "Organization : Solution and Interoperability", "Organization Unit : BwvDevConnect", "Country/Region : CA", "State/Province : ON", "City/Locality : Belleville", and "Subject Alt Name :". A note at the bottom states: "On Commit, your request will be processed to generate a certificate in X.509 format." At the bottom, there are three buttons: "< Back", "Commit", and "Cancel". The browser's status bar at the bottom shows "Done", "Internet", and "100%".

Figure 69: Server Certificate Window (cont)

Click on **Finish** button to complete and close the page.

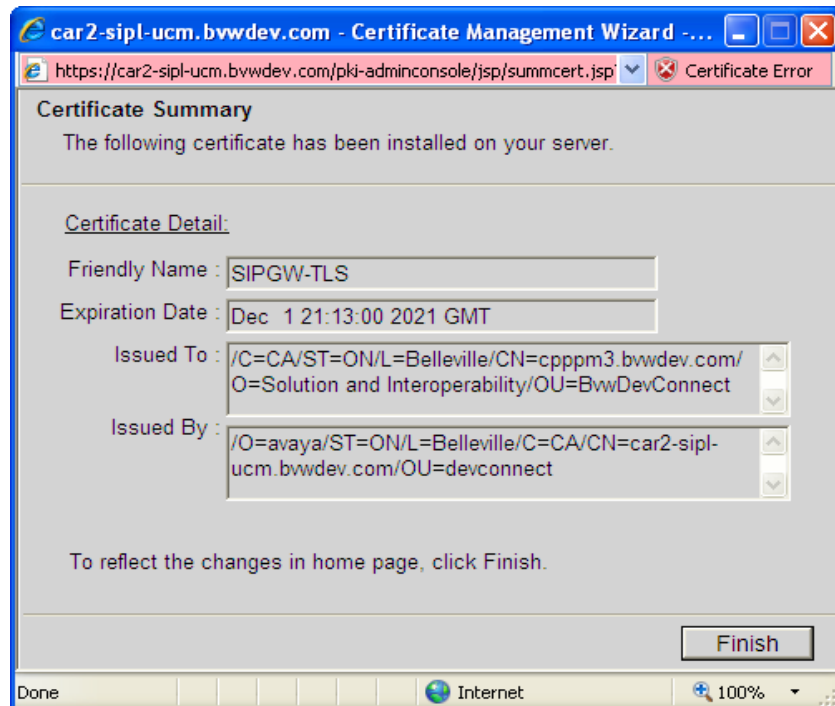


Figure 70: Server Certificate Window (cont)

Figure 71 shows the new certificate for SIP TLS has been created with status as “signed”.

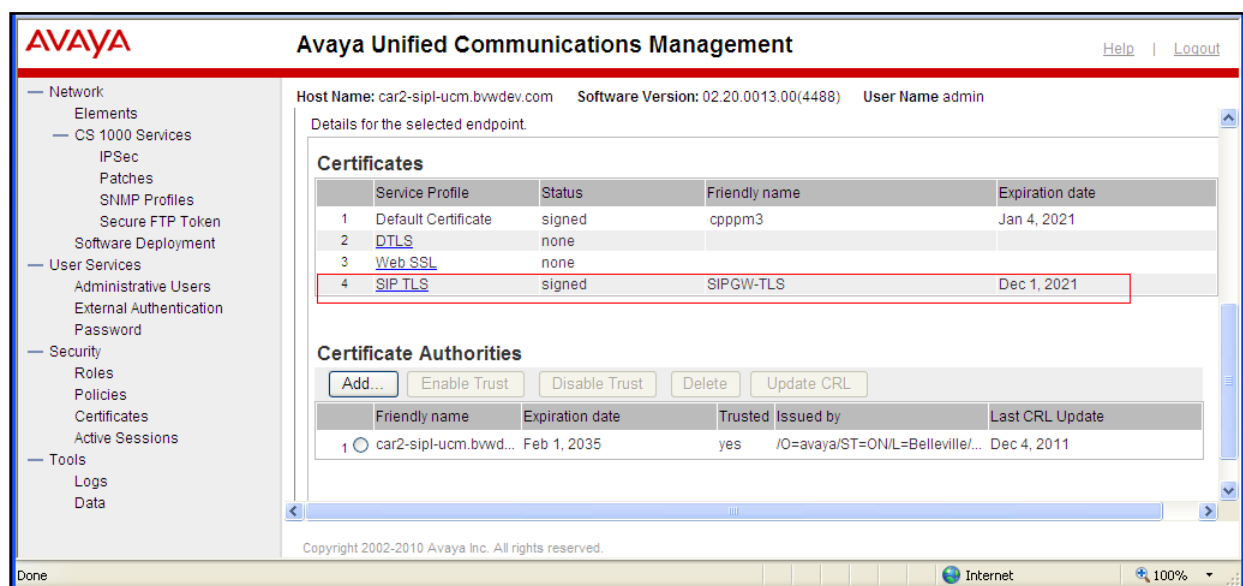


Figure 71: The New Certificate Generated for SIP TLS

7.2. Add Exchange UM Certificate to SIP Gateway Certificate Authorities

From **Certificate Authorities** section of certificate endpoints “135.10.97.150”, click on **Add** button to import Exchange UM certificate.

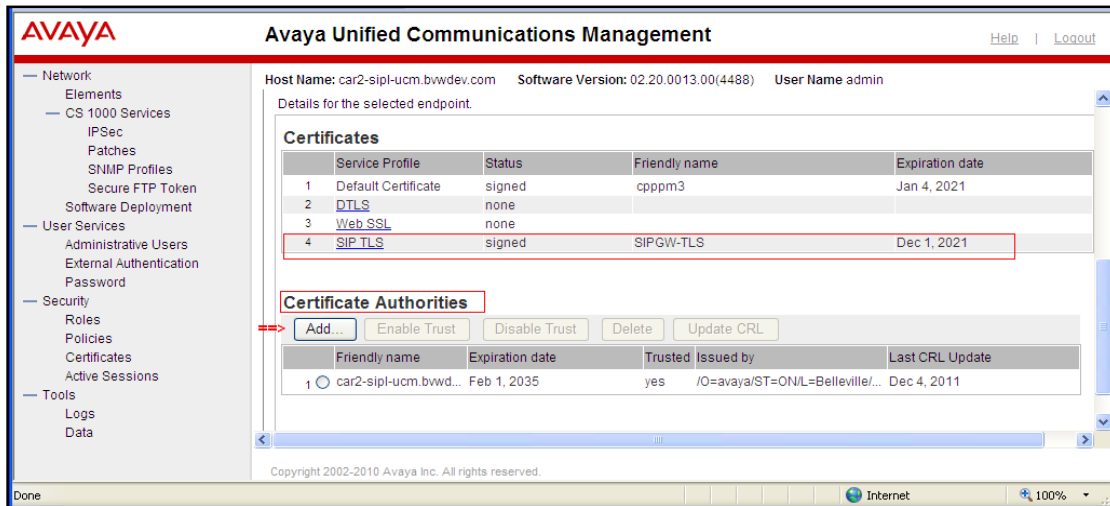


Figure 72: Certificate Authorities of SIP Gateway member

A new page pops up. In “Add a CA to the Service” section, enter “MSUM” in **Friendly Name** box, paste Exchange UM certificate into the blank box and then click on **Submit** button to install this certificate. Note: The Exchange UM certificate is provided by Microsoft UM Team and it can be opened by Microsoft Notepad application and use “copy” and “paste” command to copy and paste the certificate.

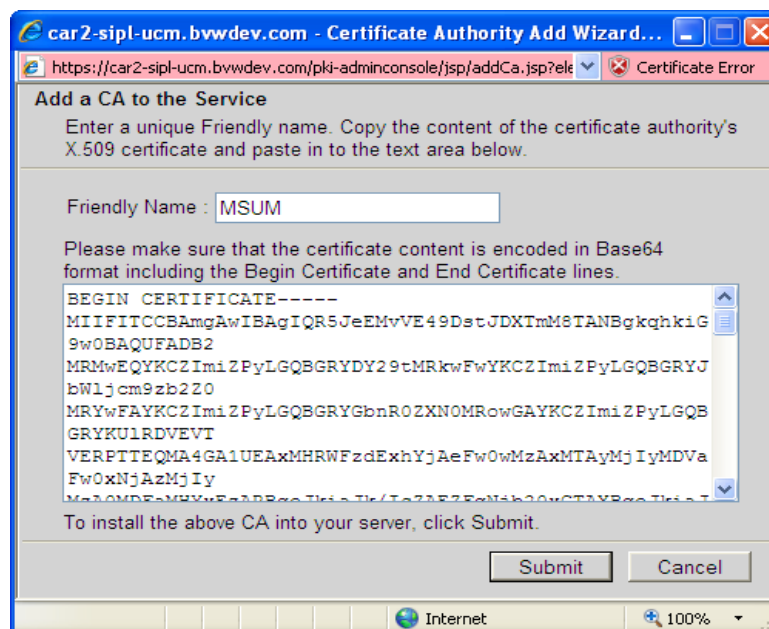


Figure 73: Add a CA to the Service Page

Figure 74 shows the Exchange UM certificate is successfully imported to the **Certificate Authorities**.

