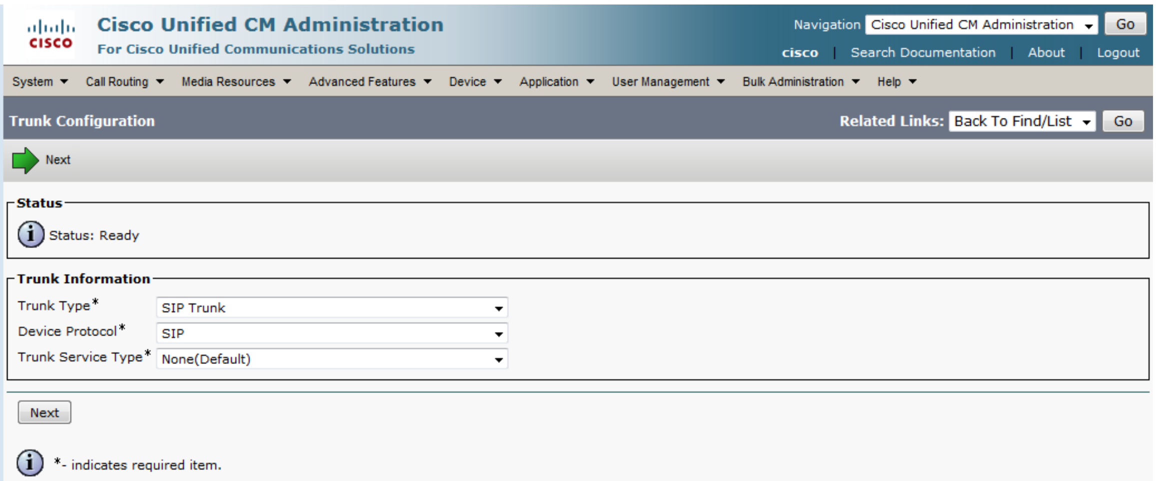
CUCM 11 - How to connect 2N® Helios IP via SIP trunk?

This FAQ describes how to connect 2N® Helios IP intercom to CUCM 11 via SIP trunk. Connection via SIP trunk will enable calls from intercom to CUCM and its main advantage is that you dont need additional "device" licence for CUCM. FAQ is diveded into the two parts. First part describes how to configure CUCM 11 and second part describes configuration of 2N® Helios IP intercom.

