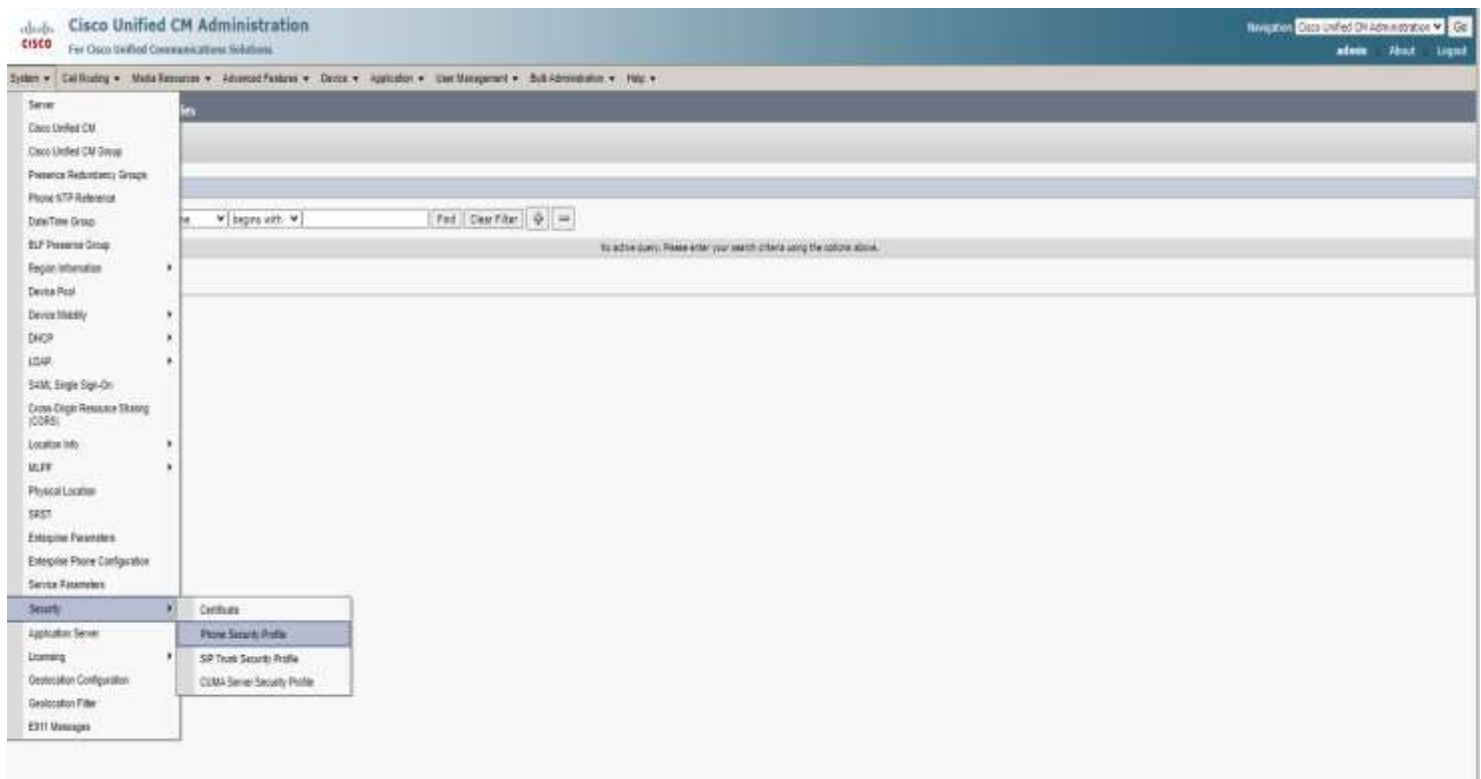


Valcom Session Initiation Protocol (SIP) VIP devices are compatible with Cisco Unified Communications Manager (formerly Cisco Unified CallManager) (SIP enabled versions). The Valcom device is added to the Communications Manager as a Third-party SIP Device (Basic or Advanced). Third-party SIP Device (Basic) supports one line, Third-party SIP Device (Advanced) supports up to eight lines.

Default, non-secure Phone Security Profiles do not require authentication for a phone to register. To enable digest authentication, a new Phone Security Profile must be configured. If an appropriate profile has already been defined, it may be used for the Valcom device. Skip to Step 5 if an existing profile will be used, or if authentication is not required and a built-in (non-secure) profile will be used.

Navigate your web browser to the IP address of your Cisco Unified Communications Manager server and login.