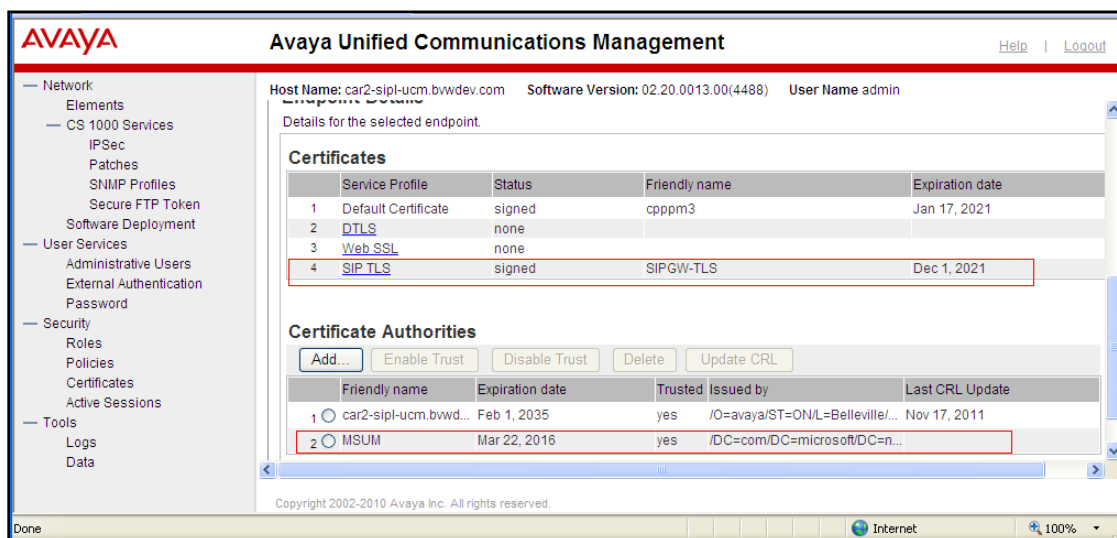


Figure 74: The Exchange UM Certificate Imported

7.3. Download a Private Authority Certificate

From the **Certification Management** page, click on **Private Certificate Authority** tab and detail of the certificate is displayed in **Private Certificate Authority Details** section.

Click on **Download** button to save the certificate.

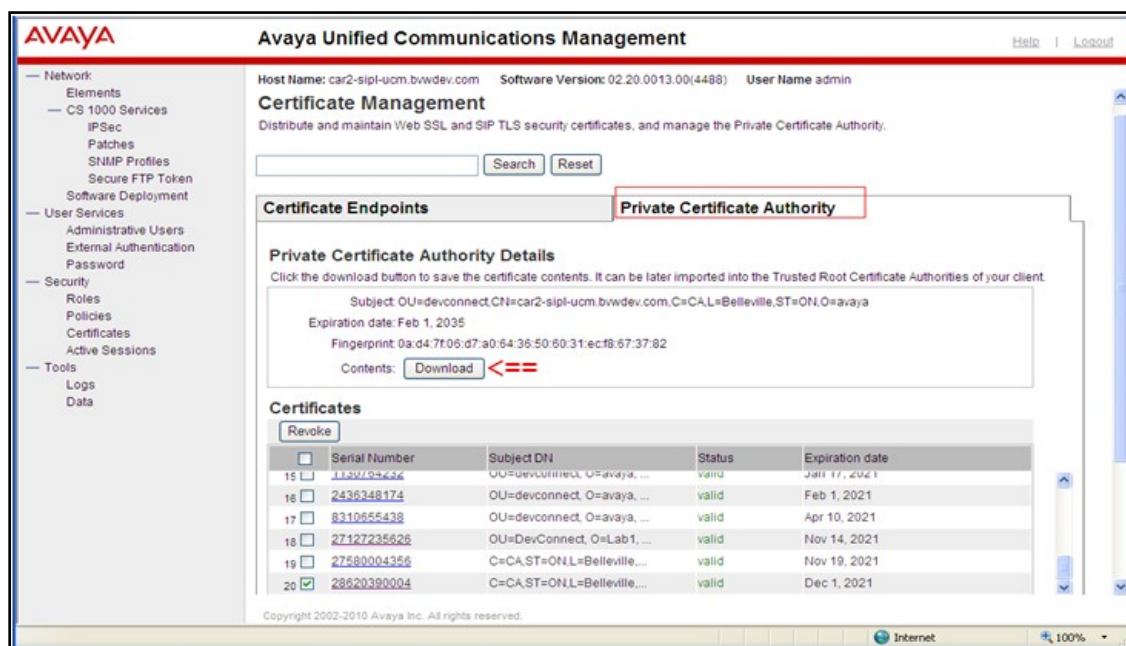


Figure 75: Private Certificate Authority Page

The **File Download** window pops up, click on **Save** button to save the certificate. This certificate will be imported to Exchange UM server.

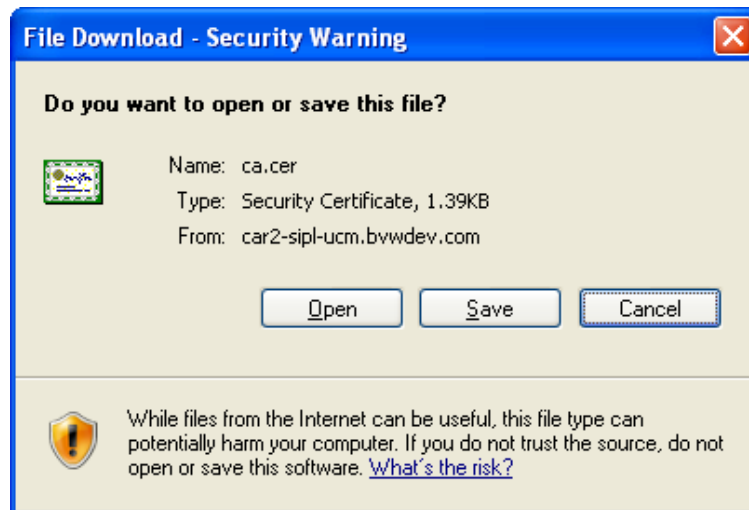


Figure 76: File Download Window of Private Certificate

7.4. Enable SIP TLS on SIP Gateway

From the UCM home page, navigate to **Network > Element > Element Name** (in this example, “CPPPM3_ON_EM”) > **System > IP Network > Nodes: Servers and Media Cards > Node ID** (in this example, 511) > **Node Details (ID: 511 - LTPS, Gateway (SIPGw)) > Gateway (SIPGw) > Node ID: 511 - Virtual Trunk Gateway Configuration Details**.

Scroll down to **SIP Gateway Settings** section, select “*Secure End to End*” in **TLS Security** dropdown menu, enter “5061” in **Port** box, and check on “*Client authentication*” and “*X509 certificate authority*” checkboxes.

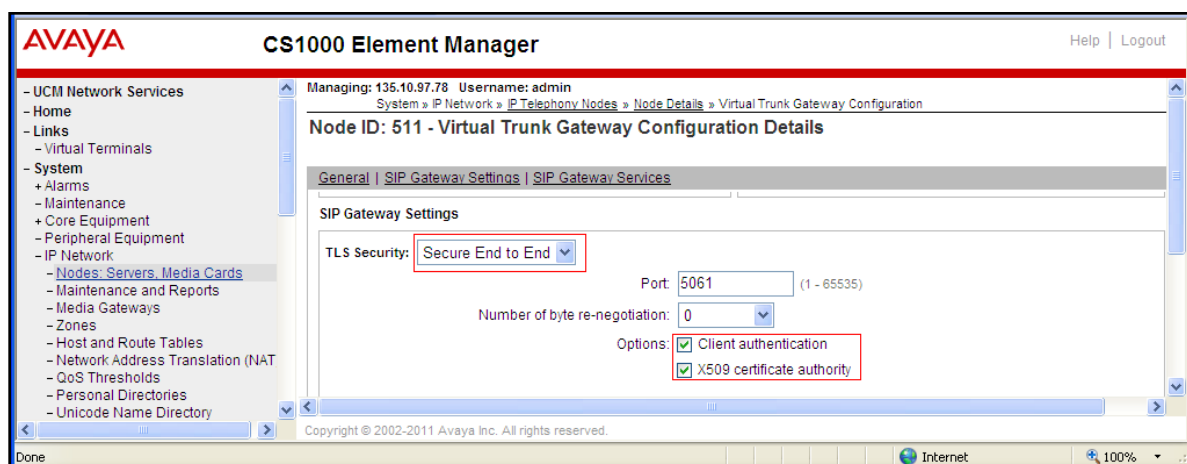


Figure 77: SIP Gateway Settings With TLS

Scroll down to **Proxy and Redirect Server** of **SIP Gateway Settings** section, enter IP address of Exchange UM server “131.107.5.62” in **Primary TLAN IP address** box, “5061” in **Port** box and select “**TLS**” in **Transport protocol**.

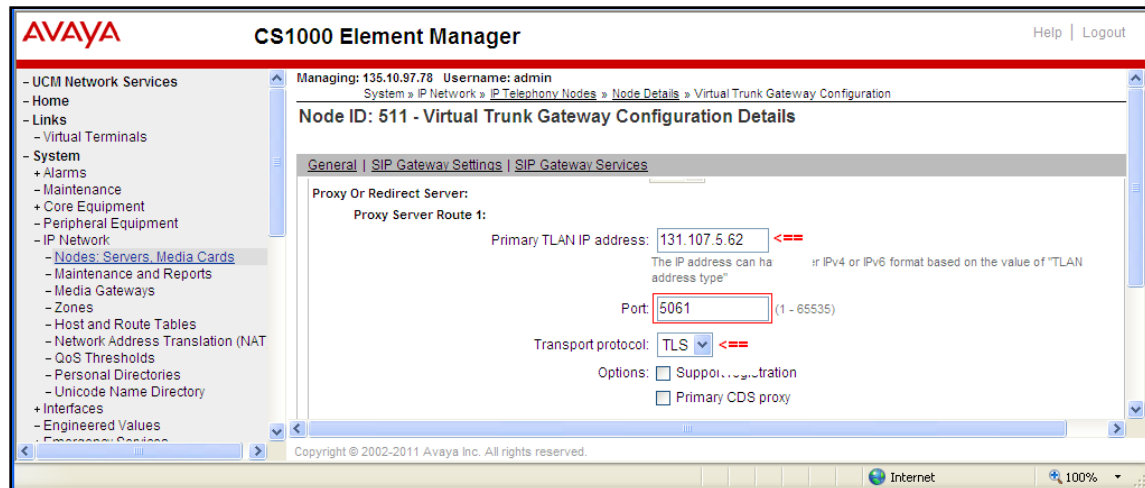


Figure 78: Proxy Or Redirect Server Settings

7.5. Enable Secure Media on SIP Gateway

The secure media can be only applied when SIP TLS is established. To enable secure media , on the **Node ID: 511 - Virtual Trunk Gateway Configuration Details** page scroll down to **SIP Gateway services** (not shown) section and under **Microsoft Unified Messaging** subsection check on “*Enable Secure Media*” check box.