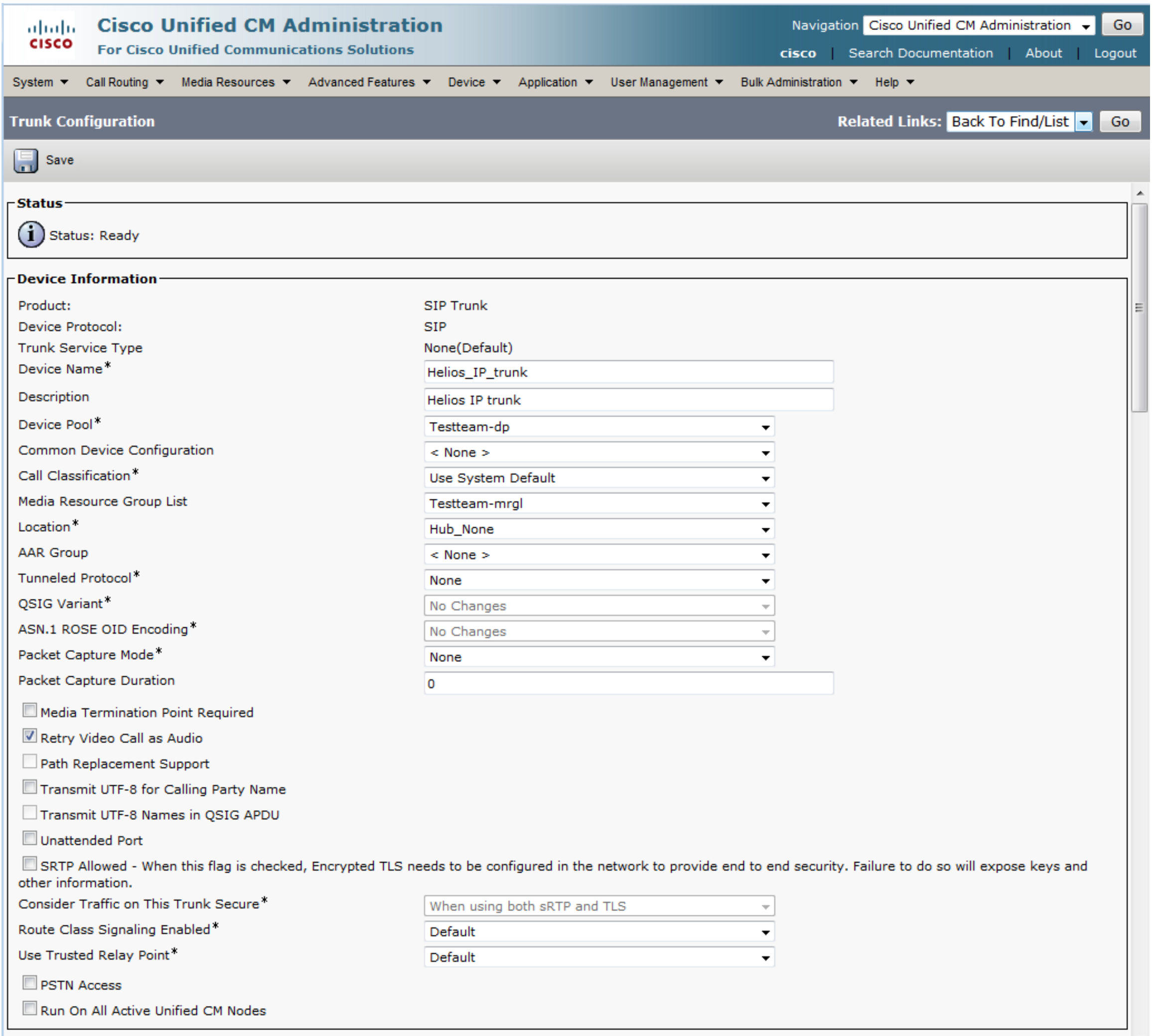
How to configure CUCM 11

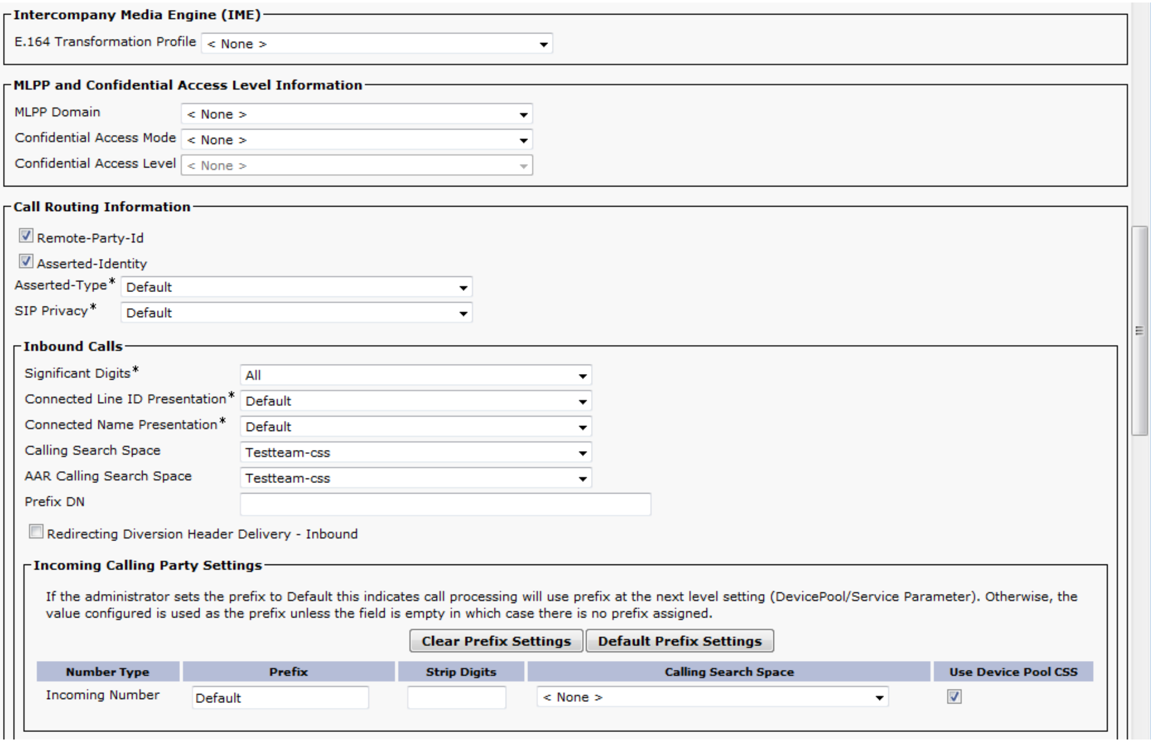
Configuration of SIP trunk

Go to section "Device->Trunk", set parameters regarding the picture below and click on "Next".



Continue in configuration according to the pictures below.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
cisco | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Trunk Configuration
Related Links: Back To Find/List Go
Save
Status
Status: Ready
Device Information
Product: SIP Trunk
Device Protocol: SIP
Trunk Service Type None(Default)
Device Name* Helios_IP_trunk
Description Helios IP trunk
Device Pool* Testteam-dp
Common Device Configuration < None >
Call Classification* Use System Default
Media Resource Group List Testteam-mrgl
Location* Hub_None
AAR Group < None >
Tunneled Protocol* None
QSIG Variant* No Changes
ASN.1 ROSE OID Encoding* No Changes
Packet Capture Mode* None
Packet Capture Duration 0
Media Termination Point Required
