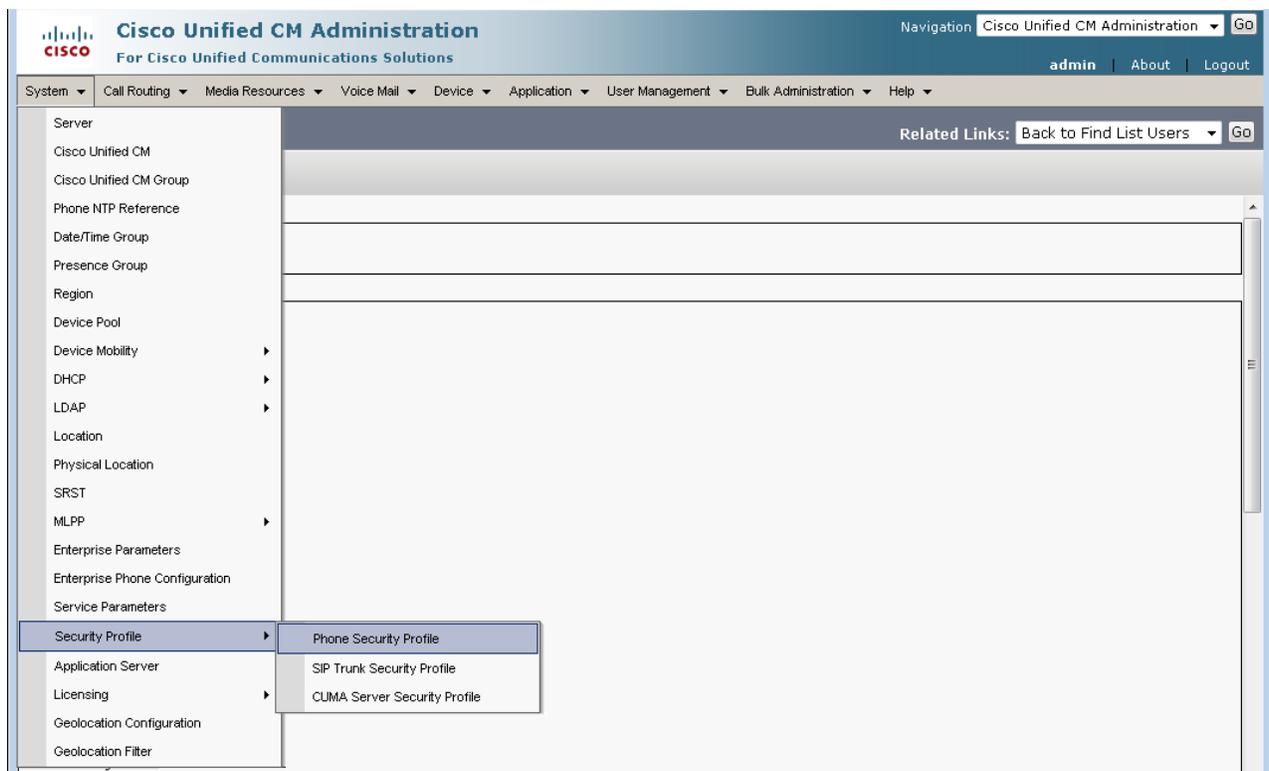


Valcom Session Initiation Protocol (SIP) VIP devices are compatible with Cisco Unified Communications Manager (formerly Cisco Unified CallManager) (SIP enabled versions). The Valcom device is added to the Communications Manager as a Third-party SIP Device (Basic or Advanced). Third-party SIP Device (Basic)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

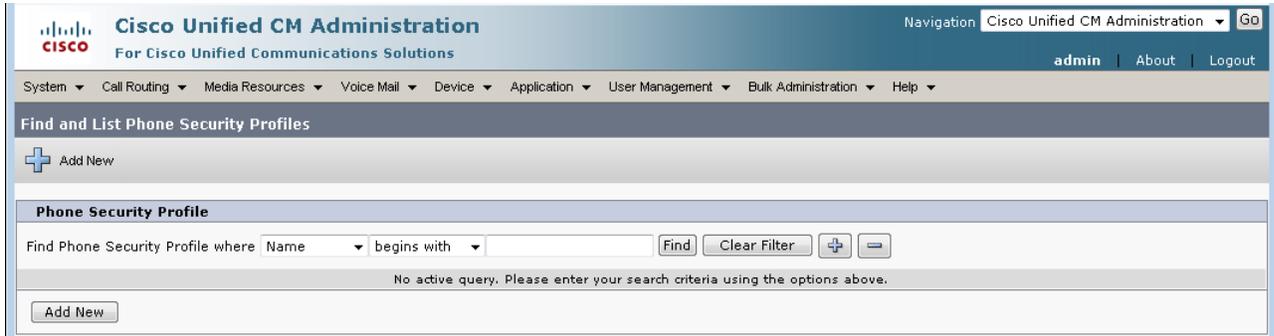
Default, non-secure Phone Security Profiles do not require authentication for a phone to register. To enable digest authentication, a new Phone Security Profile must be configured. If an appropriate profile has already been defined, it may be used for the Valcom device. Skip to Step 5 if an existing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