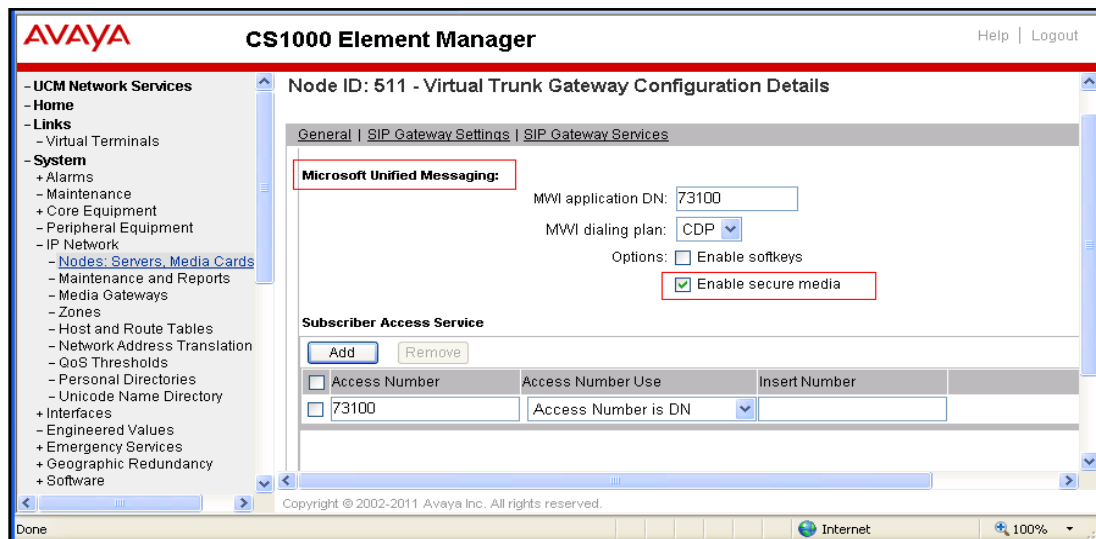


Figure 79: Enable Secure Media on SIP Gateway

The process of save, transfer and synchronization need to be applied as described in **Section 5.1** for the changes take effect.

7.6. Add a Host Entry For Exchange UM In SIP Gateway

This is important step of setting up SIP TLS, due to SIP TLS uses Full qualified domain name (FQDN) to negotiate and handshake, make sure CS 1000 SIP Gateway is able to resolve the IP address of Exchange UM to its FQDN and vice versa. This can be approached by adding a host entry in the SIP Gateway, from homepage of UCM, click on member “*cpppm3.bvwdev.com (member)*” of SIP Gateway.

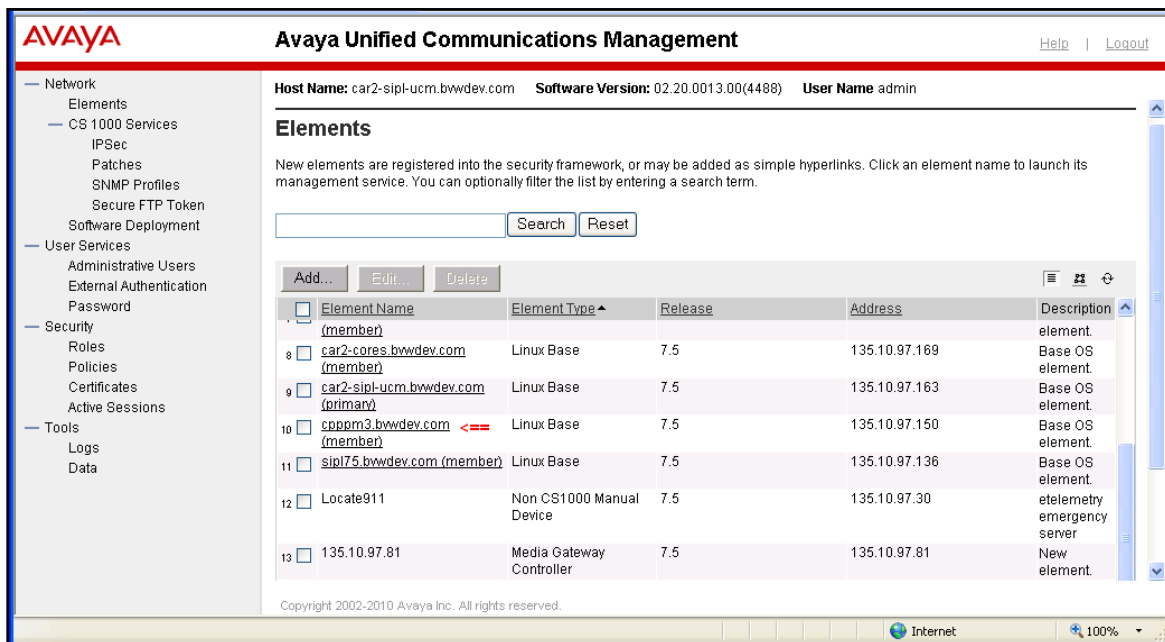


Figure 80: UCM Homepage with Linux Member

The **Base Manager** page displays. On the left-hand tree menu, click on **DNS and Hosts**. The **Domain Name Server (DNS)** displays on right-hand side of **Base Manager** page, in the **Hosts** section, click on **Add** button to add a new host.

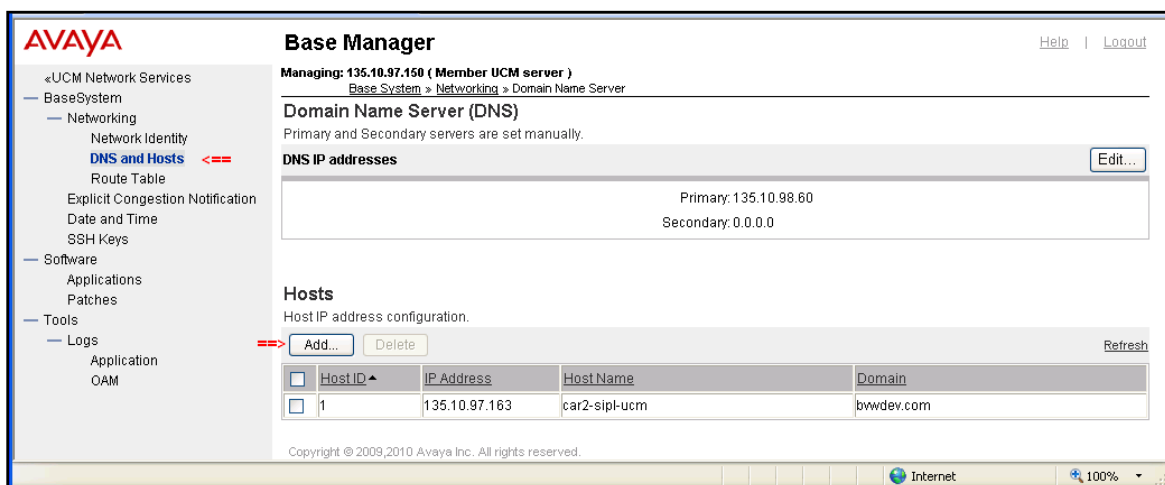


Figure 81: Base Manager of SIP Gateway

The **New Host** page displays. Enter IP “131.107.5.62” in **IP address** box, “EXCH-A-873” in **Host name** box and domain name “DFPYXV-dom.extest.microsoft.com” in **Domain** box. Click on **Save** button to complete adding new host for Exchange UM.

AVAYA Base Manager Help | Logout

Managing: 135.10.97.150 (Member UCM server)

Base System > Networking > DNS and Hosts > New Host

New Host

IP address: 131.107.5.62 * <==

Host name: EXCH-A-873 * <==

Domain: extest.microsoft.com * <==

*Required value. ==> **Save** **Cancel**

Copyright © 2009,2010 Avaya Inc. All rights reserved.

Figure 82: New Host Page

Figure 83 below shows the new host of Exchange UM server is successfully added to the SIP Gateway.

AVAYA Base Manager Help | Logout

Managing: 135.10.97.150 (Member UCM server)

Base System > Networking > Domain Name Server

Domain Name Server (DNS)

Primary and Secondary servers are set manually.

DNS IP addresses **Edit...**

Primary: 135.10.98.60

Secondary: 0.0.0.0

Hosts

Host IP address configuration.

Add... **Delete** **Refresh**

<input type="checkbox"/>	Host ID ▲	IP Address	Host Name	Domain
<input type="checkbox"/>	1	135.10.97.163	car2-sipl-ucm	bwwdev.com
<input type="checkbox"/>	2	131.107.5.62	EXCH-A-873	DFPYXV-dom.extest.microsoft.com

Copyright © 2009,2010 Avaya Inc. All rights reserved.

Figure 83: New Host of Exchange UM Added

7.7. Configure Secure Media in System and Phone Station

Enable secure media in **Section 7.5** above is just first step for enabling secure media on CS 1000 to Exchange UM server. This section provides the configuration on Call Server for enabling secure media in the system and Phone station. Log in to the Call Server as administrator and issue following overlay commands.

Overlay LD 17 to enable media security for system. The media security of system can be Media Security Always (MSAW), Media Security Best Try (MSBT) or Media Security Never (MSNV). When media security in system is enabled, all IP phone station has media security class of service matched with media security in the system will be effective.

```
LD 17
REQ CHG
Type PARM
MSEC ON
  MSSD MSBT
  NKEY 31
  TKEY 24
```

Figure 84: Enable Media Security In The System

Overlay LD 20 to enable media security class of service for IP phone station. The media security class of server in the phone station should be matched with media security set in the system, in this testing that is MSBT (Media Security Best Try).