Retry Video Call as Audio
Path Replacement Support
Transmit UTF-8 for Calling Party Name
Transmit UTF-8 Names in QSIG APDU
Unattended Port
SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
Consider Traffic on This Trunk Secure* When using both sRTP and TLS
Route Class Signaling Enabled* Default
Use Trusted Relay Point* Default
PSTN Access
Run On All Active Unified CM Nodes



Intercompany Media Engine (IME)

E.164 Transformation Profile: < None >

MLPP and Confidential Access Level Information

MLPP Domain: < None >
Confidential Access Mode: < None >
Confidential Access Level: < None >

Call Routing Information

☑ Remote-Party-Id
☑ Asserted-Identity
Asserted-Type*: Default
SIP Privacy*: Default

Inbound Calls

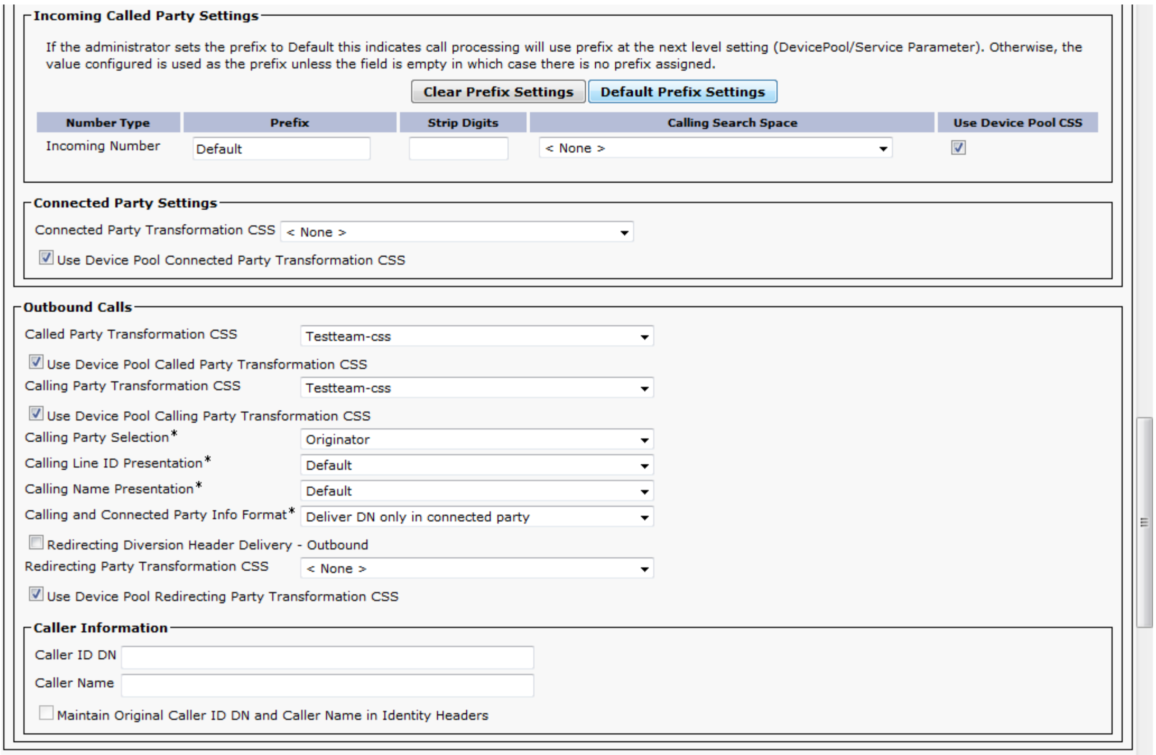
Significant Digits*: All
Connected Line ID Presentation*: Default
Connected Name Presentation*: Default
Calling Search Space: Testteam-css
AAR Calling Search Space: Testteam-css
Prefix DN:
☐ Redirecting Diversion Header Delivery - Inbound