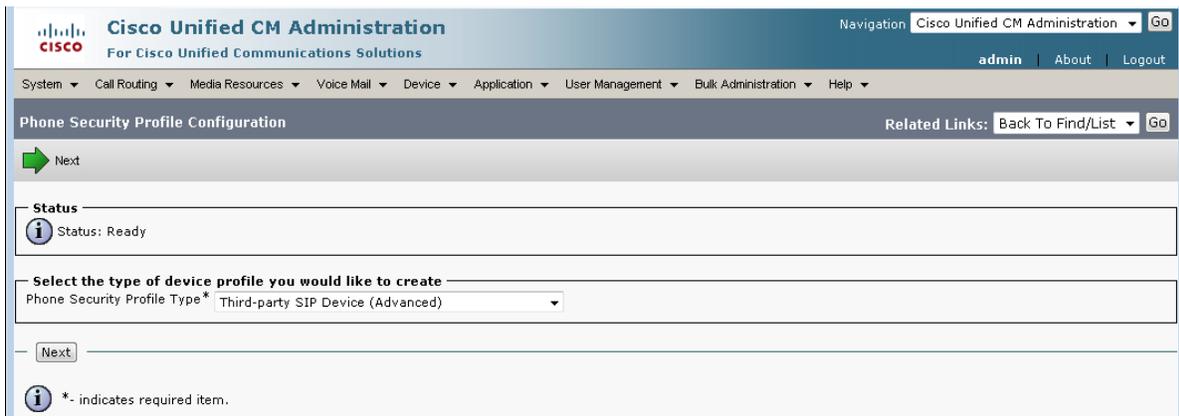
1. Go to the “System” menu, and then click “Security Profile”, then click “Phone Security Profile”.



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

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

admin | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

### Phone Security Profile Configuration

Related Links: [Back To Find/List](#)

**Status**  
 Status: Ready

**Phone Security Profile Information**

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

Name\*   
Description   
Nonce Validity Time\*   
Transport Type\*

Enable Digest Authentication

**Parameters used in Phone**

SIP Phone Port\*

 \*. indicates required item.

The following steps outline the typical device configuration process:

1. Under the “User Management” menu, select “End User”

The screenshot shows the Cisco Unified CM Administration interface. The top navigation bar includes the Cisco logo, the title 'Cisco Unified CM Administration For Cisco Unified Communications Solutions', and a 'Navigation' dropdown menu set to 'Cisco Unified CM Administration' with a 'Go' button. Below the navigation bar is a menu bar with options: System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main content area is titled 'Find and List Users' and features a '+ Add New' button. Below this is a search section for 'User' with dropdown menus for 'First name' and 'begins with', a search input field, and buttons for 'Find', 'Clear Filter', '+', and '-'. A message below the search area reads: 'No active query. Please enter your search criteria using the options above.' At the bottom left of the search area is an 'Add New' button.

2. Click on “Add New”

This screenshot is identical to the previous one, showing the 'Find and List Users' section. The '+ Add New' button is highlighted with a blue border, indicating it has been selected.

