AXIS SIP Setup and Troubleshooting Guide

Using AXIS SIP devices with different PBX server

Table of contents

Introduction

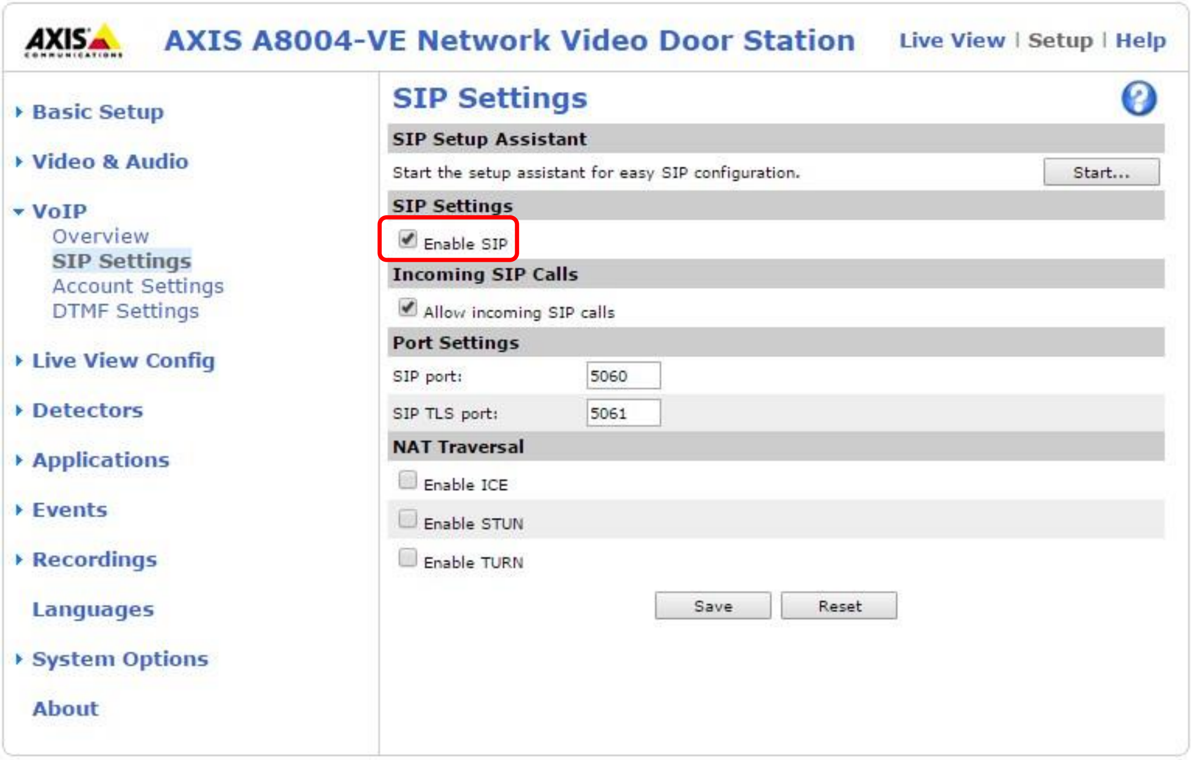
This guide aims to help users setup AXIS SIP products together with some commonly used PBX-servers. It explains how to setup an AXIS product to use a PBX-server as well as how to configure the PBX-server itself. Please note that since this guide shows how to setup 3rd party PBX-servers, future versions might vary in exact functionality and visual appearance. However, the workflow should roughly be the same.
Most of the commercial PBX manufactures are using licencing models that favours their own SIP devices therefore it is important that you have enough third party licences available to be able to register AXIS SIP devices with the PBX.

1 Preparing an AXIS SIP device to register with a PBX

Make sure to factory default your AXIS product before making the changes below. Also make sure that port 5060 (UDP and TCP) are not blocked within your network since these ports are most commonly used by the SIP protocol.

1.1 Enabling SIP

The first thing we need to do is to enable SIP-functionality in our AXIS product as shown below. Some AXIS products have a SIP Setup assistant that guides you through an easy setup for the entire product (like button-initiated calls on Network Video Door Station). This guide only shows how to set up an account in the AXIS product not the specific product capabilities. If a Setup Assistant is available, it’s recommended to be used. The same configuration specified below can be applied in the assistant separate pages.



SIP Settings

SIP Setup Assistant

Start the setup assistant for easy SIP configuration. Start...

SIP Settings

☑ Enable SIP

Incoming SIP Calls

☑ Allow incoming SIP calls

Port Settings

SIP port: 5060

SIP TLS port: 5061

NAT Traversal

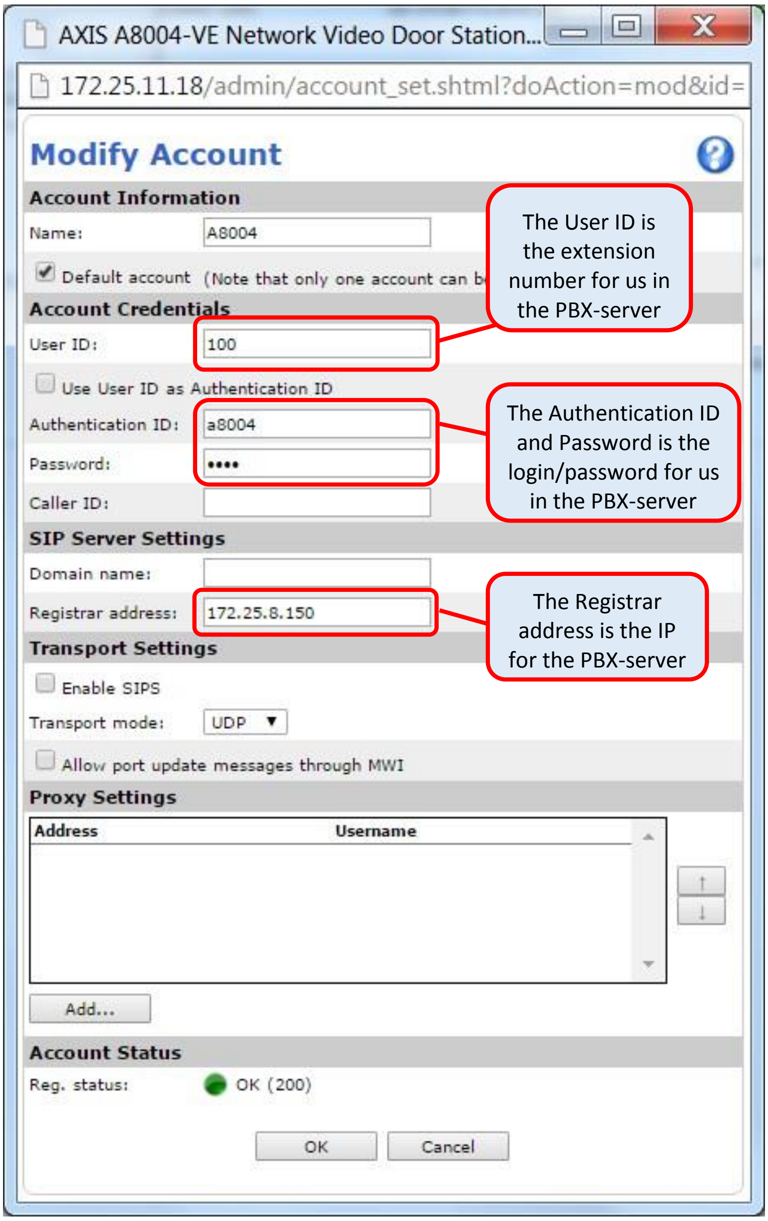
□ Enable ICE

□ Enable STUN

□ Enable TURN

1.2 Adding a SIP account

The next thing to do is to add the SIP account. Click on the **Add** button under **VoIP -> Account Settings** to bring up the screen below. The values used below are the same as in the CISCO Call manager.