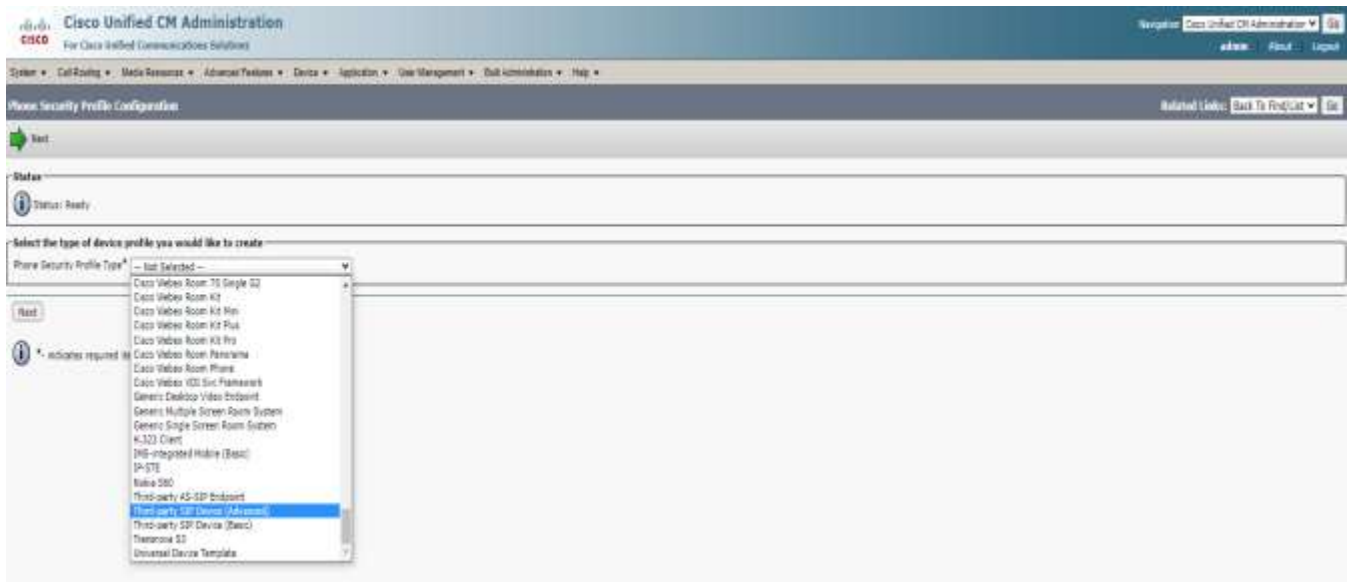
1. Go to the “System” menu, and then click “Security Profile”, then click “Phone Security Profile”.



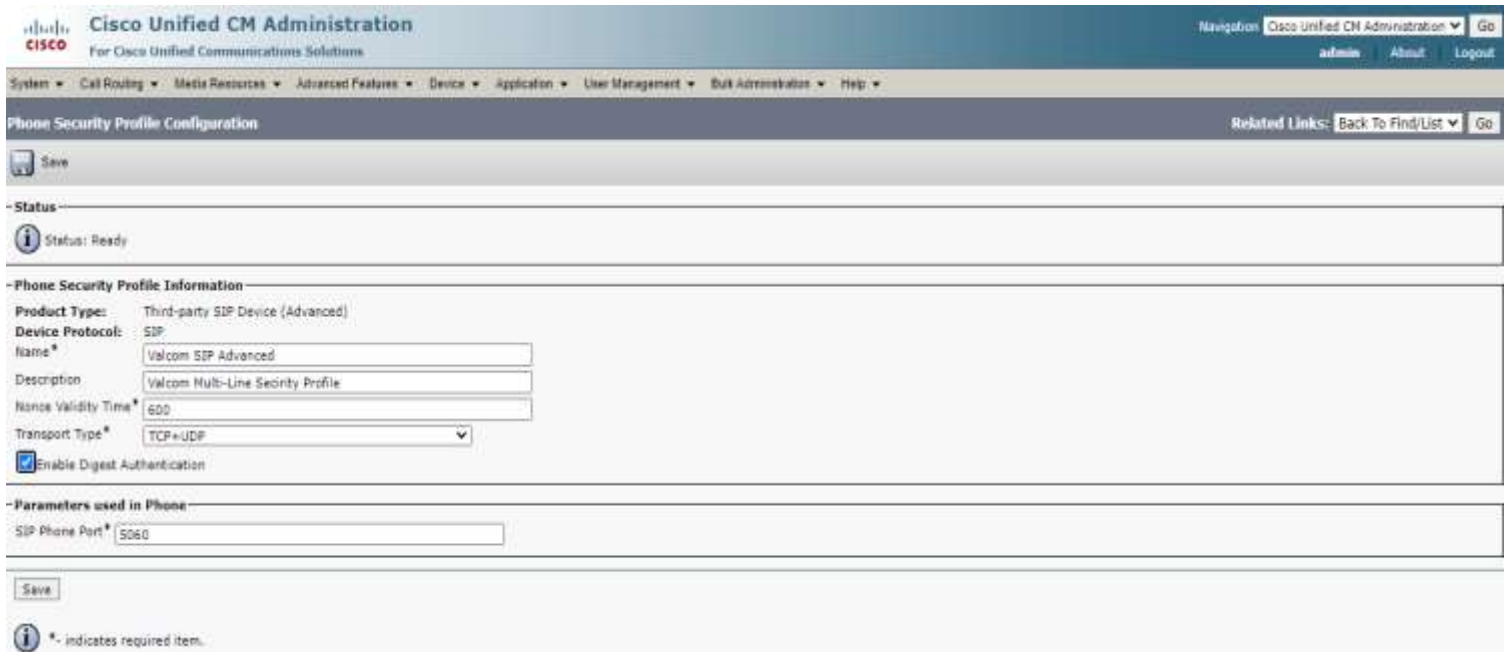
2. Click on “Add New”



3. On the Phone Security Profile Configuration screen, select the appropriate Profile Type from the dropdown list. For Valcom devices, the type will be either Third-party SIP Device (Advanced) or Third-party SIP Device (Basic). The profile being created will only be available for the phone type that is selected. Use Basic for devices that only have a single SIP identity (such as a SIP speaker). Select Advanced for devices that have multiple SIP identities (such as the VIP-201 Paging Server). Click “Next” after selecting the Type.