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

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ U

### End User Configuration

Save

---

#### User Information

User Status	Enabled Local User
User ID*	<input type="text" value="5000"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Self-Service User ID	<input type="text"/>
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
Last name*	<input type="text" value="Valcom"/>
Middle name	<input type="text"/>
First name	<input type="text"/>
Display name	<input type="text"/>
Title	<input type="text"/>
Directory URI	<input type="text"/>
Telephone Number	<input type="text"/>
Home Number	<input type="text"/>
Mobile Number	<input type="text"/>
Pager Number	<input type="text"/>
Mail ID	<input type="text"/>
Manager User ID	<input type="text"/>
Department	<input type="text"/>
User Locale	< None > ▾
Associated PC	<input type="text"/>
Digest Credentials	<input type="password" value="••••"/>
Confirm Digest Credentials	<input type="password" value="••••"/>
User Profile	Use System Default( "Standard (Factory Default) Us ▾ <a href="#">View Details</a>

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

The screenshot displays the Cisco Unified CM Administration web interface. At the top, the navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', and 'User Management'. The 'Device' menu is open, showing options: 'CTI Route Point', 'Gatekeeper', 'Gateway', 'Phone', 'Trunk', 'Remote Destination', and 'Device Settings'. The 'Phone' option is highlighted with a mouse cursor. Below the navigation, the 'End User Configuration' section contains 'Save', 'Delete', and 'Add New' buttons. A 'Status' message indicates 'Add successful'. The 'User Information' section is active, showing a form for an 'Enabled Local User' with the following fields: 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, Digest Credentials, and Confirm Digest Credentials. Two 'Edit Credential' buttons are visible on the right side of the form.

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:
  - 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” → User
  - G) Select “Owner User ID” → The “User ID” that was created in Step 3A. (ex. 5000)

**Cisco Unified CM Administration**  
 For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ B

**Phone Configuration**

Save

**Status**

Status: Ready

**Phone Type**

**Product Type:** Third-party SIP Device (Basic)  
**Device Protocol:** SIP

**Device Information**

Device is not trusted

MAC Address*	00D05F01D32C	
Description	SEP00D05F01D32C	
Device Pool*	Default	<a href="#">View Details</a>
Common Device Configuration	< None >	<a href="#">View Details</a>
Phone Button Template*	Third-party SIP Device (Basic)	
Common Phone Profile*	Standard Common Phone Profile	<a href="#">View Details</a>
Calling Search Space	< None >	
AAR Calling Search Space	< None >	
Media Resource Group List	< None >	
Location*	Hub_None	
AAR Group	< None >	
Device Mobility Mode*	Default	
Owner	<input checked="" type="radio"/> User <input type="radio"/> Anonymous (Public/Shared Space)	
Owner User ID*	5000	
Use Trusted Relay Point*	Default	
Always Use Prime Line*	Default	
Always Use Prime Line for Voice Message*	Default	
Geolocation	< None >	

Ignore Presentation Indicators (internal calls only)  
 Logged Into Hunt Group  
 Remote Device

- 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 for configuring a phone. The page title is "Cisco Unified CM Administration" with the subtitle "For Cisco Unified Communications Solutions". A navigation menu at the top includes System, Call Routing, Media Resources, Advanced Features, Device, Application, and User Management. The main heading is "Phone Configuration".

Below the heading is a "Save" button. The configuration is organized into several sections:

- Number Presentation Transformation:**
  - Caller ID For Calls From This Phone:** Calling Party Transformation CSS is set to "< None >". The checkbox "Use Device Pool Calling Party Transformation CSS (Caller ID For Calls From This Phone)" is checked.
  - Remote Number:** Calling Party Transformation CSS is set to "< None >". The checkbox "Use Device Pool Calling Party Transformation CSS (Device Mobility Related Information)" is checked.
- Protocol Specific Information:**
  - BLF Presence Group\*: Standard Presence group
  - MTP Preferred Originating Codec\*: 711ulaw
  - Device Security Profile\*: Third-party SIP Device Basic - Standard SIP Non-Se
  - 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
  - Unattended Port
  - Require DTMF Reception
- MLPP and Confidential Access Level Information:**
  - MLPP Domain: < None >
  - Confidential Access Mode: < None >
  - Confidential Access Level: < None >

At the bottom of the form, there is another "Save" button.

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

8. Complete the following steps:

- Enter “Directory Number\*” (ex. 5000)
- Enter “Description” (ex. DoorSpeaker - VIP-172L)
- Check the Active checkbox, if not already checked
- Select “Presence Group\*” → “Standard Presence group” (or what is valid for your installation)

- E) Key in “Display (Caller ID)” with a name or number to identify this (DN) extension *\*useful with talkback speakers that can call into the Call Manager.*
- F) Enter “Maximum Number of Calls\*” → “2”
- G) Enter “Busy Trigger\*” → “2”
- H) Check “Caller Name”
- I) Check “Dialed Number”
- J) Select “Save” at the bottom or top of the screen
- K) Click “Apply Config” at top of screen

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

The screenshot displays the Cisco Unified CM Administration interface for configuring a SIP device. The main configuration area is titled "Phone Configuration" and includes a toolbar with "Save", "Delete", "Copy", "Reset", "Apply Config", and "Add New" buttons. The "Apply Config" button is highlighted, indicating the next step in the process.