AXIS A8004-VE Network Video Door Station...

172.25.11.18/admin/account_set.shtml?doAction=mod&id=

Modify Account

Account Information

Name: A8004

☑ Default account (Note that only one account can b

Account Credentials

User ID: 100

□ Use User ID as Authentication ID

Authentication ID: a8004

Password: ••••

Caller ID:

SIP Server Settings

Domain name:

Registrar address: 172.25.8.150

Transport Settings

□ Enable SIPS

Transport mode: UDP ▼

□ Allow port update messages through MWI

Proxy Settings

Address	Username

Add...

Account Status

Reg. status: ● OK (200)

OK Cancel

The User ID is the extension number for us in the PBX-server

The Authentication ID and Password is the login/password for us in the PBX-server

The Registrar address is the IP for the PBX-server

Under section 3.1 you can find an example how to setup a C3003-E

2 Configuring Cisco Unified Communications Manager

2.1 Introduction

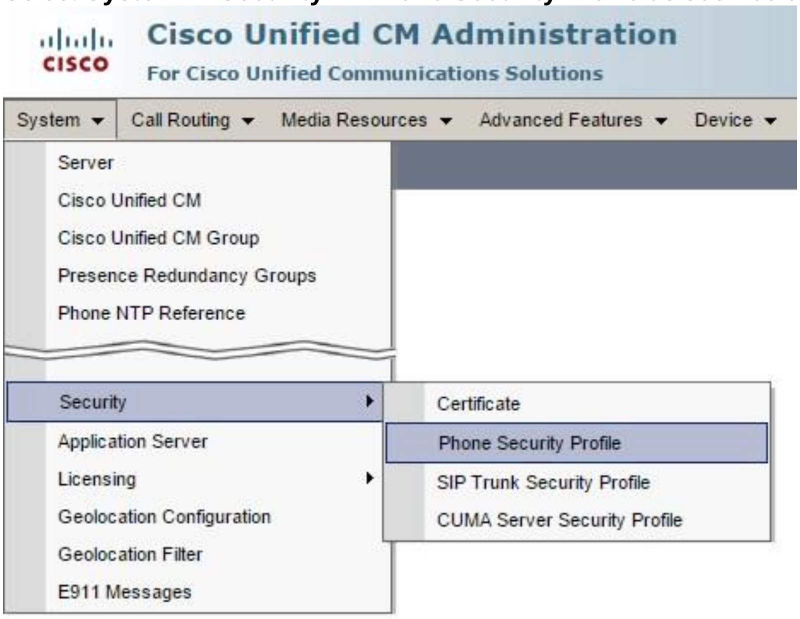
These instructions assume that you have already installed CUCM as your PBX-server. In this example, we are using version 10.5 of CUCM. Later versions should be similar to setup although the visual appearance might change. The required steps are listed below.

1. Create a single phone security profile to be used for all AXIS devices.
2. Create a user for each AXIS device.
3. Add device information to the CUCM manager.

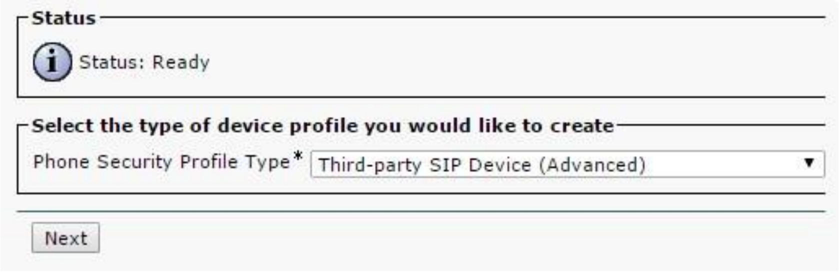
Please note that the steps described are for setting up basic functionality. There are many optional settings but they are not covered in this guide. Questions regarding the setup of Cisco PBX software should be directed to your Cisco integrator since it's not an AXIS product. You can give this guide to the Cisco Technician if he/she has questions on how the product should be configured.

2.2 Creating a Phone Security Profile

Select **System -> Security -> Phone Security** Profile as seen below.



Next click on the **Add New** button and then choose **Third-party SIP Device (Advanced)** and click on the **Next** button as seen below.



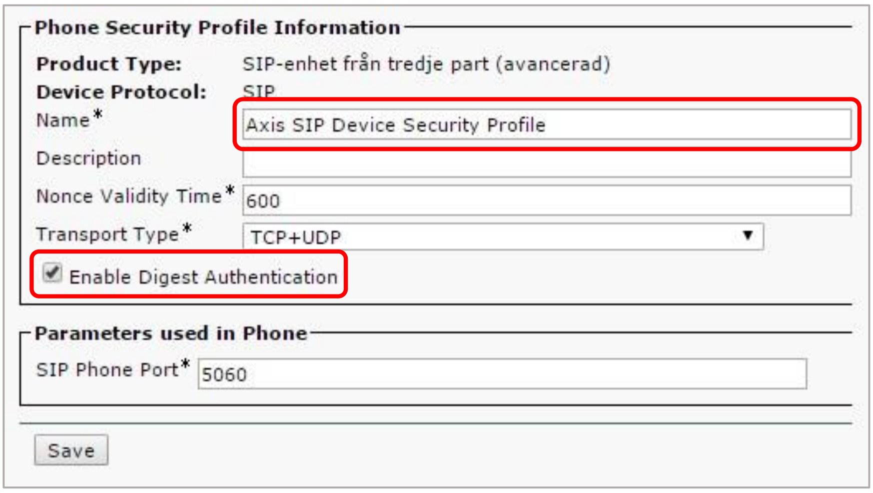
Status

Status: Ready

Select the type of device profile you would like to create

Phone Security Profile Type* Third-party SIP Device (Advanced)

Enter the name for the profile and make sure to check the digest authentication checkbox as seen below.



Phone Security Profile Information

Product Type: SIP-enhet från tredje part (avancerad)