In the configuration below, the IP Phone 1140E is set to Media Security System Default (MSSD), whatever type of media security is set in the system; the media security of IP Phone 1140E is going to be matched.

```
LD 20
REQ: CHG
TYPE: 1140
TN 96 0 4 1
ECHG yes
ITEM cls MSSD
```

Figure 85: Enable Media Security Class of Service on IP Phone

Overlay LD 14 to enable media security class of service for IP Trunks, these are SIP IP Trunks defined in the CS 1000 system used for carrying SIP to Exchange UM. It's different than phone station; IP Trunks only accept Media Security Best Try (MSBT) and Media Security Never (MSNV) and it does not accept MSSD or MSAW.

```
LD 14
REQ chg
TYPE IPTI
TN 100 0 0 0
CLS MSBT
```

Figure 86: Enable Media Security Class of Service on IP Trunks

8. Configure SIP TLS on Exchange UM 2010

This section provides the procedure for setting up:

- Export a trusted authority certificate on Exchange UM 2010 server.
- Import the CS1000 UCM private authority certificate that was downloaded and saved as mentioned in Section 7.3 to Exchange UM 2010 server.
- Check TLS on Exchange UM 2010 Server.
- Configure SIP Secured on UM Dial Plan.
- Configure VoIP Secured on UM Dial Plan.

8.1. Export a trusted authority certificate

Open **Certificates Management Console** on the Exchange UM 2010 server, by navigating to menu **Start > Run (mmc) > menu File > Add/Remove Snap-in > Add Certificates (local computer)**.

Select **Certificates** folder under **Trusted Root Certification Authorities** folder, list of certificates displays on right-hand side of **Certificate Console**.

Name of certificate needs to be imported in this list is “*EastLab*”, this certificate is created by Microsoft Exchange UM Team.

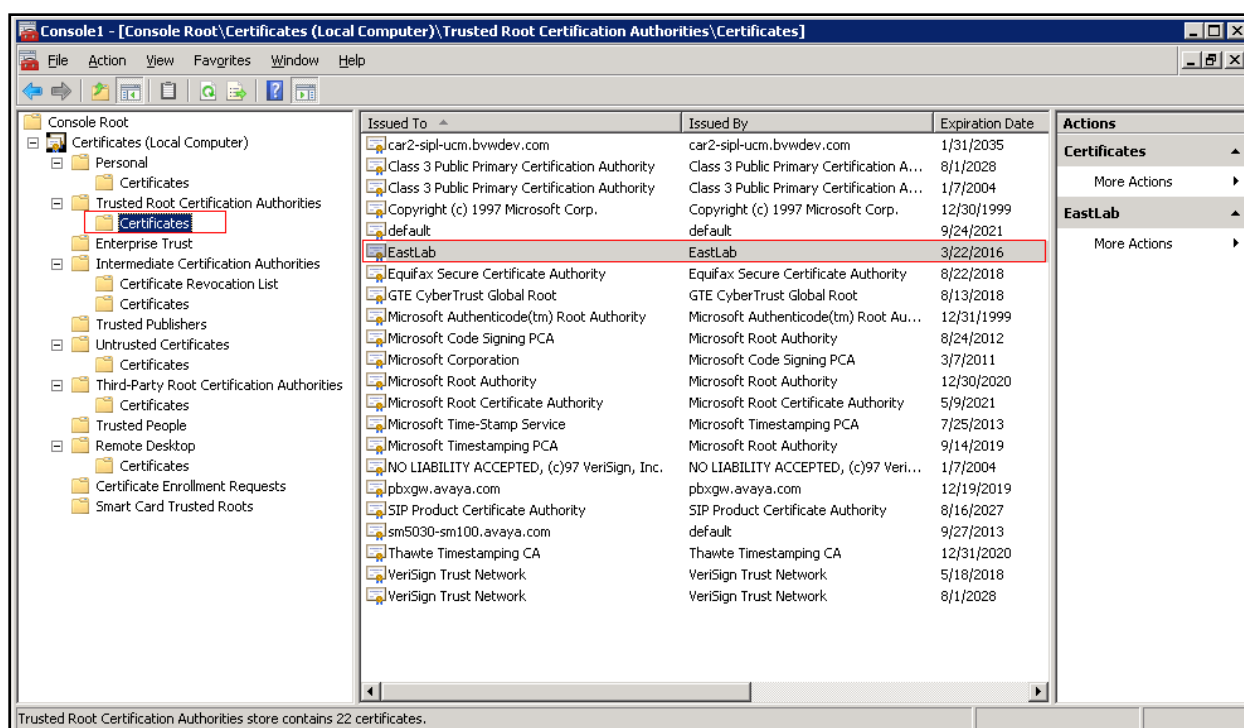


Figure 87: Certificate Console

Right-click on the “*EastLab*” certificate, select **All Task > Export**.

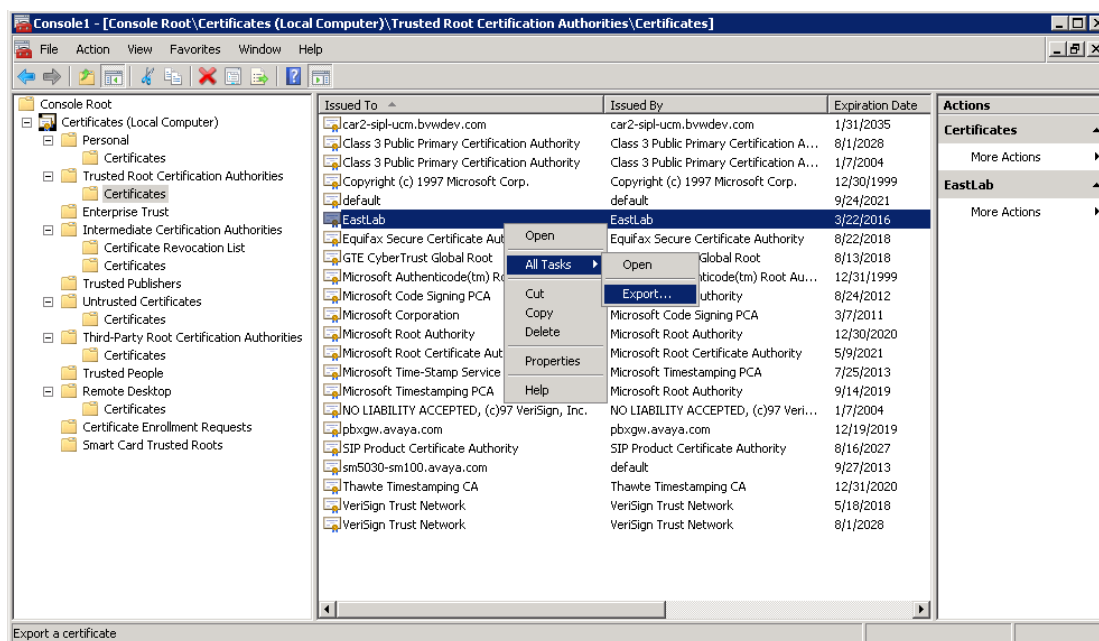


Figure 88: Certificate Console (cont)

Certificate Export Wizard displays. Click on **Next** button to continue.

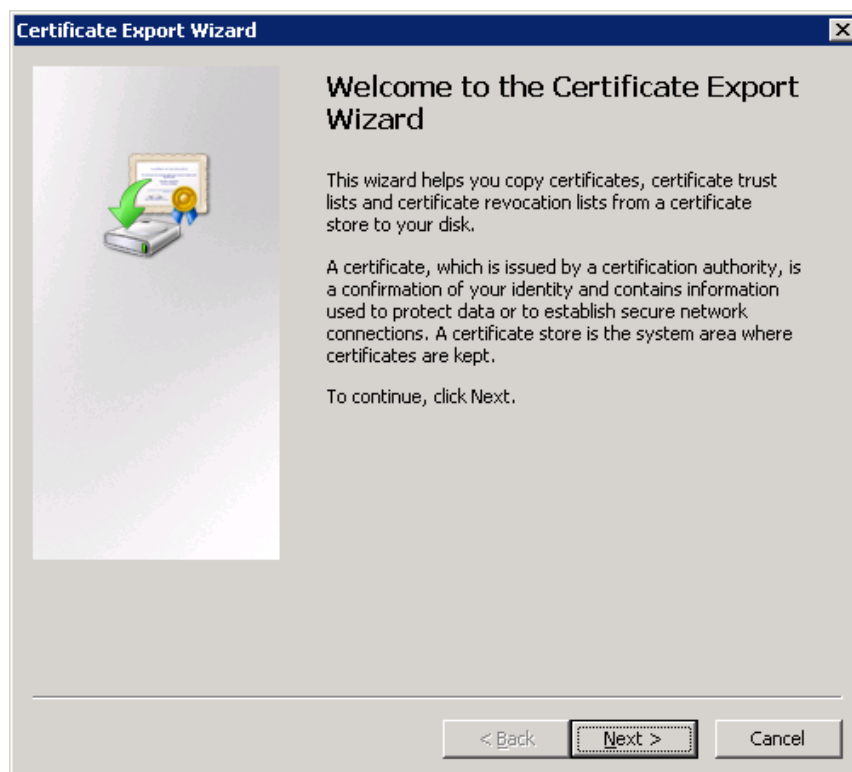


Figure 89: Certificate Export Wizard Window

Select option “*Base-64 encoded X.509 (.CER)*” in **Export File Format** section. Click on **Next** button to continue.