Incoming Calling Party Settings

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Clear Prefix Settings | Default Prefix Settings

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	Default		< None >	☑



Incoming Called Party Settings

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Clear Prefix Settings | Default Prefix Settings

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	Default		< None >	☑

Connected Party Settings

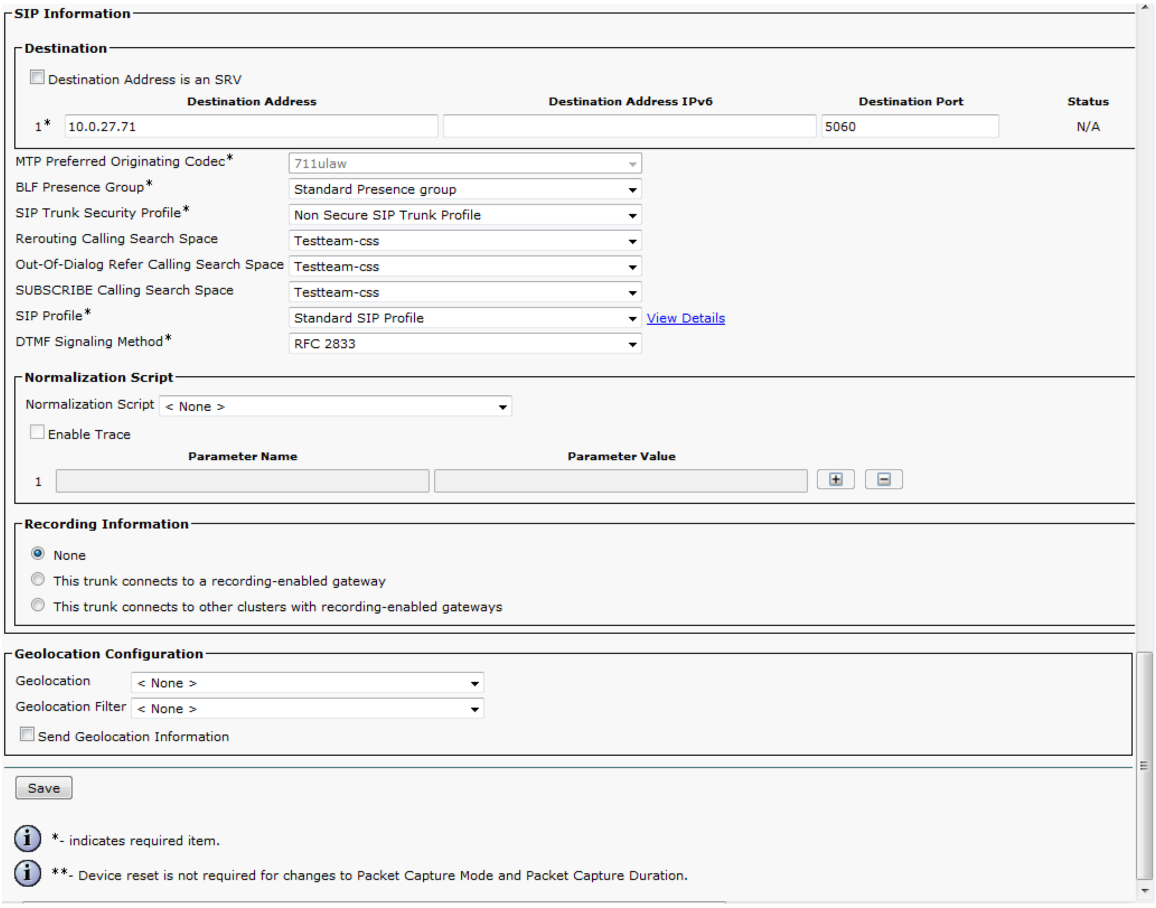
Connected Party Transformation CSS: < None >
☑ Use Device Pool Connected Party Transformation CSS