Device Protocol: SIP

Name* Axis SIP Device Security Profile

Description

Nonce Validity Time* 600

Transport Type* TCP+UDP

☑ Enable Digest Authentication

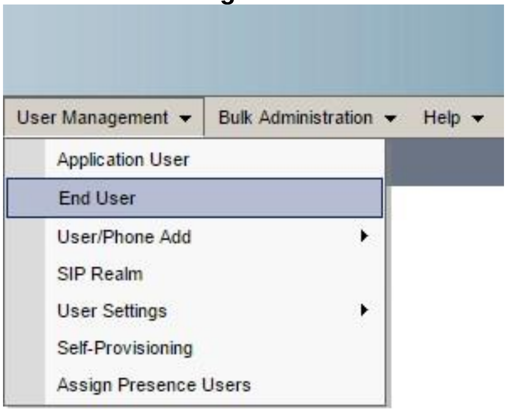
Parameters used in Phone

SIP Phone Port* 5060

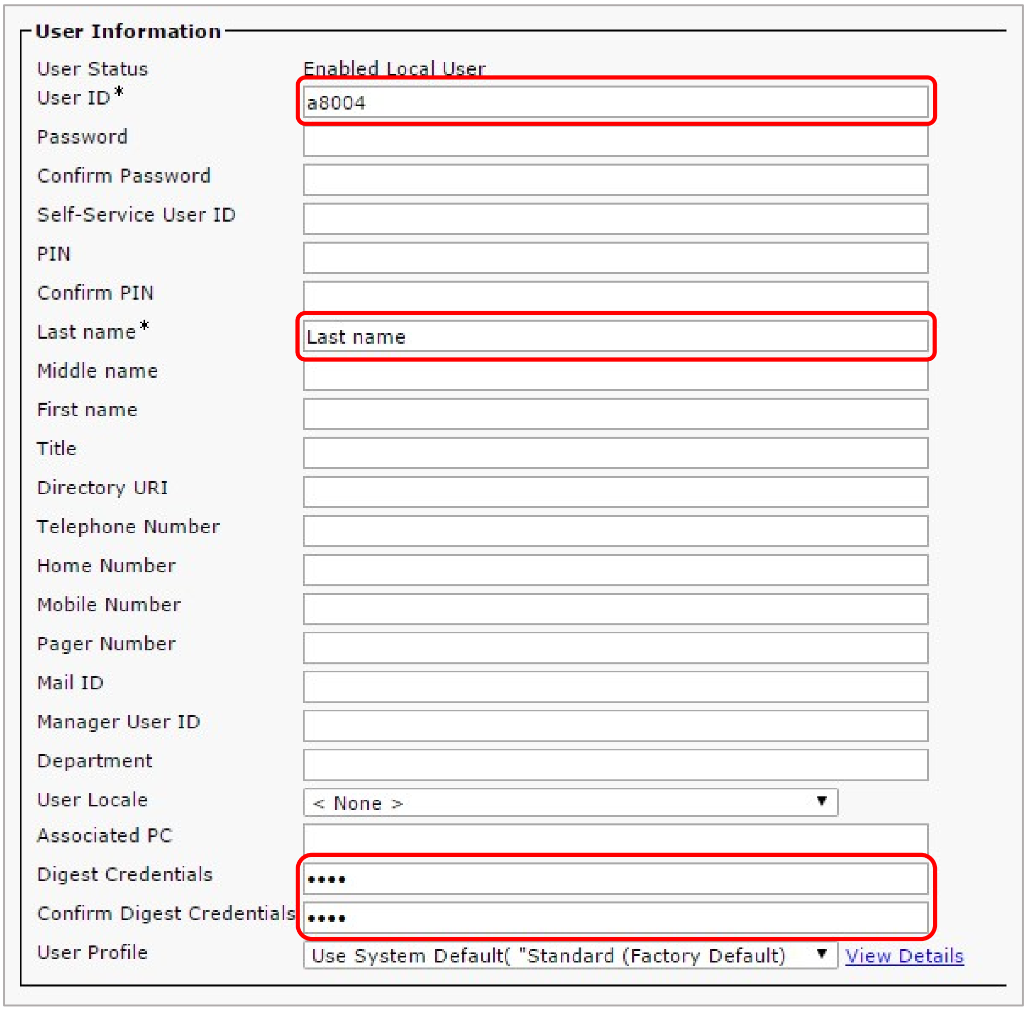
Finally click on the **Save** button.

2.3 Creating a user

Select **User Management -> End User** as seen below.



Next click on the **Add New** Button and enter the **User ID**, **Last name** and **Digest Credentials** as seen below. We do not need to enter anything under Password since we are using digest authentication instead.



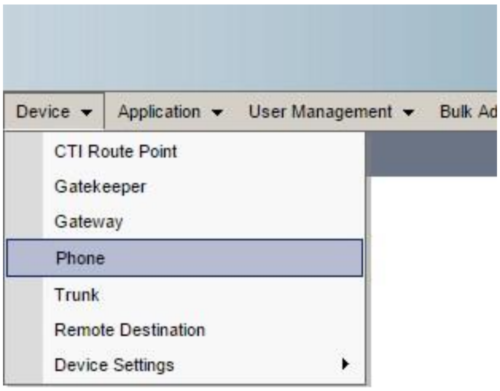
User Information

User Status	Enabled Local User
User ID*	a8004
Password	
Confirm Password	
Self-Service User ID	
PIN	
Confirm PIN	
Last name*	Last name
Middle name	
First 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	••••
Confirm Digest Credentials	••••
User Profile	Use System Default("Standard (Factory Default) View Details

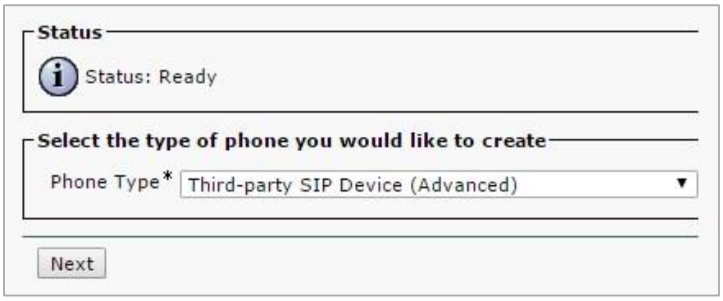
Finally click on the **Save** button.

2.4 Creating the device information

Select **Device->Phone** as seen below



Next click on the **Add New** button and then choose **Third-party SIP Device (Advanced)** and click on the **Next** button as seen below.