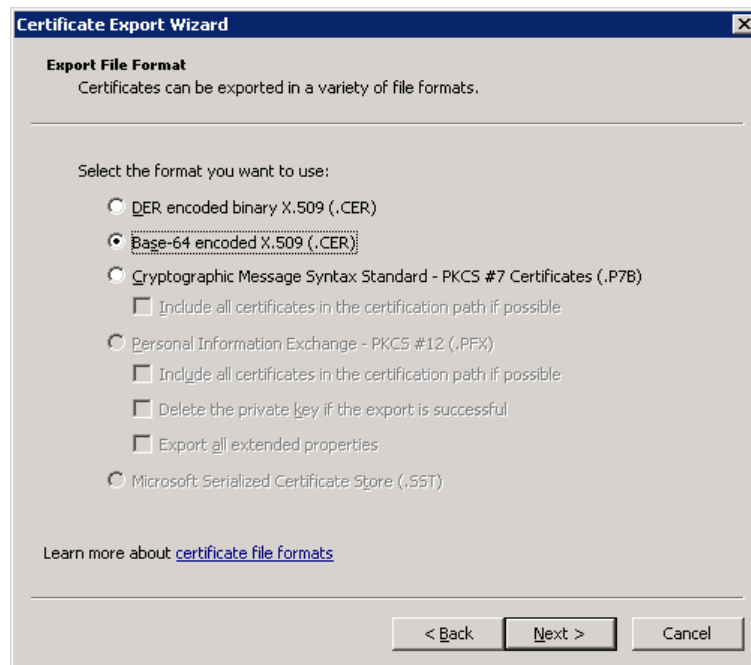


Figure 90: Certificate Export Wizard (cont)

Type the name “*ExchangeUM2010Cert*” in **File name** box. Click **Next** button to continue.

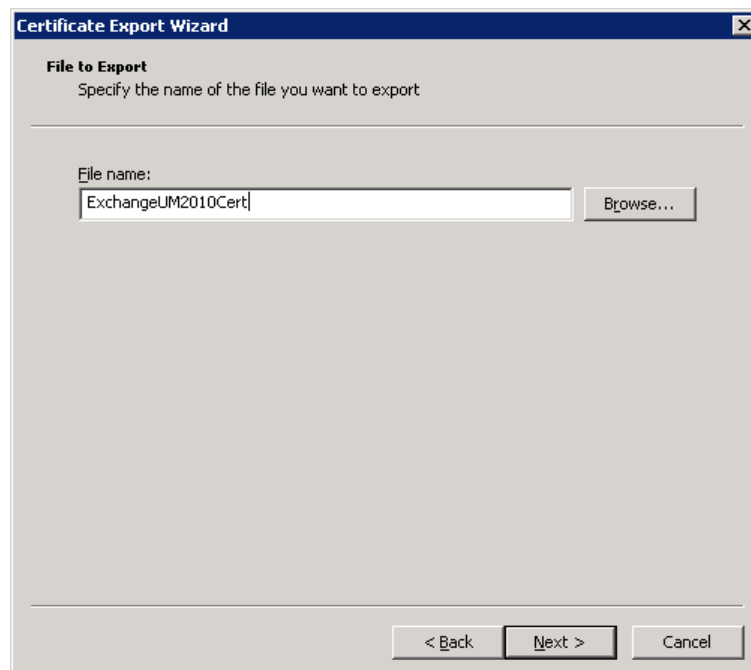


Figure 91: Certificate Export Wizard (cont)

Completing the Certificate Export Wizard section displays with summary settings. Click **Finish** button to complete.

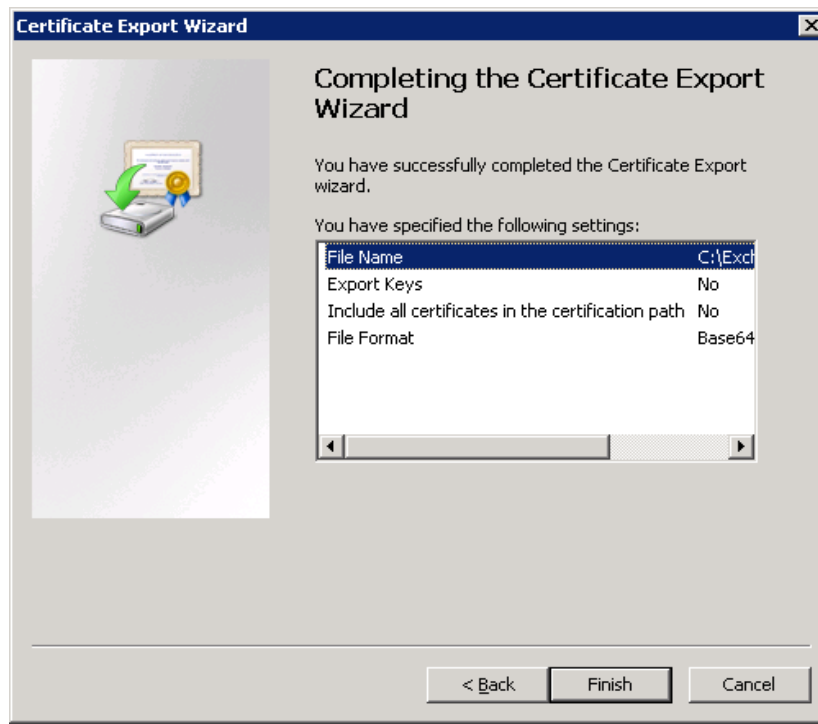


Figure 92: Certificate Export Wizard (cont)

Note: This certificate is used to import to Certificates Authorities of CS1000 SIP Gateway member in **Section 7.2**.

8.2. Import the CS1000 UCM private authority certificate to Exchange Certificate Console

From **Actions** column in the **Certificates** window of **Trusted Root Certification Authorities** folder, navigate to **More Actions > All Tasks > Import**.

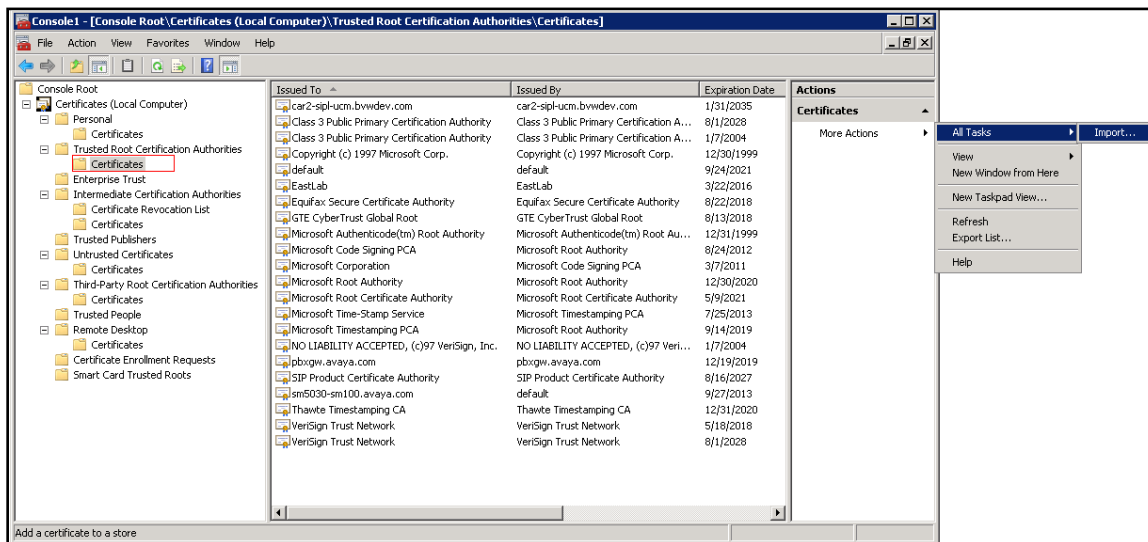


Figure 93: Export a Certificate

Certificate Import Wizard window displays. Click on **Next** button to continue.

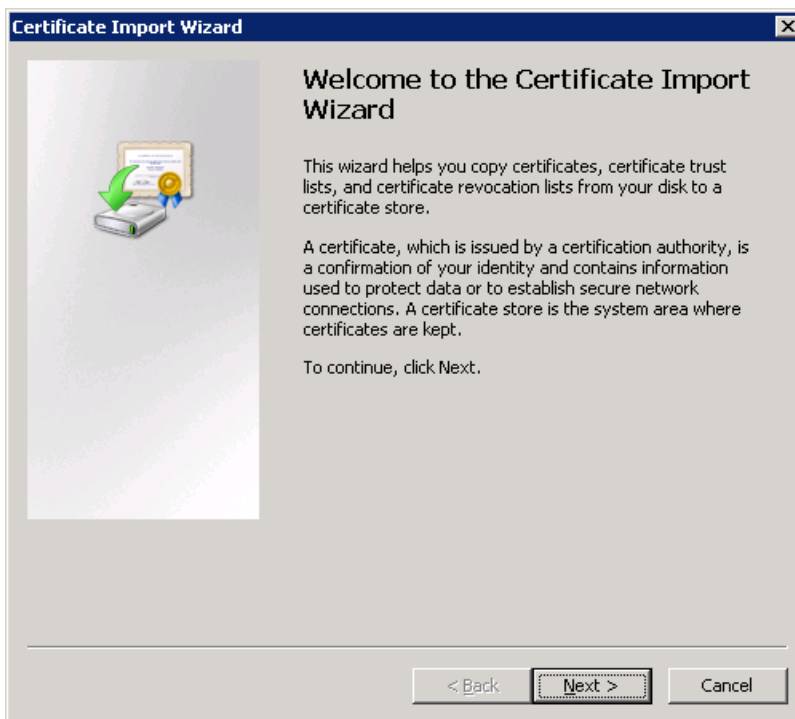


Figure 94: Certificate Export Wizard

In **File name** box, click on **Browse** button to upload the CS 1000 UCM certificate as downloaded and saved in **Section 7.3**.