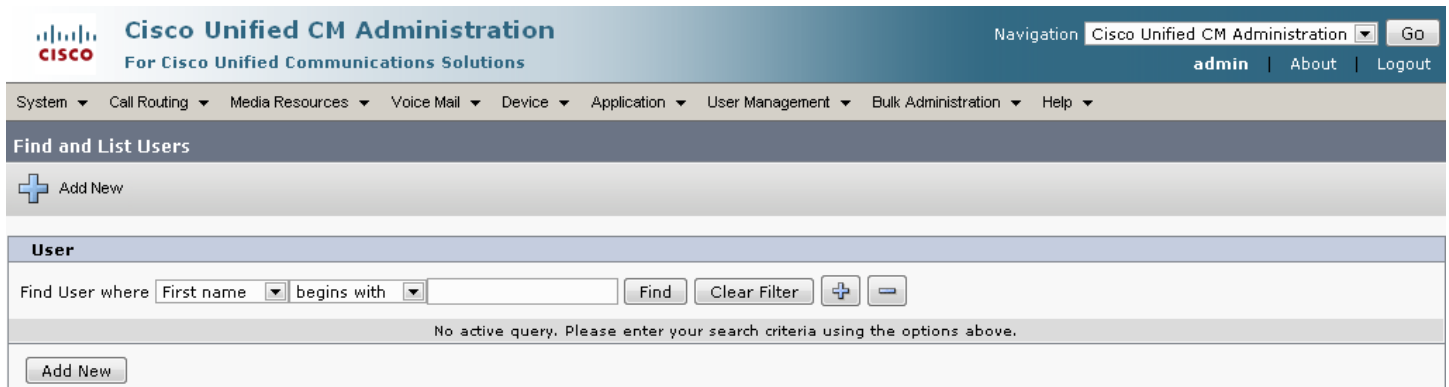
4. Enter the Phone Security Profile Information.
- Enter “Name*” (ex. Valcom SIP Advanced)
 - Enter “Nonce Validity Time*” in seconds (default 600)
 - For “Transport Type*” select “UDP” or TCP+UDP from the dropdown list
 - Check the box for “Enable Digest Authentication”
 - The “SIP Phone Port*” should be left at the default of 5060, unless it is also changed in the Valcom device.
 - Click the “Save” button when all fields have been entered.



The screenshot displays the 'Phone Security Profile Configuration' page in the Cisco Unified CM Administration interface. The page includes a navigation menu at the top with options like 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The main content area is titled 'Phone Security Profile Configuration' and features a 'Save' button. Below this, there is a 'Status' section showing 'Status: Ready'. The 'Phone Security Profile Information' section contains several fields: 'Product Type' (Third-party SIP Device (Advanced)), 'Device Protocol' (SIP), 'Name' (Valcom SIP Advanced), 'Description' (Valcom Multi-Line Security Profile), 'Name Validity Time' (600), and 'Transport Type' (TCP+UDP). There is also a checkbox for 'Enable Digest Authentication'. The 'Parameters used in Phone' section includes 'SIP Phone Port' (5060). A 'Save' button is located at the bottom of the form. A legend indicates that an asterisk (*) denotes a required item.

The following steps outline the typical device configuration process:

1. Under the “User Management” menu, select “End User”
2. Click on “Add New”



The screenshot shows the 'Find and List Users' page in the Cisco Unified CM Administration interface. The navigation menu is similar to the previous screenshot, with 'User Management' selected. The main content area is titled 'Find and List Users' and features an 'Add New' button. Below this, there is a 'User' section with a search form. The search form includes a 'Find User where' dropdown menu, a 'First name' dropdown menu, a 'begins with' dropdown menu, and a text input field. There are 'Find', 'Clear Filter', and '+ -' buttons. Below the search form, there is a message: 'No active query. Please enter your search criteria using the options above.' and an 'Add New' button.

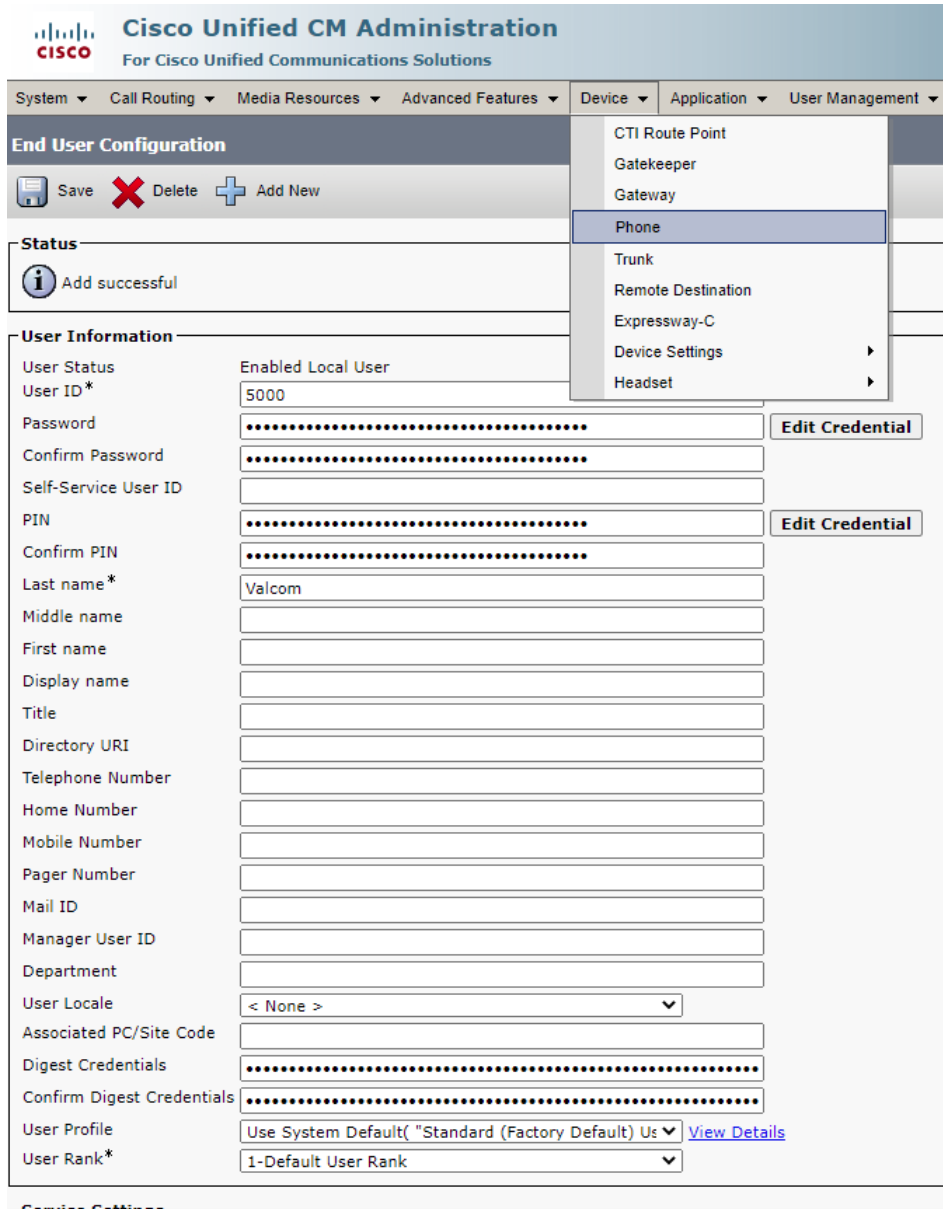
3. Complete the following steps:
 - A) Enter “User ID*” (ex. 5000) –[required for Valcom device]
 - B) Enter “Last name*” (ex. 5000) –[required for Call Manager only]
 - C) Enter “Digest Credentials” (ex. 1234) –[required for Valcom device]