Outbound Calls

Called Party Transformation CSS: Testteam-css
☑ Use Device Pool Called Party Transformation CSS
Calling Party Transformation CSS: Testteam-css
☑ Use Device Pool Calling Party Transformation CSS
Calling Party Selection*: Originator
Calling Line ID Presentation*: Default
Calling Name Presentation*: Default
Calling and Connected Party Info Format*: Deliver DN only in connected party
☐ Redirecting Diversion Header Delivery - Outbound
Redirecting Party Transformation CSS: < None >
☑ Use Device Pool Redirecting Party Transformation CSS

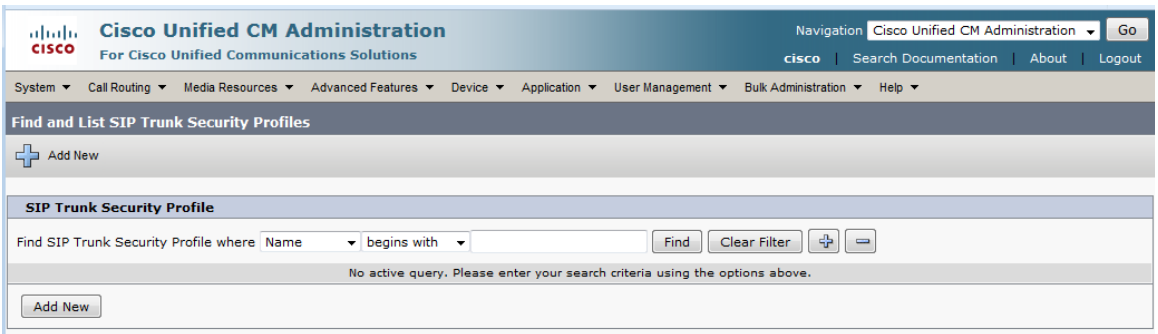
Caller Information

Caller ID DN:
Caller Name:
☐ Maintain Original Caller ID DN and Caller Name in Identity Headers