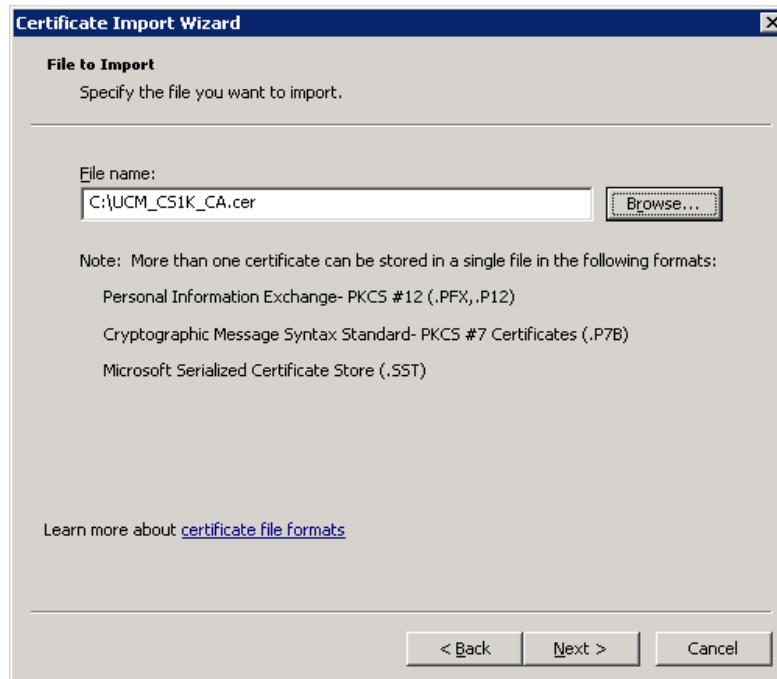


Figure 95: Export a Certificate (cont)

Select option **Place all certificates in following store** and make sure in **Certificates Store** field it should be **Trusted Root Certification Authorities**.

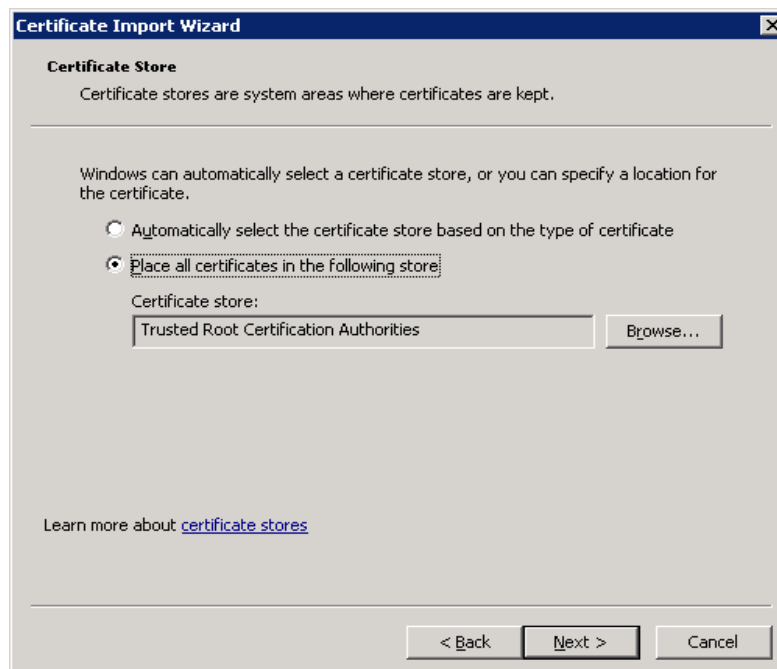


Figure 96: Export a Certificate (cont)

Click on **Finish** button to complete the import of CS 1000 UCM certificate to the Exchange UM server.

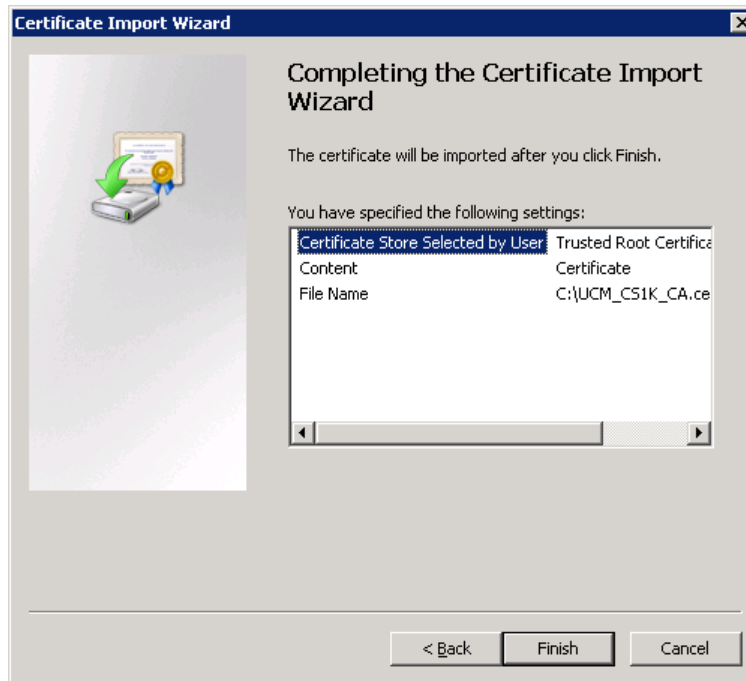


Figure 97: Export a Certificate (cont)

Figure 98 shows the CS 1000 UCM certificate has been imported to the Exchange server under **Trusted Root Certification Authorities and Certificates**.

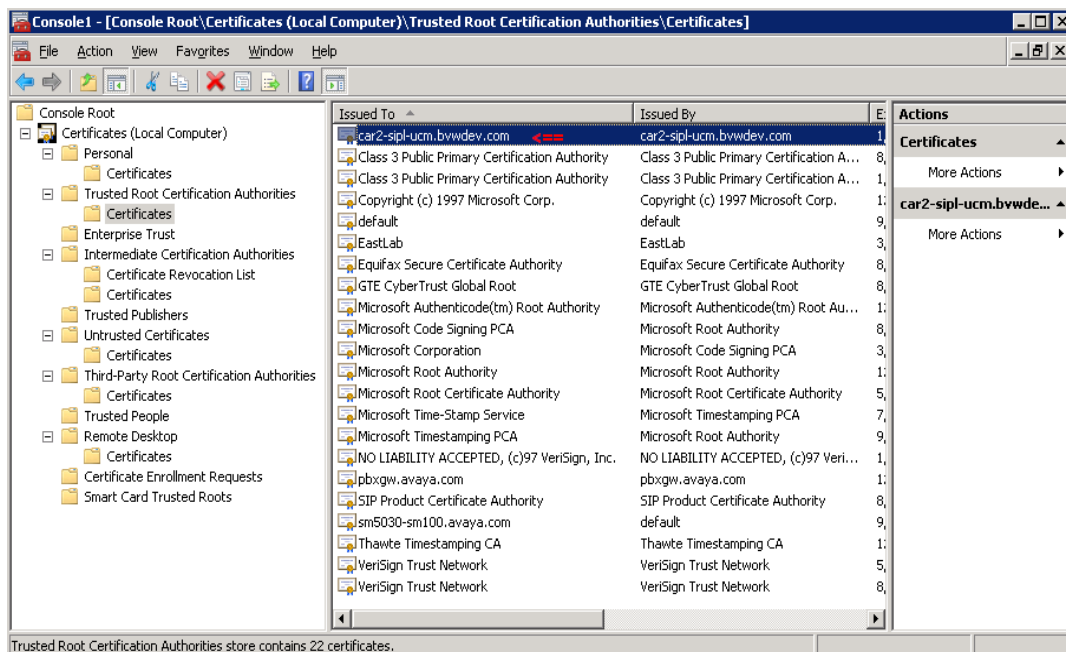


Figure 98: The UCM Certificate Imported to Exchange UM

8.3. Enable TLS on Exchange UM Server Setting

From the **Exchange Management Console** window, navigate to **Microsoft Exchange > Microsoft Exchange On-Premise > Server Configuration > Unified Messaging**. The name of Exchange server (EXCH-A-873) displays in right-hand side of the window.

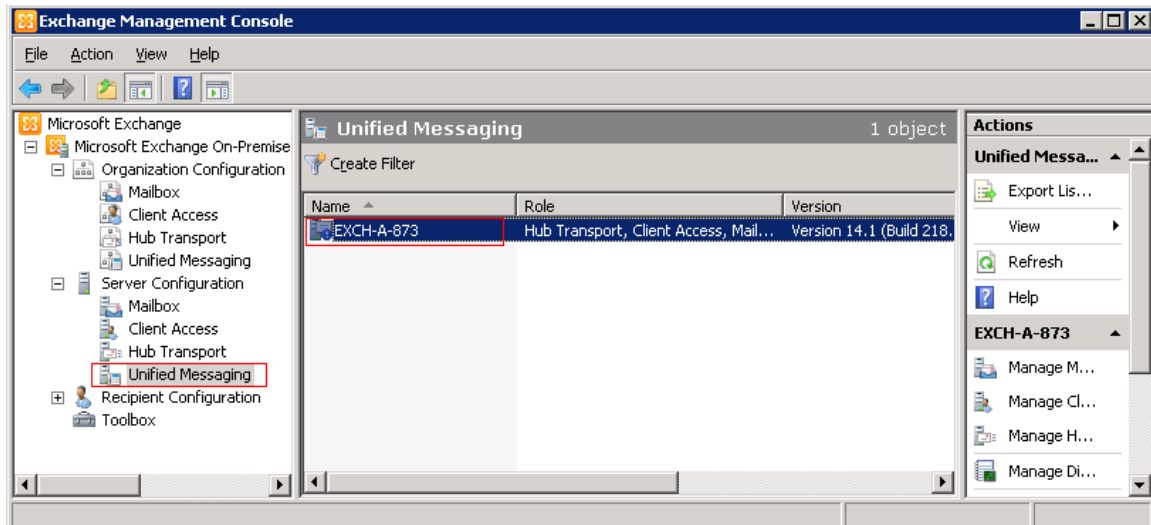


Figure 99: Server UM Settings

Double-click on this name of Exchange UM server, properties window of this sever displays. Click on **UM Settings** tab, under **Associated Dial Plans** box, select “*CS1K_CDP_5Digit*” dial plan that belongs to CS 1000 UM IP Gateway, make sure **TLS** is selected in **Startup Mode** dropdown menu.