- D) Enter "Confirm Digest Credentials" (ex. 1234) –[required for Valcom device]
- E) Select "Save" at the top of the screen

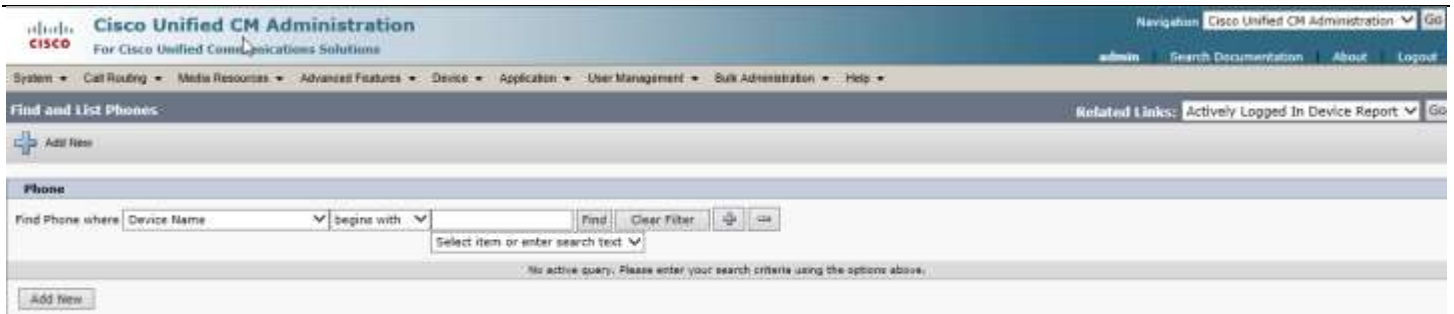
The screenshot shows the Cisco Unified CM Administration interface. At the top, there is a navigation bar with the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions". Below this is a breadcrumb trail: System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management. The main heading is "End User Configuration". Below the heading is a "Save" button. A "Status" section shows "Status: Ready". The "User Information" section contains the following fields:

User Status	Enabled Local User
User ID*	5000
Password	
Confirm Password	
Self-Service User ID	
PIN	
Confirm PIN	
Last name*	Valcom
Middle name	
First name	
Display name	
Title	
Directory URI	
Telephone Number	
Home Number	
Mobile Number	
Pager Number	
Mail ID	
Manager User ID	
Department	
User Locale	< None >
Associated PC/Site Code	
Digest Credentials	*****
Confirm Digest Credentials	*****
User Profile	Use System Default("Standard (Factory Default) Us" View Details
User Rank*	1-Default User Rank

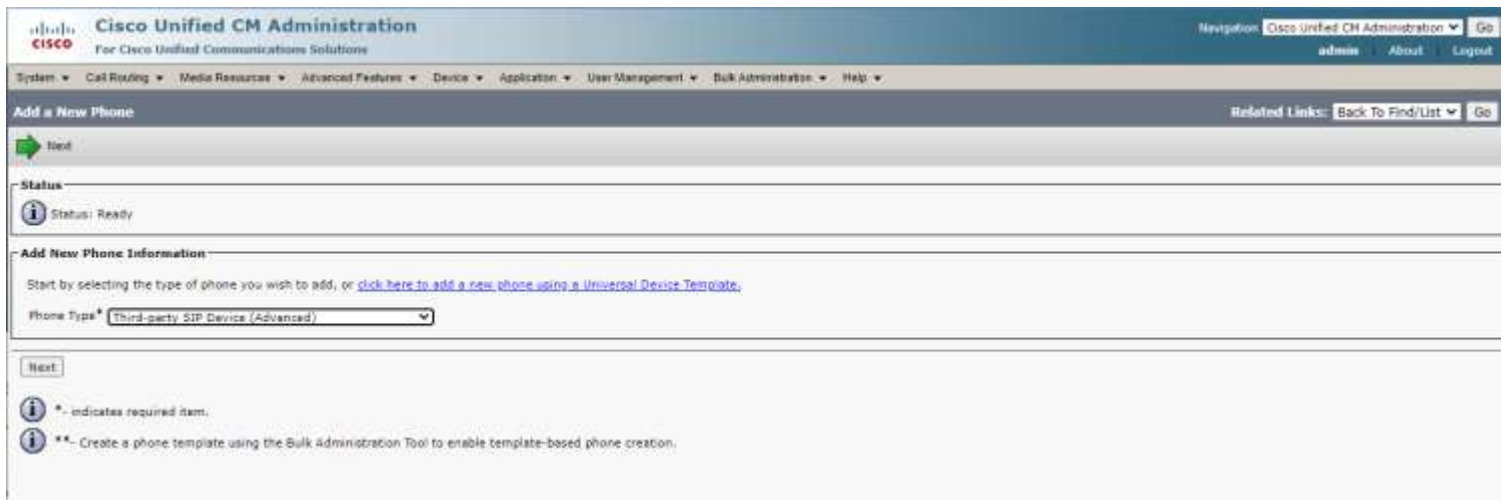
4. Click on “Device”, then click on “Phone”