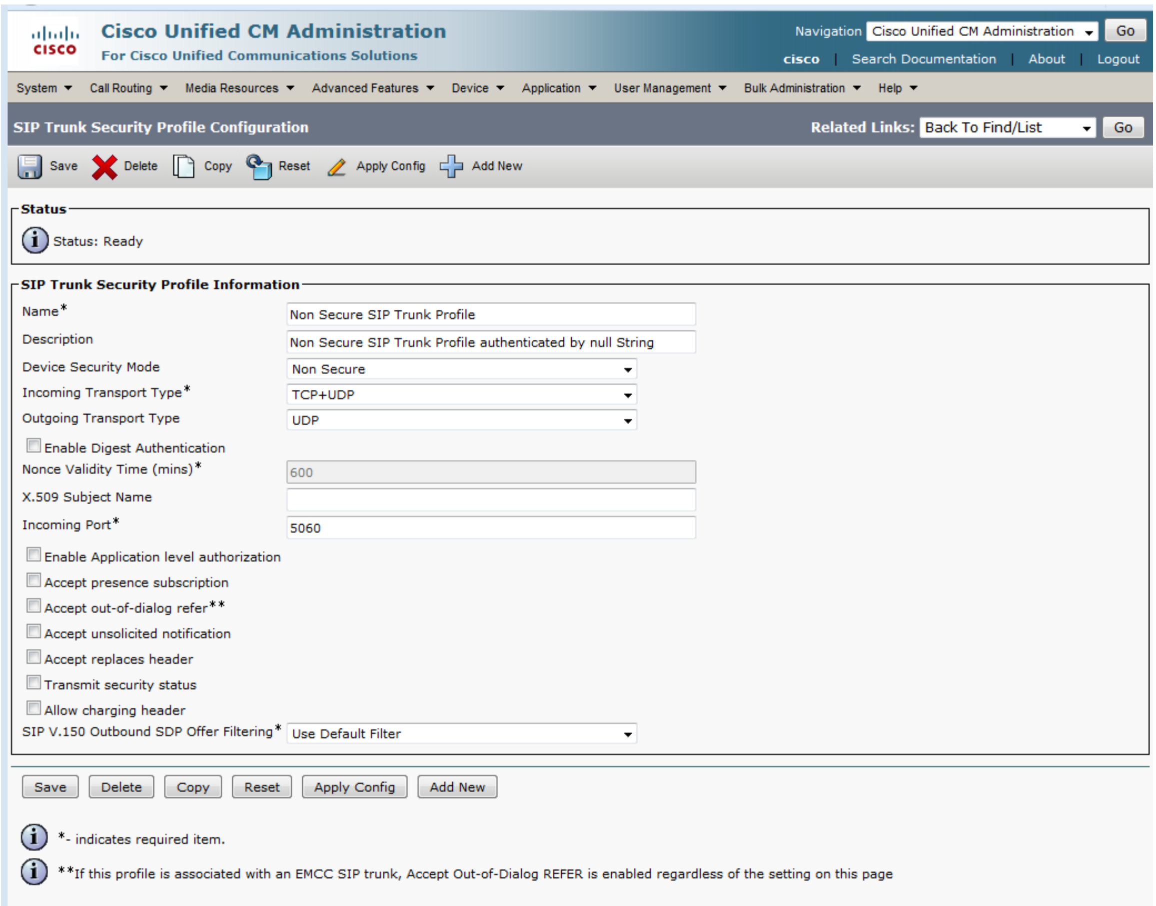


Configuratin of trunk security

In next step configure trunk security (password which will be used for registration to the trunk). Security is configured in section "System->Security->SIP Trunk Security Profile". Click on "Add New".

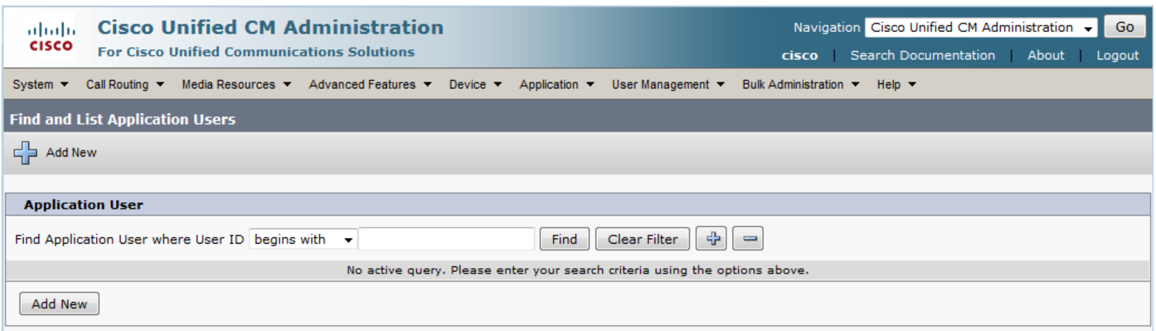


Configure the rest according to the pictures below.