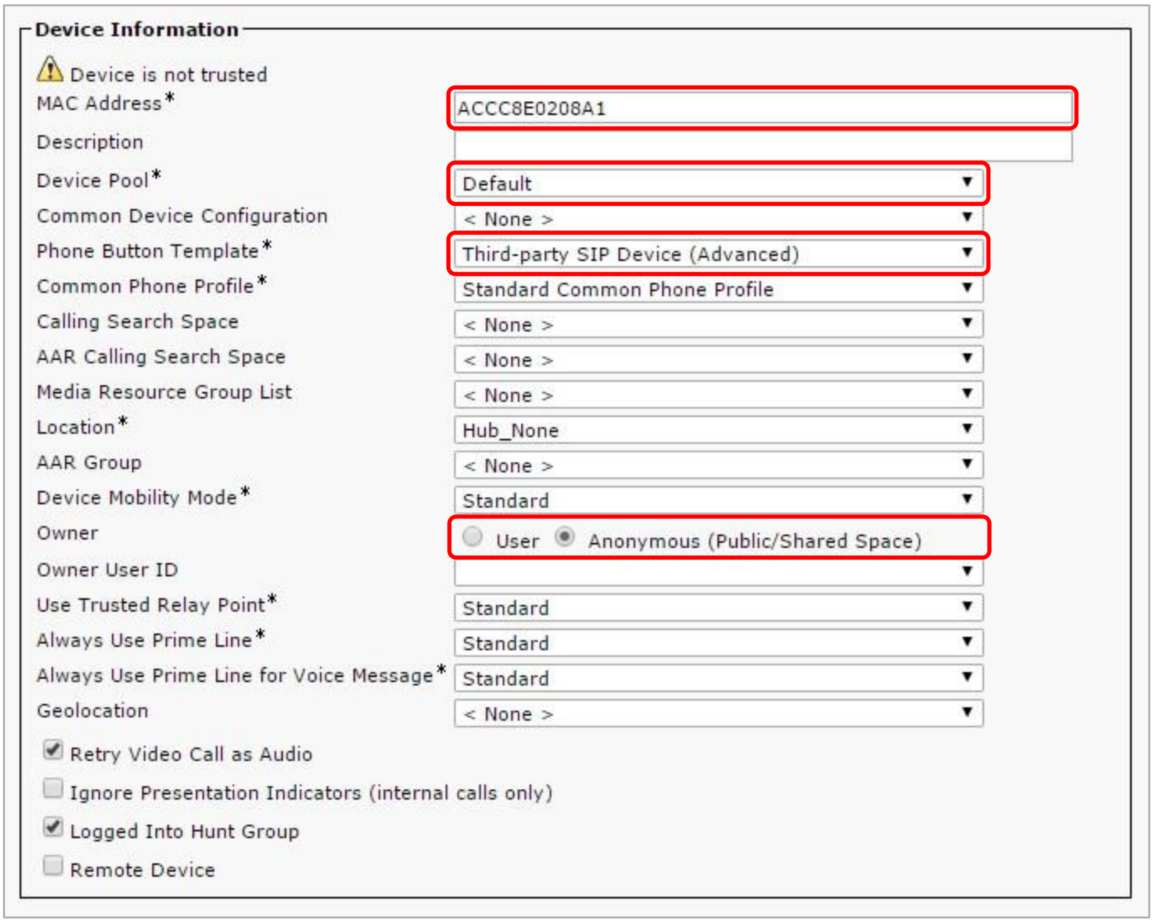
Status

Status: Ready

Select the type of phone you would like to create

Phone Type* Third-party SIP Device (Advanced)

Enter the **MAC Address** and set the **Device Pool** and **Phone Button Template** as seen below. You can also set the **Owner** to **Anonymous** as we are using digest authentication instead.



Device Information

Device is not trusted

MAC Address*	ACCC8E0208A1
Description	
Device Pool*	Default
Common Device Configuration	< None >
Phone Button Template*	Third-party SIP Device (Advanced)
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*	Standard
Owner	○ User ● Anonymous (Public/Shared Space)
Owner User ID	
Use Trusted Relay Point*	Standard
Always Use Prime Line*	Standard
Always Use Prime Line for Voice Message*	Standard
Geolocation	< None >

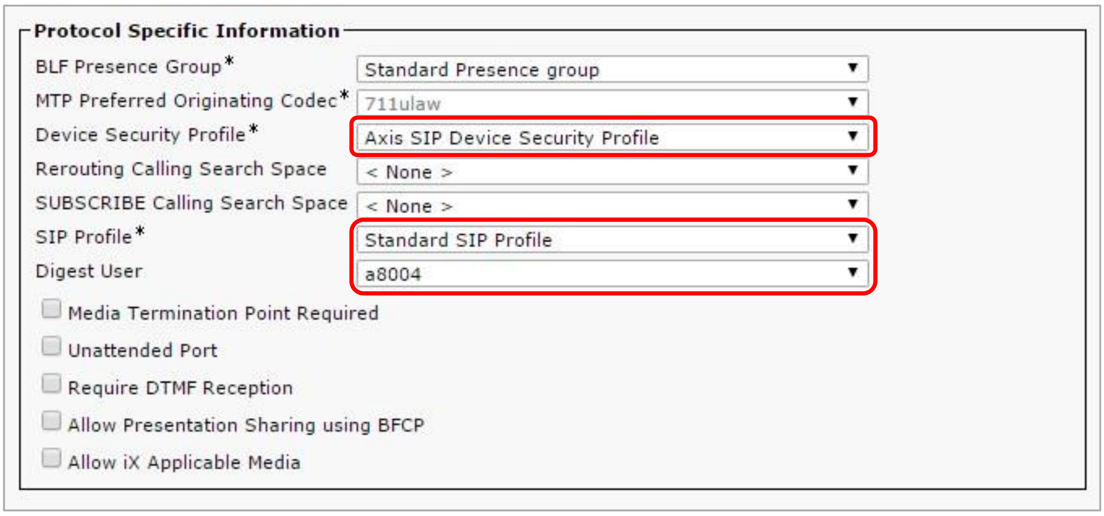
☑ Retry Video Call as Audio

☐ Ignore Presentation Indicators (internal calls only)

☑ Logged Into Hunt Group

☐ Remote Device

Then set the **Device Security Profile**, **SIP Profile** and **Digest User** as seen below.



Protocol Specific Information

BLF Presence Group*	Standard Presence group
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Axis SIP Device Security Profile
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile
Digest User	a8004

☐ Media Termination Point Required

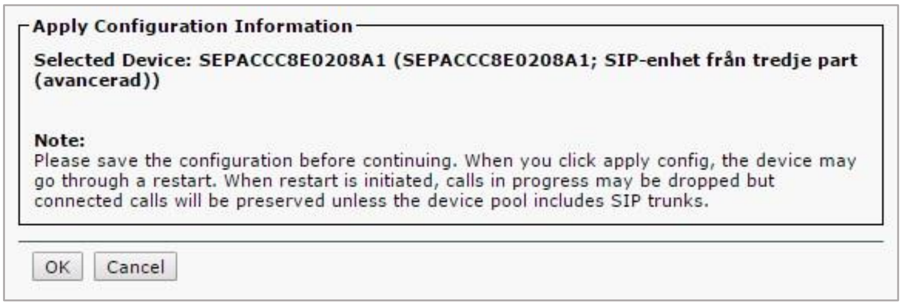
☐ Unattended Port

☐ Require DTMF Reception

☐ Allow Presentation Sharing using BFCP

☐ Allow iX Applicable Media

Click on the **Save** button and then click on the **Apply Configuration** button which displays the following window.

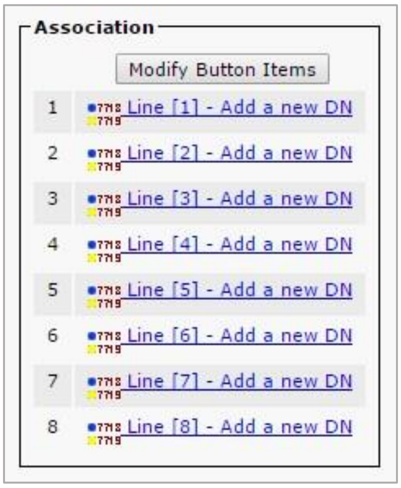


Apply Configuration Information

Selected Device: SEPACCC8E0208A1 (SEPACCC8E0208A1; SIP-enhet från tredje part (avancerad))

Note:
Please save the configuration before continuing. When you click apply config, the device may go through a restart. When restart is initiated, calls in progress may be dropped but connected calls will be preserved unless the device pool includes SIP trunks.

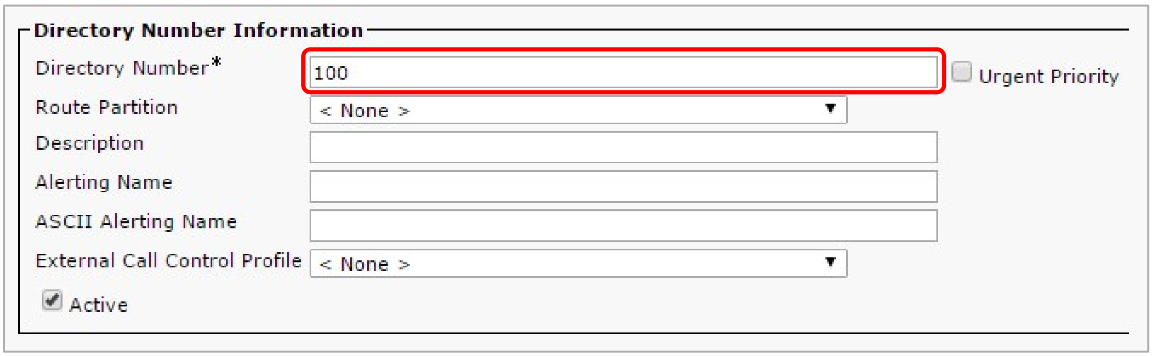
Click on the **OK** button and then click on the **Line [1] – Add a new DN** link to set the extension number for the device.