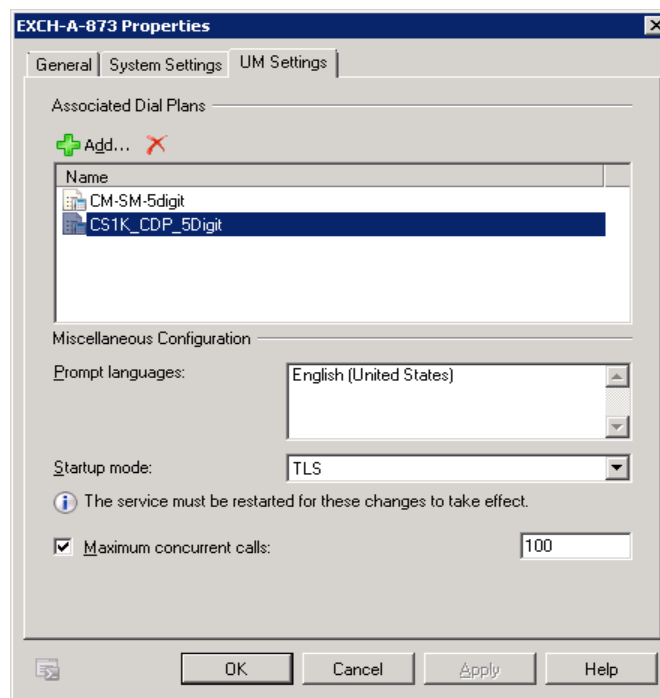
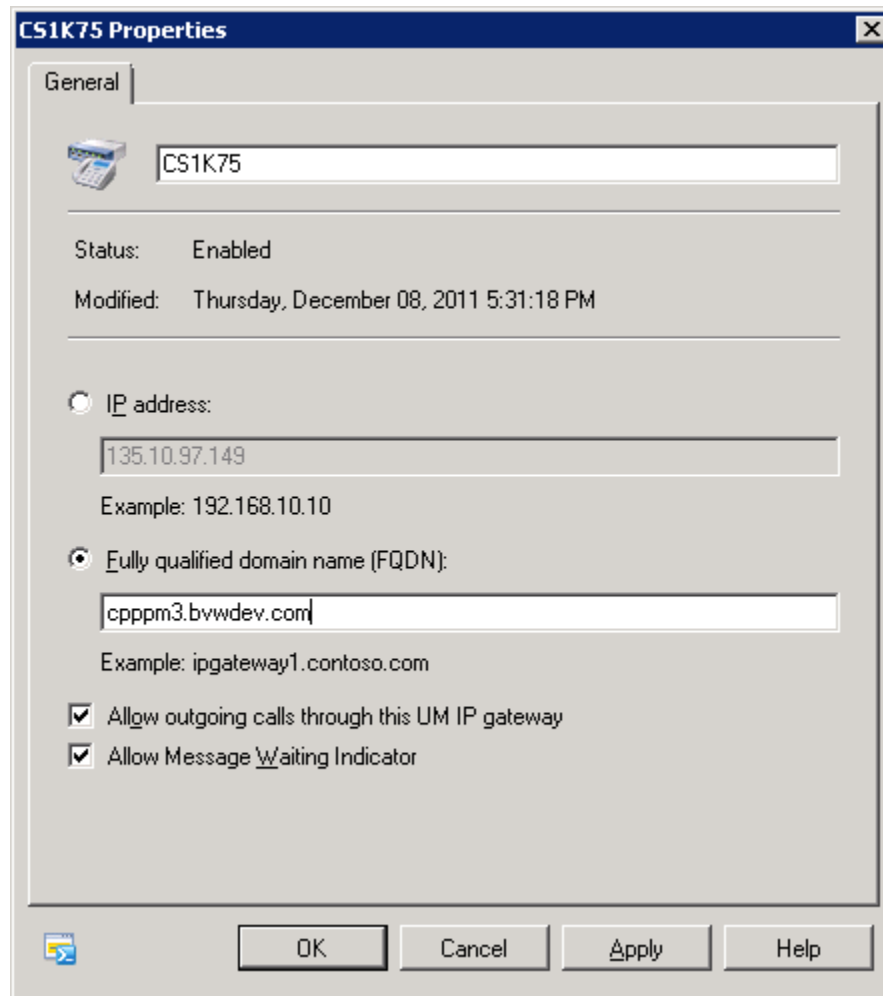



Figure 100: UM Server Properties Window

From Exchange Management Console, navigate to **Organization Configuration > Unified Messaging > UM IP Gateway** tab, and double-click on the “CS1K75” UM IP Gateway, the **CS1K Properties** Window displays, select radio option **Full qualified domain name (FQDN)** and enter “*cpppm3.bvwdev.com*” which is FQDN of SIP Gateway in the text box. Click on **Apply** button to save the change and click **OK** button to close the window.



CS1K75 Properties

General

 CS1K75

Status: Enabled

Modified: Thursday, December 08, 2011 5:31:18 PM

☐ IP address:

Example: 192.168.10.10

☒ Fully qualified domain name (FQDN):

Example: ipgateway1.contoso.com

☒ Allow outgoing calls through this UM IP gateway

☒ Allow Message Waiting Indicator


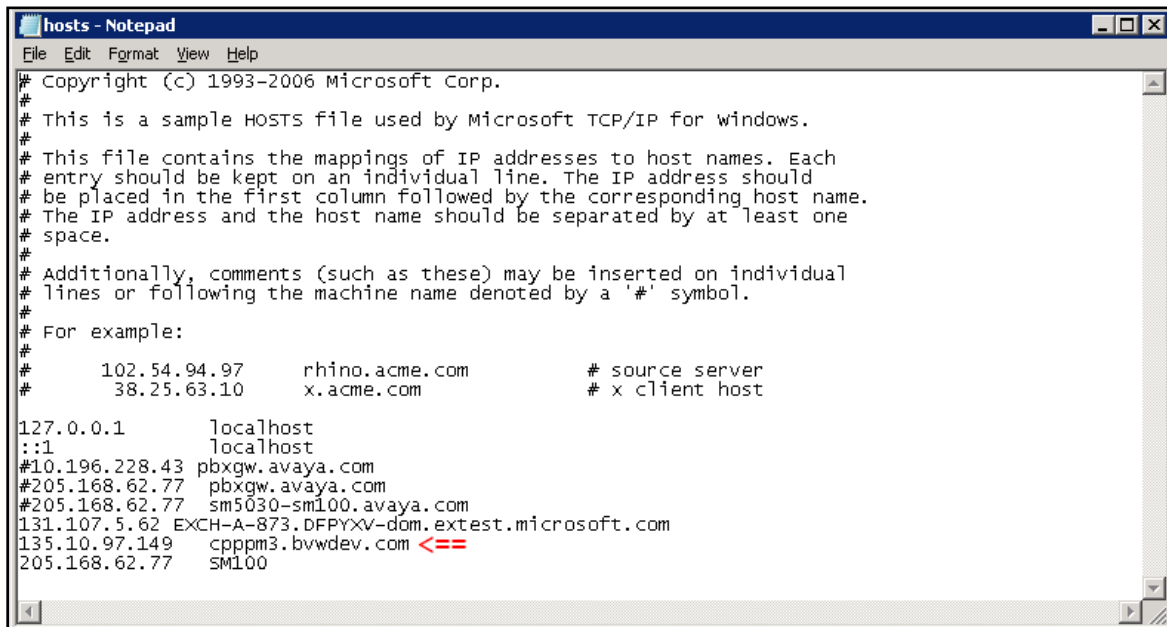


Figure 101: UM IP Gateway Properties Window

In order to SIP TLS working, the IP address of CS 1000 SIP Gateway also needs to be resolved to its FQDN in Exchange UM server. Open the hosts file in Exchange UM server to add an entry for the SIP Gateway.

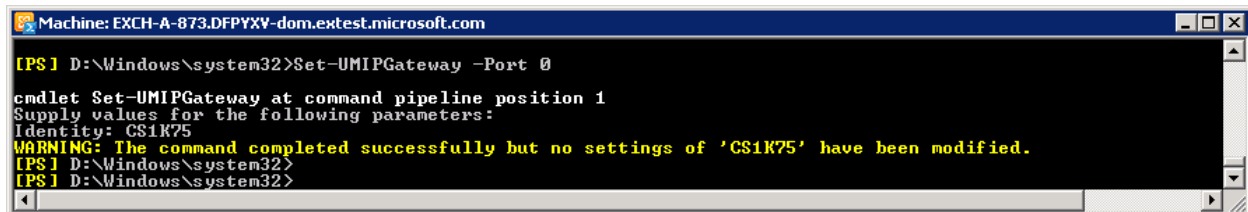


```
# Copyright (c) 1993-2006 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10       x.acme.com               # x client host

127.0.0.1       localhost
::1            localhost
#10.196.228.43    pbxgw.avaya.com
#205.168.62.77    pbxgw.avaya.com
#205.168.62.77    sm5030-sm100.avaya.com
131.107.5.62     EXCH-A-873.DFPYXV-dom.extest.microsoft.com
135.10.97.149    cpppm3.bvwdev.com <==
205.168.62.77    SM100
```

Figure 102: SIP Gateway Entry added in Hosts File

By default, Exchange UM is using port 5060 for SIP TCP, when SIP TLS is enabled the port 5060 has to change from 5060 to port 0 by using command line “Set-UMIPGateway –Port 0” in **Exchange Management Console**.



```
Machine: EXCH-A-873.DFPYXV-dom.extest.microsoft.com

[PS] D:\Windows\system32>Set-UMIPGateway -Port 0

cmdlet Set-UMIPGateway at command pipeline position 1
Supply values for the following parameters:
Identity: CS1K75
WARNING: The command completed successfully but no settings of 'CS1K75' have been modified.
[PS] D:\Windows\system32>
[PS] D:\Windows\system32>
```

Figure 103: Exchange Management Console

8.4. Configure SIP Secured on the UM Dial Plan

From the **Exchange Management Console** window, navigate to **Microsoft Exchange > Microsoft Exchange On-Premise > Organization Configuration > Unified Messaging**. List of UM dial plans displays in the UM Dial Plan tab, right-click on “*CS1K_CDP_5Digit*” dial plan and select **Properties**.