and Click on “Add New”



5. Select “Third-party SIP Device (Basic)” or “Third-party SIP Device (Advanced)” from the dropdown, then click “Next”
(VIP speakers would be “Basic”, other VIP devices can be either, depending on whether more than one extension/Directory Number will be used on a VIP device)



6. Complete the following steps :
 - in Device Information Section
 - A) Enter “MAC Address*” (ex. 00D05F01D32C, use the MAC address from the Valcom device that will be registered)
 - B) Select “Device Pool*” → “Default” (or what is valid for your installation)
 - C) Select “Phone Button Template*” → “Third-party SIP Device (Basic)” or “Third-party SIP Device (Advanced)”
 - D) Select “Common Phone Profile*” → “Standard Common Phone Profile”
 - E) Select “Location*” → “Hub_None” (or what is valid for your installation)
 - F) Select “Owner” → Anonymous
 - G) Remaining Options in Device Information section can be left as default

- Status

Status: Ready

Phone Type

Product Type: Third-party SIP Device (Advanced)
Device Protocol: SIP

Device Information

Device is not trusted

MAC Address*	<input type="text" value="00D05F01D32C"/>
Description	<input type="text" value="SEP00D05F01D32C"/>
Device Pool*	<input type="text" value="Default"/> View Details
Common Device Configuration	<input type="text" value="< None >"/> View Details
Phone Button Template*	<input type="text" value="Third-party SIP Device (Advanced)"/>
Common Phone Profile*	<input type="text" value="Standard Common Phone Profile"/> View Details
Calling Search Space	<input type="text" value="< None >"/>
AAR Calling Search Space	<input type="text" value="< None >"/>
Media Resource Group List	<input type="text" value="< None >"/>
Location*	<input type="text" value="Hub_None"/>
AAR Group	<input type="text" value="< None >"/>
Device Mobility Mode*	<input type="text" value="Default"/>
Owner	<input type="radio"/> User <input checked="" type="radio"/> Anonymous (Public/Shared Space)
Owner User ID	<input type="text" value=""/>
Mobility User ID	<input type="text" value="< None >"/>
Use Trusted Relay Point*	<input type="text" value="Default"/>
Always Use Prime Line*	<input type="text" value="Default"/>
Always Use Prime Line for Voice Message*	<input type="text" value="Default"/>
Geolocation	<input type="text" value="< None >"/>
<input checked="" type="checkbox"/> Retry Video Call as Audio	
<input type="checkbox"/> Ignore Presentation Indicators (internal calls only)	
<input checked="" type="checkbox"/> Logged Into Hunt Group	
<input type="checkbox"/> Remote Device	

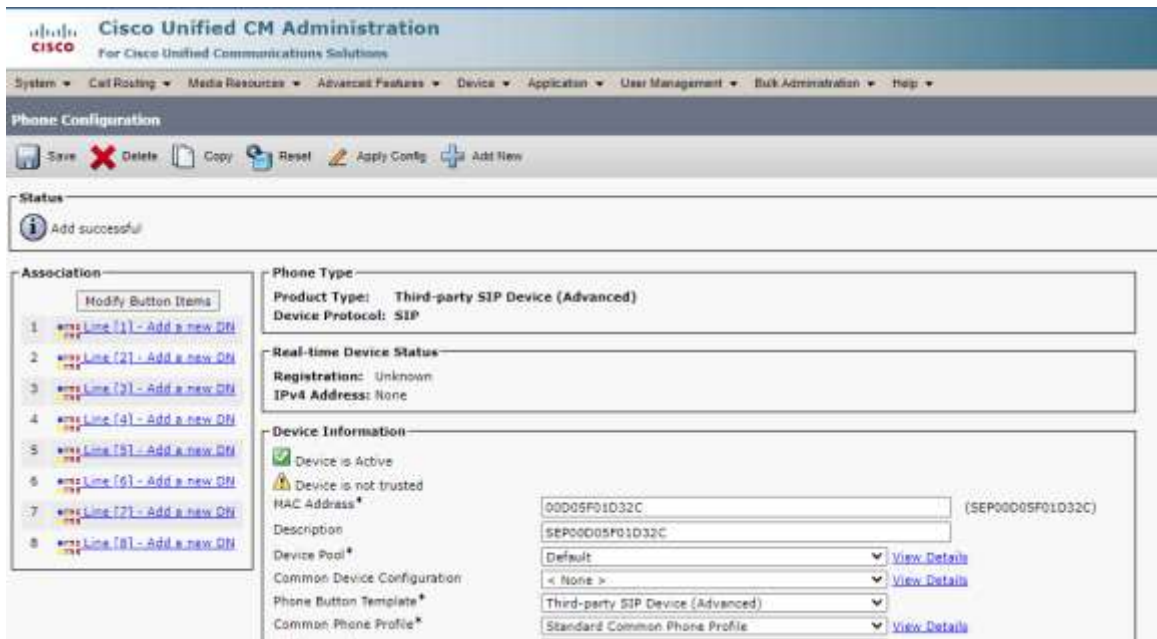
-in Protocol Specific Information Section