Association

1	Line [1] - Add a new DN
2	Line [2] - Add a new DN
3	Line [3] - Add a new DN
4	Line [4] - Add a new DN
5	Line [5] - Add a new DN
6	Line [6] - Add a new DN
7	Line [7] - Add a new DN
8	Line [8] - Add a new DN

Enter the **Directory Number** (extension number) as seen below.



Directory Number Information

Directory Number*	100	□ Urgent Priority
Route Partition	< None > ▼	
Description		
Alerting Name		
ASCII Alerting Name		
External Call Control Profile	< None > ▼	

☑ Active

Finally, click on the **Save** button and then you have completed the basic configuration of the AXIS SIP device.

2.5 Common causes of problems

If you are having problems getting the AXIS SIP device to register with the CUCM, go back to **Device → Phone** and click on the link to your SIP device and then click on the **Apply Config** button again. Some changes can take some time to apply.

If your PBX-server is not on your local network and you can’t connect to it, looking into using STUN, ICE or TURN is advisable.
STUN and ICE are explained in chapter 6.1

.

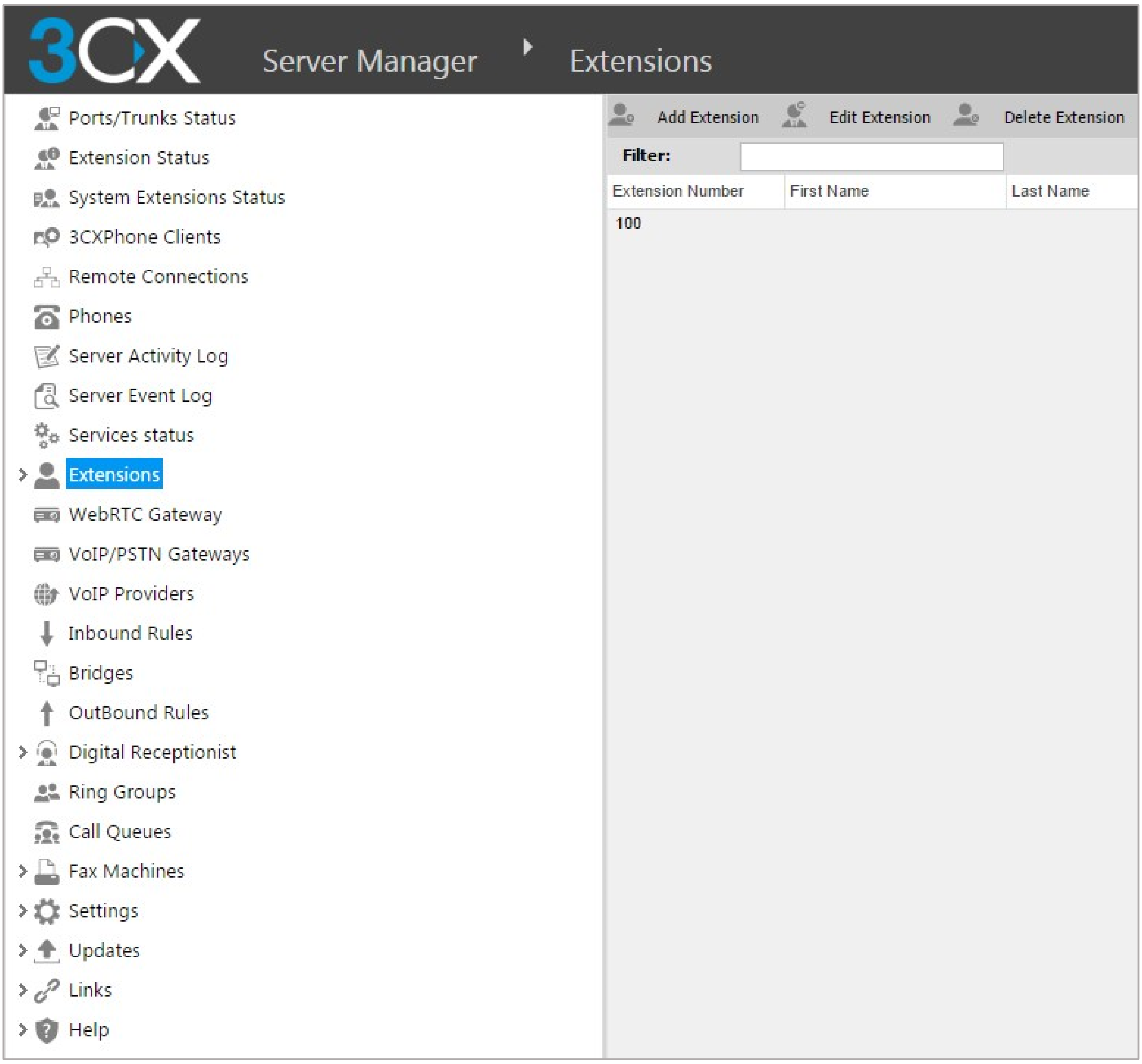
3 Configuring a 3CX Phone System

3.1 Introduction

These instructions assume that you have already installed the 3CX Phone System. In this example, we are using version 14.x of the 3CX Phone System. Later versions should be similar to setup although the visual appearance might change. Please note that the steps described are for setting up basic functionality. There are many optional settings but they are not covered in this guide. Questions regarding the setup of 3CX software should be directed to your local 3CX representative since it’s not an AXIS product.

3.2 Setting up extensions

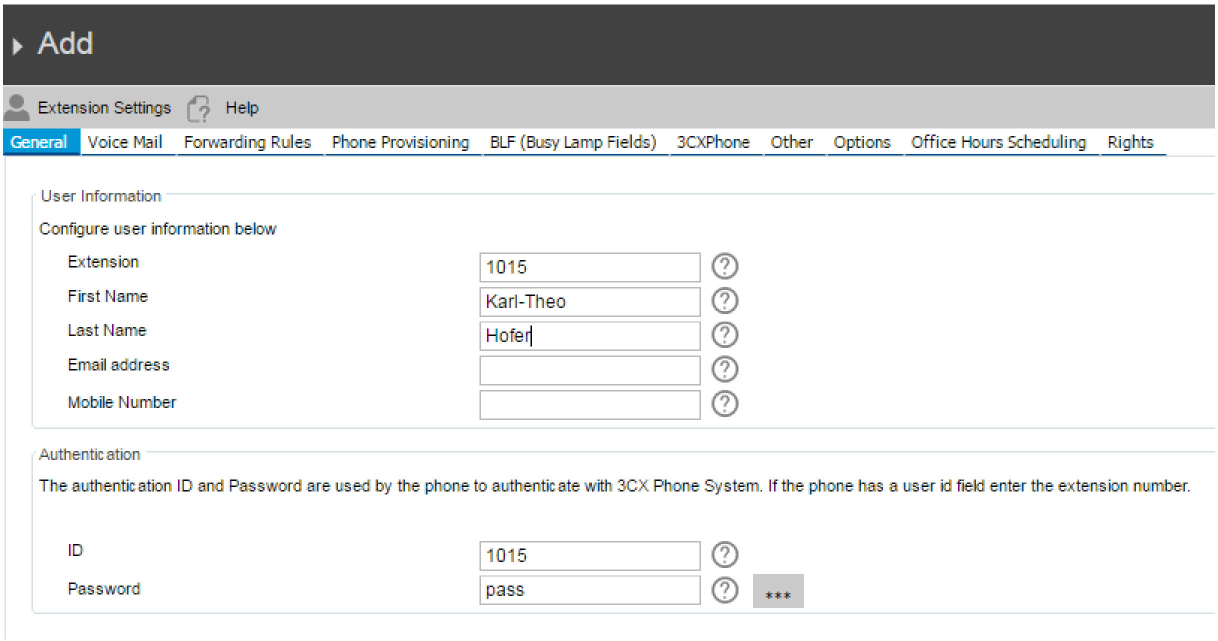
Open up a web browser and go to the IP-address where you installed your 3CX Phone System. This will open up the 3CX management interface. Enter your credentials (the default credentials are admin/admin) and you should see the following menu to the left.