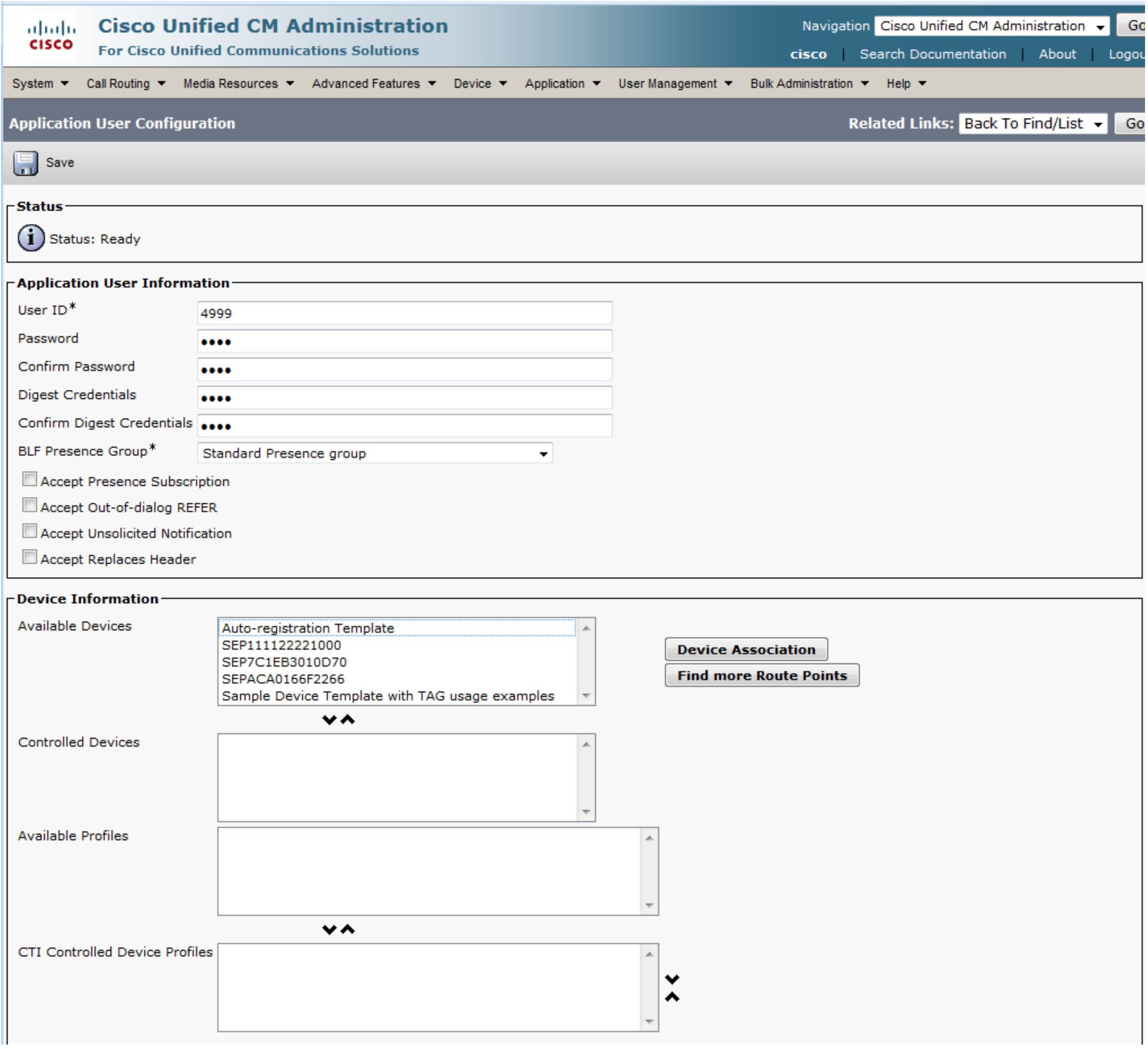


Add user

In this step add a user in section "User Management->Application User". Click on "Add New".

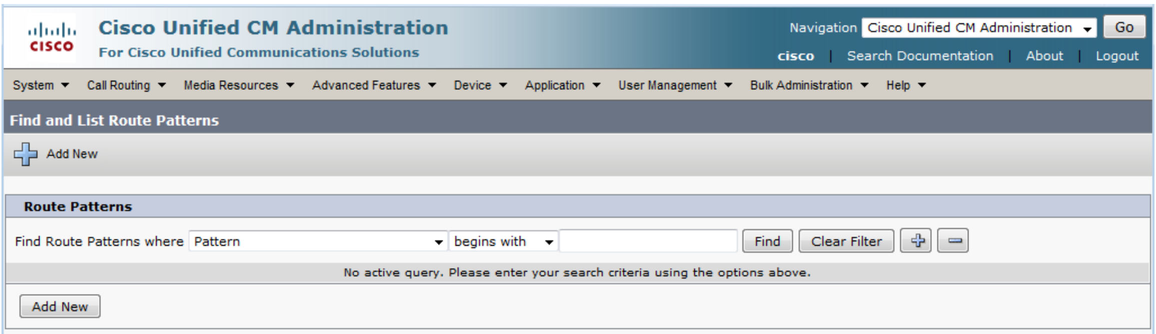


Continue with configuration according to pictures below.