- H) Select “Presence Group*” → “Standard Presence group” (or what is valid for your installation)
- I) Select “MTP Preferred Originating Codec*” → “711ulaw”
- J) Select “Device Security Profile*” → “Third-party SIP Device Basic – Standard SIP Non-Secure Profile” (or a Secure Profile that you may have created –see Step 1 at the beginning of this document)
- K) Select “SIP Profile*” → “Standard SIP Profile”
- L) Select “Media Termination Point Required”
- M) Select “Digest User” → The “User ID” that was created in Step 3A. (ex. 5000)
- N) All other fields can be left at default or configure per your server/site.
- O) Select “Save” at the top of the screen.

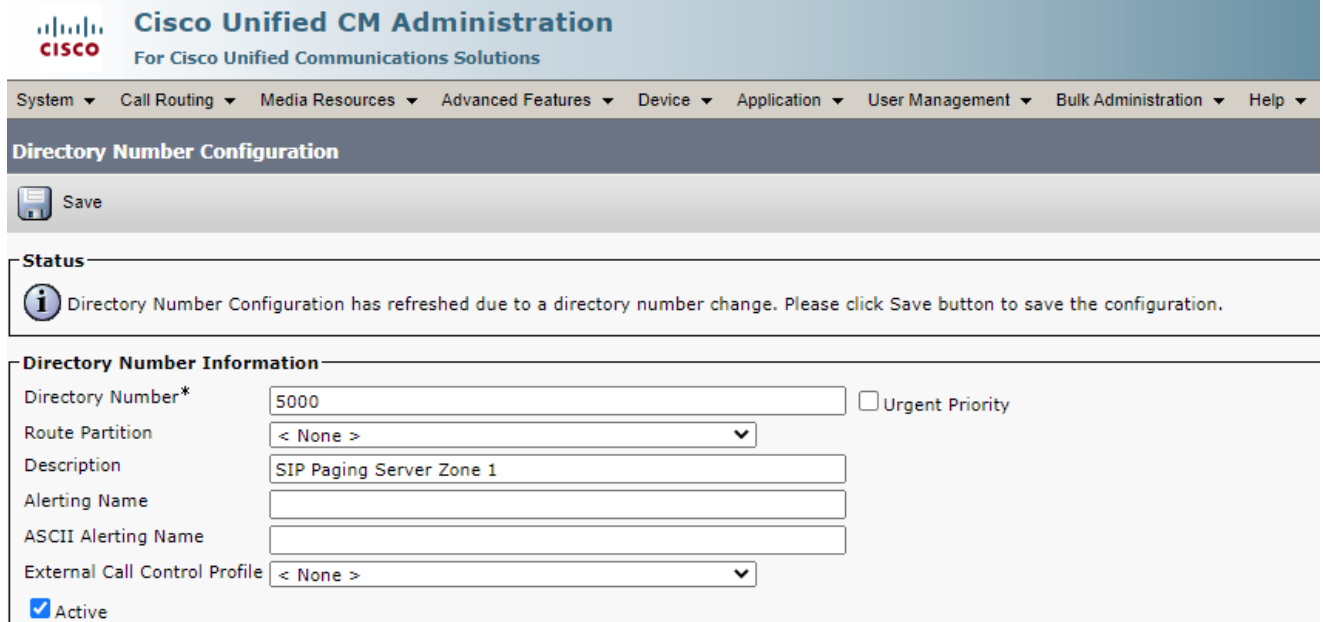
The screenshot displays the Cisco Unified CM Administration web interface. At the top, the header includes the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions". Below the header is a navigation menu with items: System, Call Routing, Media Resources, Advanced Features, Device, Application, and User Management. The main content area is titled "Phone Configuration" and contains several sections:

- Save**: A button at the top left of the configuration area.
- Use Device Pool Calling Party Transformation CSS (Caller ID For Calls From This Phone)**: A checked checkbox.
- Remote Number**: A section containing a dropdown menu for "Calling Party Transformation CSS" set to "< None >" and a checked checkbox for "Use Device Pool Calling Party Transformation CSS (Device Mobility Related Information)".
- Protocol Specific Information**: A section with several dropdown menus and checkboxes:
 - BLF Presence Group*: Standard Presence group
 - MTP Preferred Originating Codec*: 711ulaw
 - Device Security Profile*: Valcom SIP Device Advanced - Standard SIP Secure
 - Rerouting Calling Search Space: < None >
 - SUBSCRIBE Calling Search Space: < None >
 - SIP Profile*: Standard SIP Profile (with a "View Details" link)
 - Digest User: 5000
 - Media Termination Point Required: checked
 - Unattended Port: unchecked
 - Require DTMF Reception: unchecked
 - Allow Presentation Sharing using BFCP: unchecked
 - Allow iX Applicable Media: unchecked
- MLPP and Confidential Access Level Information**: A section with three dropdown menus, all set to "< None >":
 - MLPP Domain
 - Confidential Access Mode
 - Confidential Access Level
- Save**: A button at the bottom of the configuration area.