Extension Number	First Name	Last Name
100		

In the screenshot above we can see all the extensions currently listed in the PBX-server. There is only the default “100” extension to start with.
We can now add all the extensions that we want to use. Name them appropriately and setup a password for each one.

Click on **Add Extension** to start adding an extension. Enter the specific **Extension Number** and then enter a suitable **First Name** and **Last Name**, as this is what is used as Caller ID. Finally enter your **ID** and **Password** which are the login details setup in the AXIS SIP device.



User Information

Configure user information below

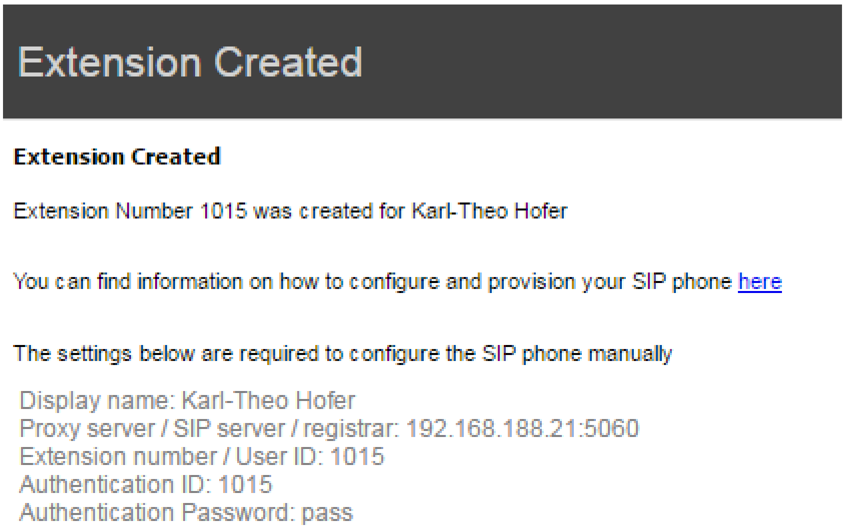
Extension	1015
First Name	Karl-Theo
Last Name	Hofer
Email address	
Mobile Number	

Authentication

The authentication ID and Password are used by the phone to authenticate with 3CX Phone System. If the phone has a user id field enter the extension number.

ID	1015
Password	pass

Finally click on the **OK** button to save and activate the changes.
After pressing the **OK** button a new view will give you the setup parameters you can use to configure the AXIS SIP device.



Extension Created

Extension Created

Extension Number 1015 was created for Karl-Theo Hofer

You can find information on how to configure and provision your SIP phone here

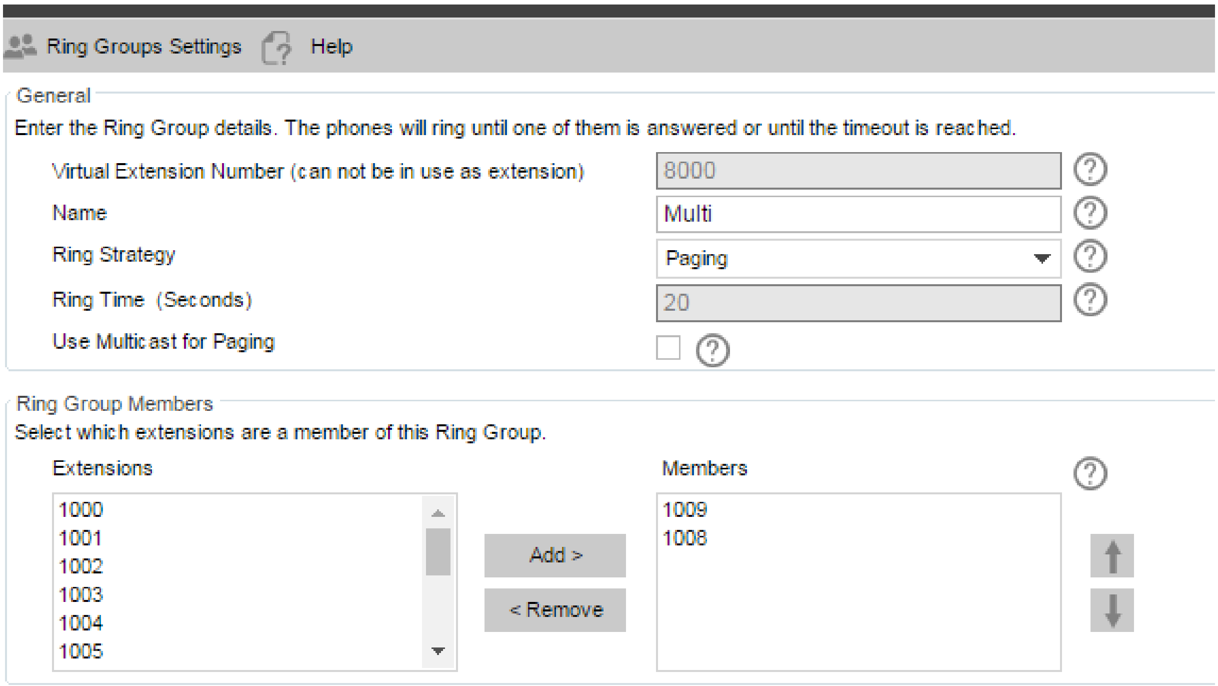
The settings below are required to configure the SIP phone manually

Display name: Karl-Theo Hofer
Proxy server / SIP server / registrar: 192.168.188.21:5060
Extension number / User ID: 1015
Authentication ID: 1015
Authentication Password: pass

3.3 Setting up paging

This can be useful to address and speak to several C3003-E at the same time.
To do so please create for every C3003-E its own extension please repeat step 3.2 as often as needed.

Click on **Ring Groups** →Add Ring Group



General

Enter the Ring Group details. The phones will ring until one of them is answered or until the timeout is reached.

Virtual Extension Number (can not be in use as extension)	8000
Name	Multi
Ring Strategy	Paging
Ring Time (Seconds)	20
Use Multicast for Paging	□

Ring Group Members

Select which extensions are a member of this Ring Group.