**Phone Configuration Summary:**

- Phone Type:** Third-party SIP Device (Basic)
- Device Protocol:** SIP
- Real-time Device Status:**
  - Registration: Unknown
  - IPv4 Address: None
- Device Information:**
  - Device is Active:
  - Device is not trusted:
  - MAC Address\*: 00D05F01D32C
  - Description: SEP00D05F01D32C
  - Device Pool\*: Default
  - Common Device Configuration: < None >
  - Phone Button Template\*: Third-party SIP Device (Basic)
  - Common Phone Profile\*: Standard Common Phone Profile
  - Calling Search Space: < None >
  - AAR Calling Search Space: < None >
  - Media Resource Group List: < None >
  - Location\*: Hub\_None
  - AAR Group: < None >
  - Device Mobility Mode\*: Default
  - Owner:  User  Anonymous (Public/Shared Space)
  - Owner User ID\*: 5000
  - Use Trusted Relay Point\*: Default
  - Always Use Prime Line\*: Default
  - Always Use Prime Line for Voice Message\*: Default
  - Geolocation: < None >
  - Ignore Presentation Indicators (internal calls only):
  - Logged Into Hunt Group:

L) Click “Apply Config”

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

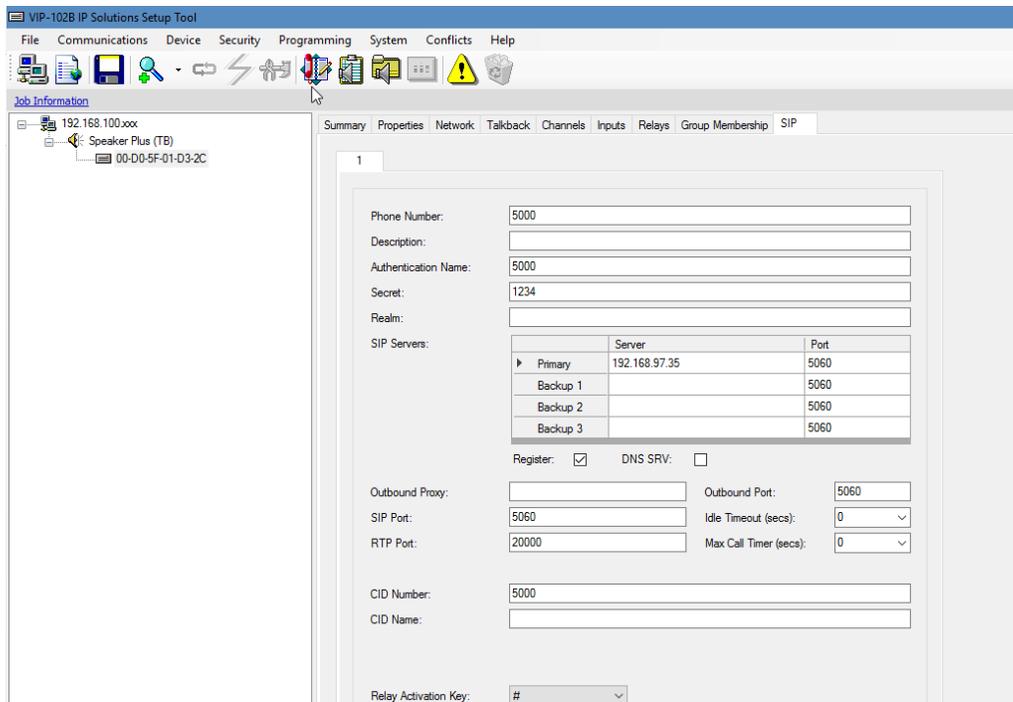
*Note: The information contained in this guide is limited to configuration of the “SIP” tab in the VIP-102B IP Solutions Setup Tool for the Valcom VIP device that is to be registered to the SIP server. More information on Valcom VIP device configuration, such as IP address assignment, relay activation,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