7. Select “Line [1] – Add a new DN” under “Association”.



8. Complete the following steps:
 - in Directory Number Information
 - A) Enter “Directory Number*” (ex. 5000)
 - B) Route Partition use default or what is applicable to your site
 - C) Enter “Description” (ex. SIP Paging Server Zone 1)
 - D) Check the Active checkbox, if not already checked
 - in Directory Number Settings
 - E) Select “Presence Group*” → “Standard Presence group” (or what is valid for your installation)



The screenshot shows the Cisco Unified CM Administration interface. At the top, there is a navigation menu with options: System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. Below this is a header for "Directory Number Configuration" with a "Save" button. A status message indicates that the configuration has refreshed due to a directory number change and prompts the user to click the Save button. The main configuration area, titled "Directory Number Information", contains the following fields:

- Directory Number*: 5000
- Route Partition: < None >
- Description: SIP Paging Server Zone 1
- Alerting Name: (empty)
- ASCII Alerting Name: (empty)
- External Call Control Profile: < None >
- Urgent Priority: (unchecked)
- Active: (checked)

-in Line 1 on Device SEP00D05F01D32C

F) Key in "Display (Caller ID)" with a name or number to identify this (DN) extension **useful if using talkback speakers that can call into the Call Manager.*

-in Multiple Call/Call Waiting Settings on Device SEP00D05F01D32C

G) Enter "Maximum Number of Calls*" → "2"

H) Enter "Busy Trigger*" → "2"

-in Forwarded Call Information Display on Device SEP00D05F01D32C

I) Check "Caller Name"

J) Check "Dialed Number"

K) Select "Save" at the bottom or top of the screen

L) Click "Apply Config" at top of screen

The screenshot shows the 'Directory Number Configuration' page in Cisco Unified CM Administration. The page is titled 'Directory Number Configuration' and includes a 'Save' button. The configuration fields are as follows:

- Target (Destination): [Text Input]
- HLPP Calling Search Space: [None]
- HLPP No Answer Ring Duration (seconds): [Text Input]
- Confidential Access Mode: [None]
- Confidential Access Level: [None]
- Call Control Agent Profile: [None]

- Line Settings for All Devices -

- Hold Reversion Ring Duration (seconds): [Text Input] Setting the Hold Reversion Ring Duration to zero will disable the feature.
- Hold Reversion Notification Interval (seconds): [Text Input] Setting the Hold Reversion Notification Interval to zero will disable the feature.
- Party Entrance Tone: [Default]

- Line 1 on Device SEP00005F01D32C -

- Display (Caller ID): [Text Input] Display text for a line appearance is intended for displaying text such as a name instead of a directory number for calls. If you specify a number, the person receiving a call may not see the proper identity of the caller.
- ASCII Display (Caller ID): [Text Input]
- External Phone Number Mask: [Text Input]
- Monitoring Calling Search Space: [None]

- Multiple Call/Call Waiting Settings on Device SEP00005F01D32C -

- Note: The range to select the Max Number of calls is: 1-15
- Maximum Number of Calls*: [2]
- Busy Trigger*: [2] (Less than or equal to Max. Calls)

- Forwarded Call Information Display on Device SEP00005F01D32C -

- Caller Name
- Caller Number
- Redirected Number
- Dialed Number

M) Click Related Links: Configure Device Go button to return to device screen

This screenshot shows the same 'Directory Number Configuration' page, but with the action buttons at the bottom visible: Save, Delete, Reset, Apply Config, and Add New. The 'Related Links' section at the top right shows 'Configure Device (SEP00005F01D32C)' with a 'Go' button next to it.

The screenshot displays the Cisco Unified CM Administration web interface. At the top, the navigation menu includes System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main header reads "Cisco Unified CM Administration For Cisco Unified Communications Solutions".

The "Phone Configuration" section is active, showing a toolbar with Save, Delete, Copy, Reset, Apply Config, and Add New buttons. Below this, the "Status" section indicates the phone is "Ready".

The "Association" panel on the left lists eight lines, each with a "Modify Button Items" link and a "Add a new DN" link. Line 1 is selected, showing "Line 1] - 5000 (no partition)".

The main configuration area is divided into several sections:

- Phone Type:** Product Type: Third-party SIP Device (Advanced); Device Protocol: SIP
- Real-time Device Status:** Registration: Unknown; IPv4 Address: None
- Device Information:**
 - Device is Active:
 - Device is not trusted:
 - MAC Address*: 00D05F01D32C (SEP00D05F01D32C)
 - Description: SEP00D05F01D32C
 - Device Pool*: Default (View Details)
 - Common Device Configuration: < None > (View Details)
 - Phone Button Template*: Third-party SIP Device (Advanced)
 - Common Phone Profile*: Standard Common Phone Profile (View Details)
 - Calling Search Space: < None >
 - AAR Calling Search Space: < None >
 - Media Resource Group List: < None >
 - Location*: Hub_None
 - AAR Group: < None >
 - Device Mobility Mode*: Default (View Current Device Mobility Settings)
 - Owner: User Anonymous (Public/Shared Space)
 - Owner User ID: < None >
 - Mobility User ID: < None >
 - Use Trusted Relay Point*: Default
 - Always Use Prime Line*: Default
 - Always Use Prime Line for Voice Message*: Default
 - Geolocation: < None >
 - Retry Video Call as Audio:
 - Ignore Presentation Indicators (internal calls only):
 - Logged Into Hunt Group:
 - Remote Device:

- N) You can repeat steps A-F if configuring more than 1 extension
- O) When done Click "Apply Config"



Cisco Unified Communications Manager 14.0 SIP Configuration Guide

-
9. Open the VIP-102B tool interface for the Valcom SIP enabled VIP device.