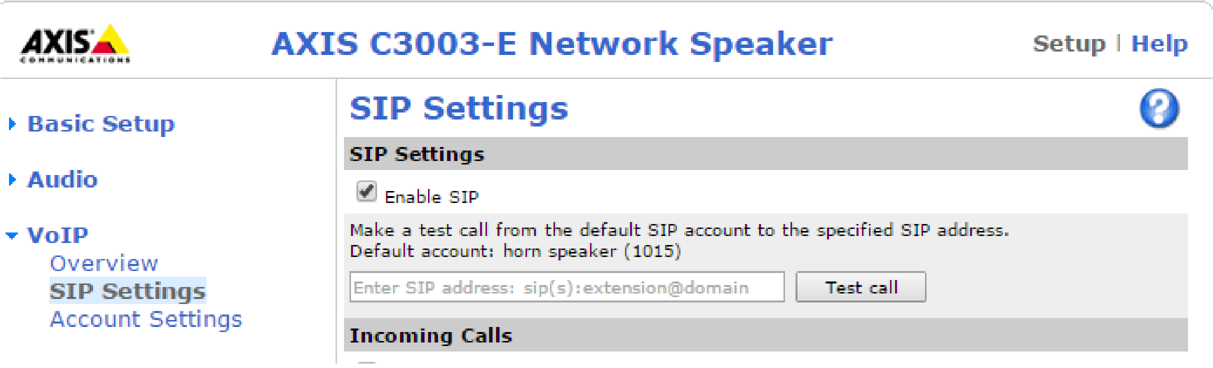
Extensions	Members
1000	1009
1001	1008
1002	
1003	
1004	
1005	

Choose Paging as Ring Strategy
Move the extension that shall be member of the Ring Group into the member section.
Press OK to safe the configuration.

If you now dial 8000 from one of the extensions the C3003-E will auto answer and you can transmit to all members at the same time.

3.4 Setting up the horn C3003-E

Go to Setup →VoIP→ SIP Settings check the Enable SIP checkbox



SIP Settings

SIP Settings

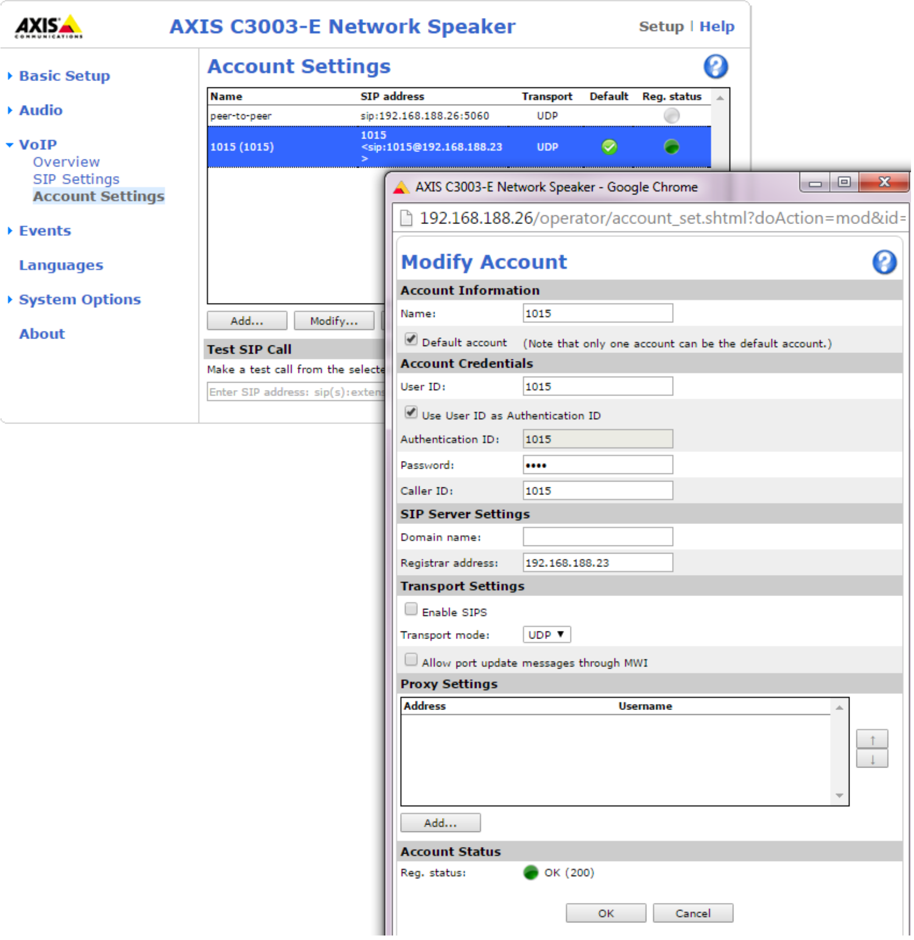
☑ Enable SIP

Make a test call from the default SIP account to the specified SIP address.
Default account: horn speaker (1015)

Enter SIP address: sip(s):extension@domain [Test call]

Incoming Calls

Then go to Setup →VoIP→ Account Settings click Add
And a new window opens called Add Account see screenshot below.



Account Settings

Name	SIP address	Transport	Default	Reg. status
peer-to-peer	sip:192.168.188.26:5060	UDP		○
1015 (1015)	1015 <sip:1015@192.168.188.23 >	UDP	✓	●

Test SIP Call

Make a test call from the selecte

Enter SIP address: sip(s):extens

192.168.188.26/operator/account_set.shtml?doAction=mod&id=

Modify Account

Account Information

Name: 1015

☑ Default account (Note that only one account can be the default account.)

Account Credentials

User ID: 1015

☑ Use User ID as Authentication ID

Authentication ID: 1015

Password: ••••

Caller ID: 1015

SIP Server Settings

Domain name:

Registrar address: 192.168.188.23

Transport Settings

☐ Enable SIPS

Transport mode: UDP ▼

☐ Allow port update messages through MWI

Proxy Settings

Address	Username

Add...