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

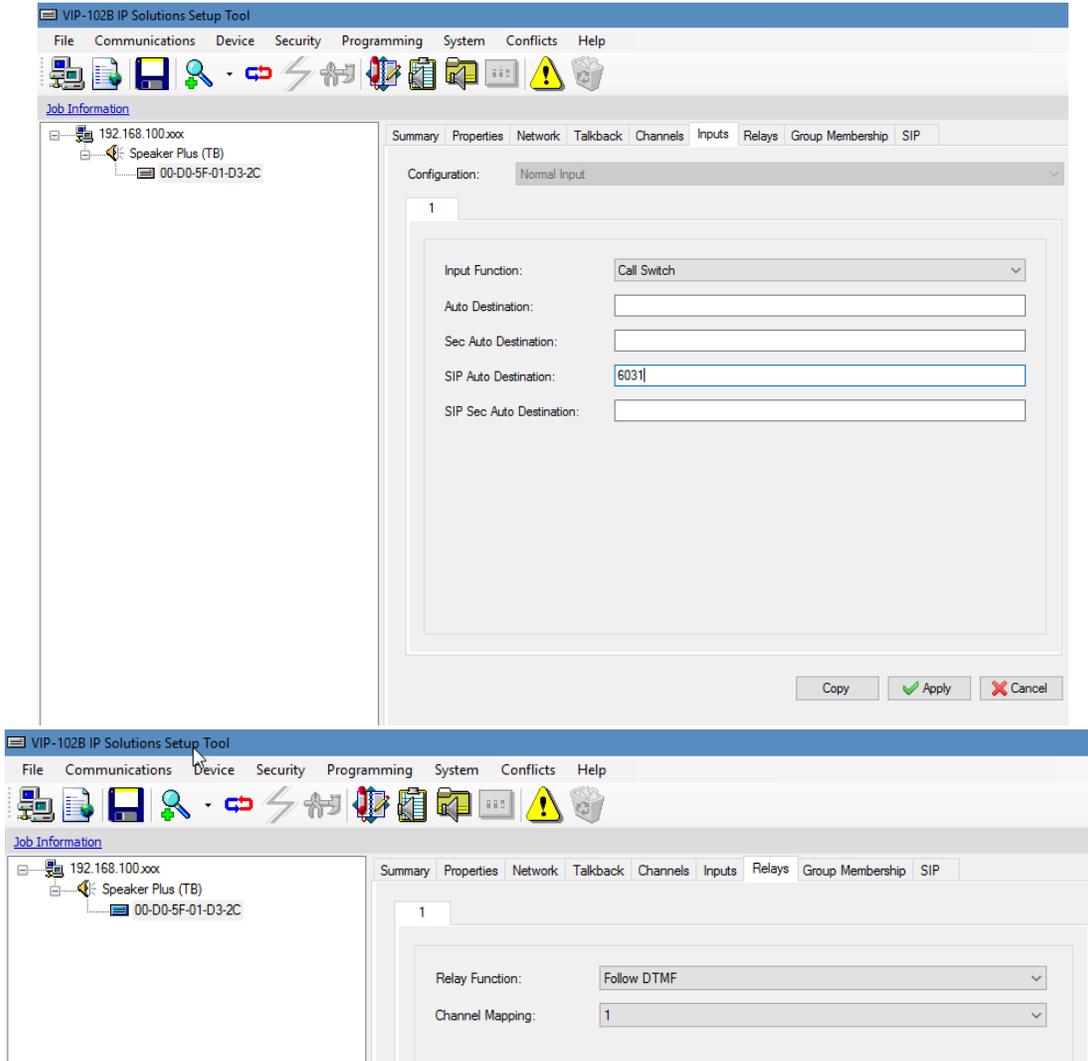
**Optional Fields:** Description, Realm, SIP Server Backup 1, 2, and 3, DNS SRV, CID Name, CID Number, Relay Activation Key applies to our example device. Other VIP devices may not show this field.

*In our example, the SIP Server IP address is the same as our Cisco Call Manager, “192.168.97.35”. 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 your server/site requirements.*

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.



On the Inputs tab make sure Call Switch is selected and the appropriate SIP extension to be dialed, when this device is activated by its call button, is entered in the SIP Auto Destination field. All other fields should be left blank. This may not apply for other devices that do not have an Input tab.



Also for this example only the relay is enabled by setting the Relay Function on the Relay tab to “Follow DTMF”. May not apply to other VIP devices.

10. 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”