Note: The information contained in this guide is limited to configuration of the "SIP" tab in the VIP-102B IP Solutions Setup Tool for the Valcom VIP device that is to be registered to the SIP server. More information on Valcom VIP device configuration, such as IP address assignment, relay activation, etc, may be found in the VIP-102B Reference Manual. This document may be downloaded from our website at <http://www.valcom.com>

In order to Register:

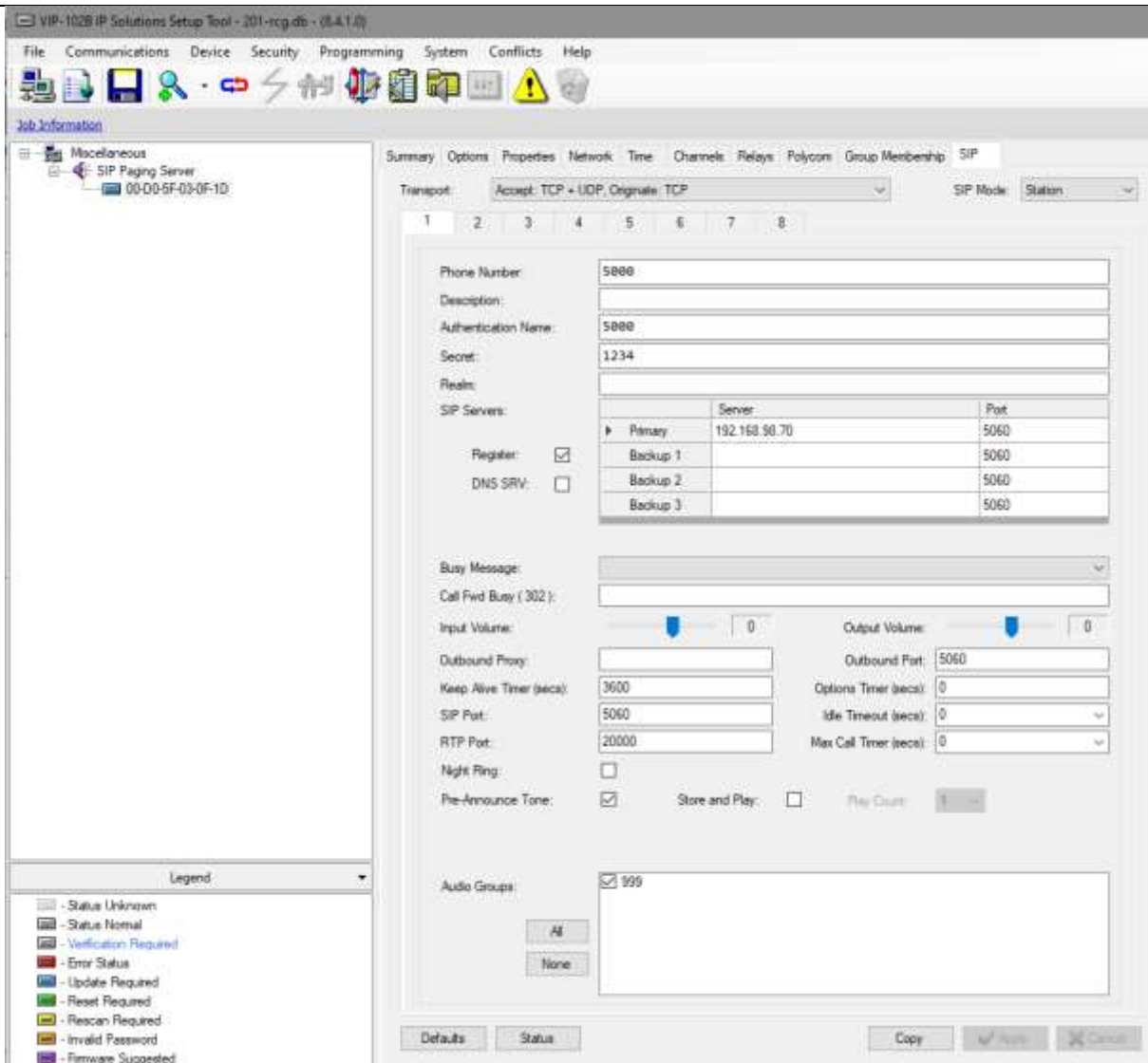
Required Fields: Phone Number, Authentication Name, Secret, SIP Server (primary), Register, SIP Server Port, SIP Port, RTP Port

Optional Fields: Description, Realm, SIP Server Backup 1, 2, and 3, DNS SRV, CID Name, CID Number.

*In our example, the SIP Server IP address is the same as our Cisco Call Manager, "192.168.98.70". If using a host name here you must specify at least one DNS server on the Network tab to resolve the name.
Phone Number is the same as our Directory Number in the Cisco Call Manager configuration, "5000".
Secret is the same as our Digest Credentials in the Cisco Call Manager configuration, "1234".
SIP Server Port is the port number, on which the Cisco Call Manager SIP server is listening for SIP data.
SIP Port is the port number, on which the Valcom VIP device is listening for SIP data. By default this is set for "5060".
RTP Port is the port number, on which the Valcom VIP device is set to send/receive audio packets, via SIP. By default this is set for "20000". All other optional fields may be used based on your server/site requirements.*

For this particular device, the SIP paging server, other fields on the SIP tab relate to functionality of the device. Definition of these fields may be found in the VIP-102B Reference Manual under the SIP Tab (VIP-201, VIP-204). This document may be downloaded from our website at <http://www.valcom.com>

When the Valcom VIP device configuration is complete, select the "Update Changed Devices" button, at the upper left. When update is complete, click reset, to reboot the device.



- To confirm a successful configuration, return to Call Manager and click on "Device", then Phone, then locate the VIP device in the search results. If successfully registered, the status column should show the VIP device is registered to the IP address of the Call Manager with the VIP device's IP address in the next column under "IP Address"