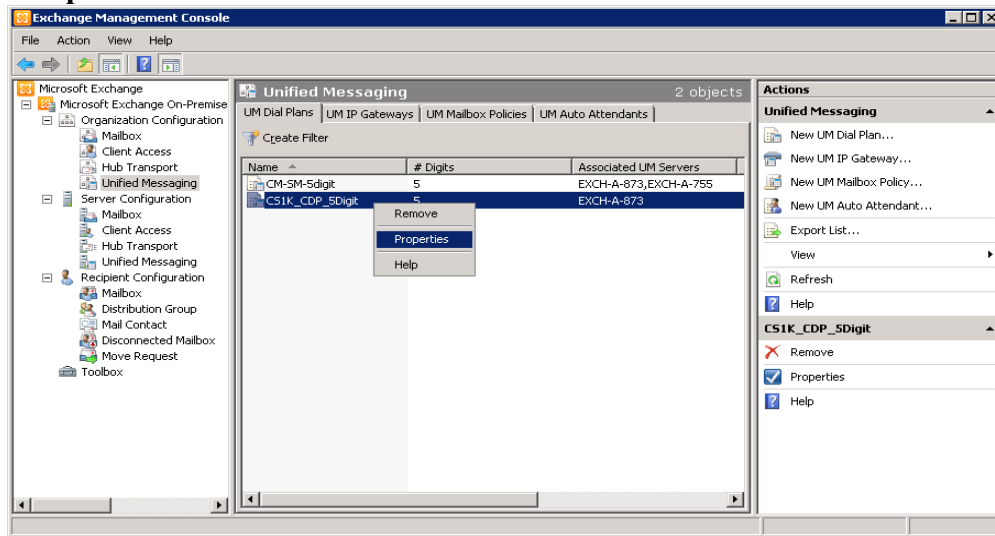


Figure 104: Properties Menu of UM Dial Plan

Select **General** tab in “*CS1K_CDP_5Digit Properties*” window, make sure **SIP Secured** is selected in **VoIP Security** dropdown menu. Note: “*SIP Secured*” selected in **VoIP Security** field means Exchange UM 2010 is just configured to work with TLS for negotiating SIP message but media is not encrypted.

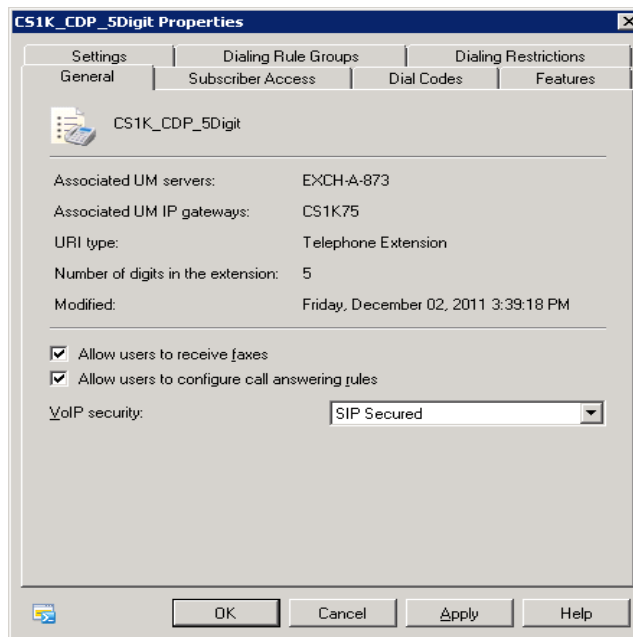


Figure 105: UM Dial Plan Properties Window

8.5. Configure VoIP Secured on UM Dial Plan

Apply the same procedures in **Section 8.4** however select **Secured** in the **VoIP Security** dropdown menu. With this selection, Exchange UM server will work with SIP TLS and its media is also secured on the “**CS1K_CDP_5Digit**” UM dial plan.

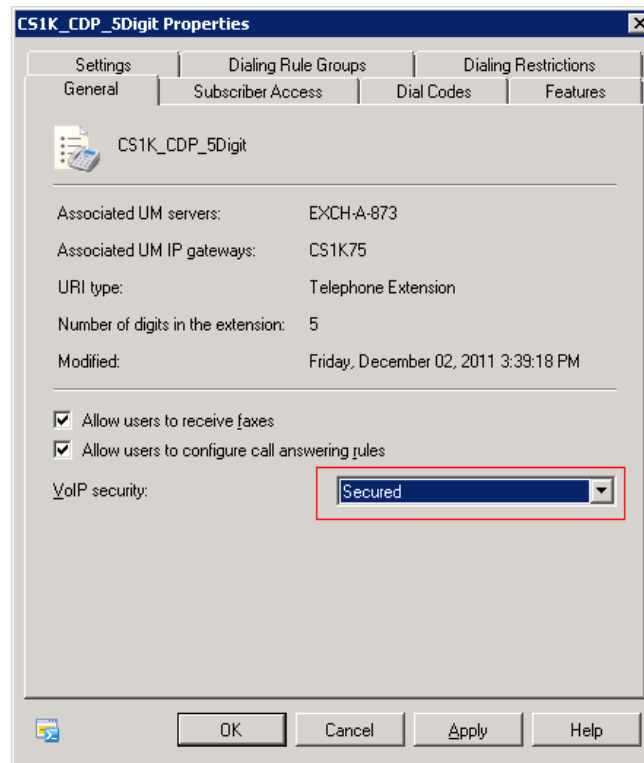


Figure 106: UM Dial Plan Properties Window with Secured Selected

Any change is made on UM Dial Plan or UM IP Gateway, Exchange UM Service needs to restart. This can be done by going to the Services application in Administration Tools and restart the Exchange UM service.

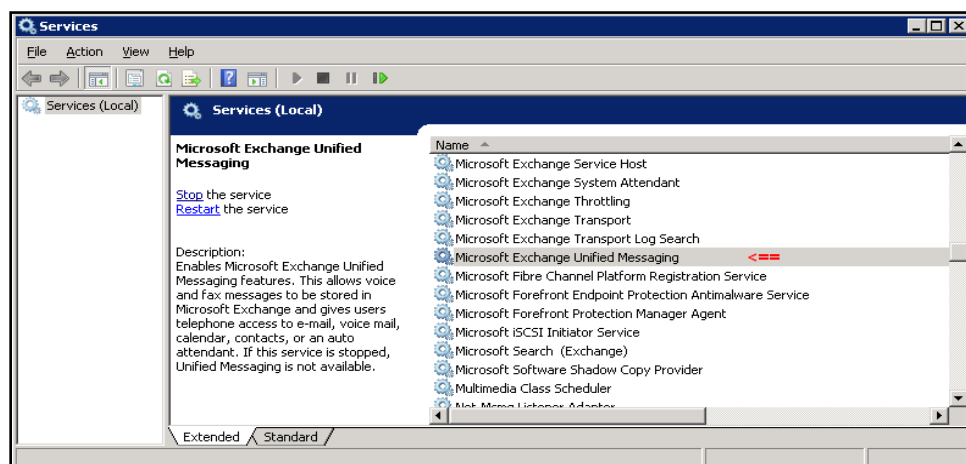


Figure 107: Services Windows with Exchange UM service.

9. Verification Steps

The following steps can be used to verify the integration of ...:

- Verify that users can dial the UM pilot number and that the proper greeting is played. If Exchange UM is called by a UM subscriber, the user should not be prompted for the extension, only the password.
- Place a call to a UM subscriber and let the call cover to voicemail. Verify that the proper greeting is played.
- Leave a voice message for a UM subscriber and verify that the MWI of the user's telephone is illuminated.
- Log on to Exchange UM to retrieve voice messages from a telephone. Use the telephone or voice interface to navigate through the menu. Verify that the voice message is heard by the user.
- Retrieve voice messages from Outlook Web Access (OWA). Enter <https://<ip-addr>/owa>, where <ip-addr> is the IP address of the Exchange 2010 server, as the URL in an Internet browser and log on. Use the Play-on-Phone feature to play the messages on a telephone.
- Delete the voice messages and verify that the MWI lamp is extinguished.
- Verify that users can dial the UM pilot number with SIP TLS and secure media, if secure media is enabled, there is a secure icon displayed on IP Unistim Phone.

10. Conclusion

These Application Notes have described the configuration steps required to integrate Microsoft Exchange Server 2010 Unified Messaging with Avaya Communication Server 1000.

Observations are noted in **Section 2.2**.

11. Additional References

Product documentation for Avaya CS 1000 products may be found at:

<https://support.avaya.com/css/Products/>

Product document for Microsoft Exchange 2010 product may be found at:

<http://www.microsoft.com/exchange/en-us/default.aspx>

[1] Avaya Communication Server 1000 Documents:

Avaya Communication Server 1000E Installation and Commissioning, Doc# NN43041-310, Issue 05.06, Date Nov 2011.

Avaya CS 1000 Co-resident Call Server and Signaling Server Fundamentals, Doc# NN43001-509, Issue 03.03, Date Aug 2011.

Avaya CS 1000 Element Manager System Reference – Administration, Doc# NN43001-632, Issue 05.13, Date Nov 2011.

Avaya Communication Server 1000 Security Management Fundamentals Release 7.5, Doc# NN43001-604, Issue 05.05, Date May 2011.

©2012 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.