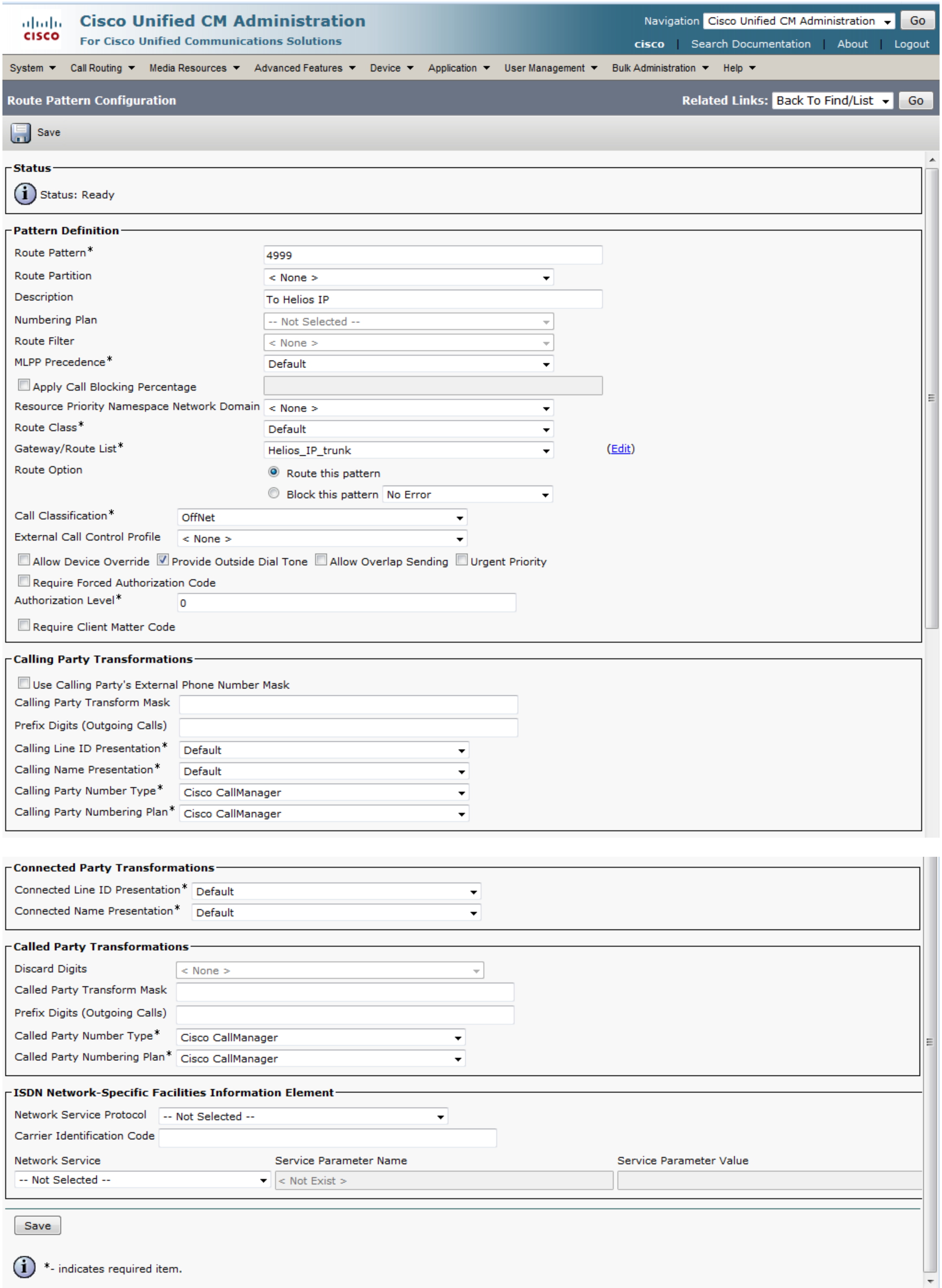


Add route pattern

In next step create route pattern (number which will be called by the intercom). Add Route pattern in section "Call Routing->Route->Hunt->Route Pattern". Click "Add New".



Continue with configuration according to pictures below.



How to configure 2N® Helios IP intercom

Now you can register the intercom to the newly created SIP trunk. Credentials for this example are 4999/4999 an d address of CUCM 11 is 10.0.27.36. Instead of this address fill here address of your CUCM.