Account Status

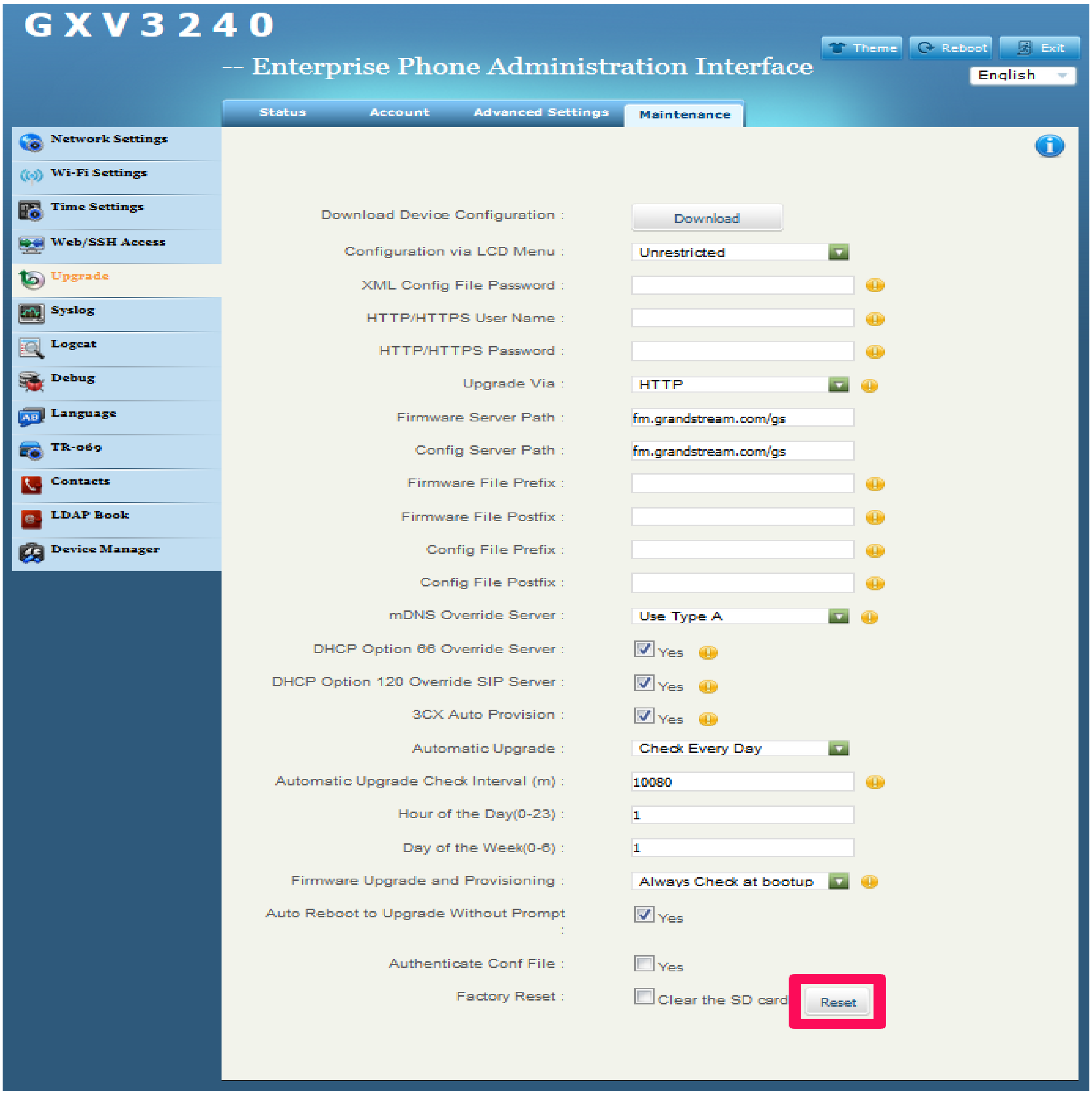
Reg. status: ● OK (200)

[OK] [Cancel]

Now the C3003 is registered with the3CX phone system and can call other extensions.

4 Peer to Peer call from GXV3240 IP phone to a A8004-VE

The easiest way to set up this IP phone is via web interface but you can also use phones touch screen to configure the device. All settings are done after factory reset which is available in the "Maintenance/Upgrade" section.



Download Device Configuration : Download

Configuration via LCD Menu : Unrestricted

XML Config File Password :

HTTP/HTTPS User Name :

HTTP/HTTPS Password :

Upgrade Via : HTTP

Firmware Server Path : fm.grandstream.com/gs

Config Server Path : fm.grandstream.com/gs

Firmware File Prefix :

Firmware File Postfix :

Config File Prefix :

Config File Postfix :

mDNS Override Server : Use Type A

DHCP Option 66 Override Server : ☑ Yes

DHCP Option 120 Override SIP Server : ☑ Yes

3CX Auto Provision : ☑ Yes

Automatic Upgrade : Check Every Day

Automatic Upgrade Check Interval (m) : 10080

Hour of the Day(0-23) : 1

Day of the Week(0-6) : 1

Firmware Upgrade and Provisioning : Always Check at bootup

Auto Reboot to Upgrade Without Prompt : ☑ Yes

Authenticate Conf File : □ Yes

Factory Reset : □ Clear the SD card Reset

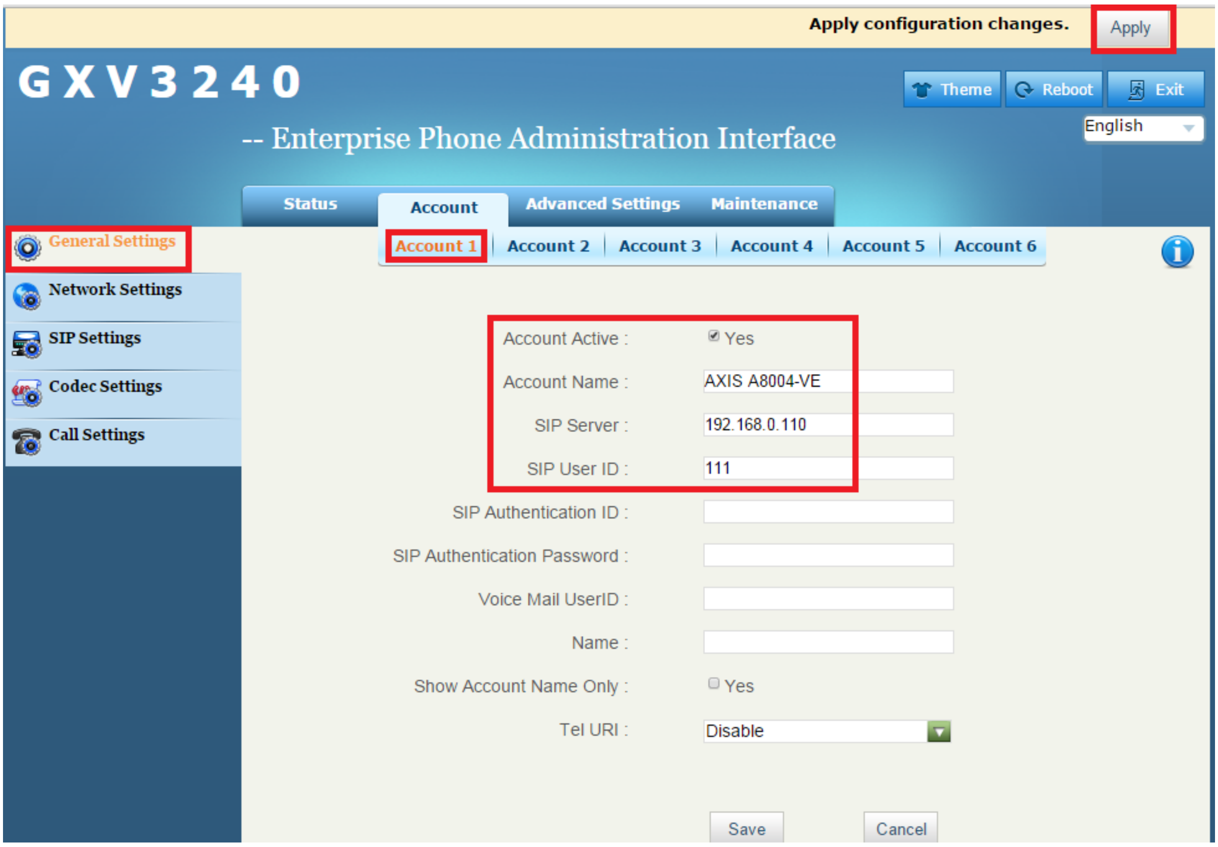
Login to the Grandstream GXV3240 via the web interface by using the IP address.

Username = admin
Password = admin

Enable "Account 1" and set all necessary information for this account in the "General Settings" section.

Account Active: check the box **Yes**
Account Name: **AXIS A8004-VE** *(this will appear on the screen of the phone)*
SIP Server: **enter the IP address of the A8004-VE**
SIP User ID: **111**
Click **Save** at the bottom
Click **Apply** to apply the configuration changes

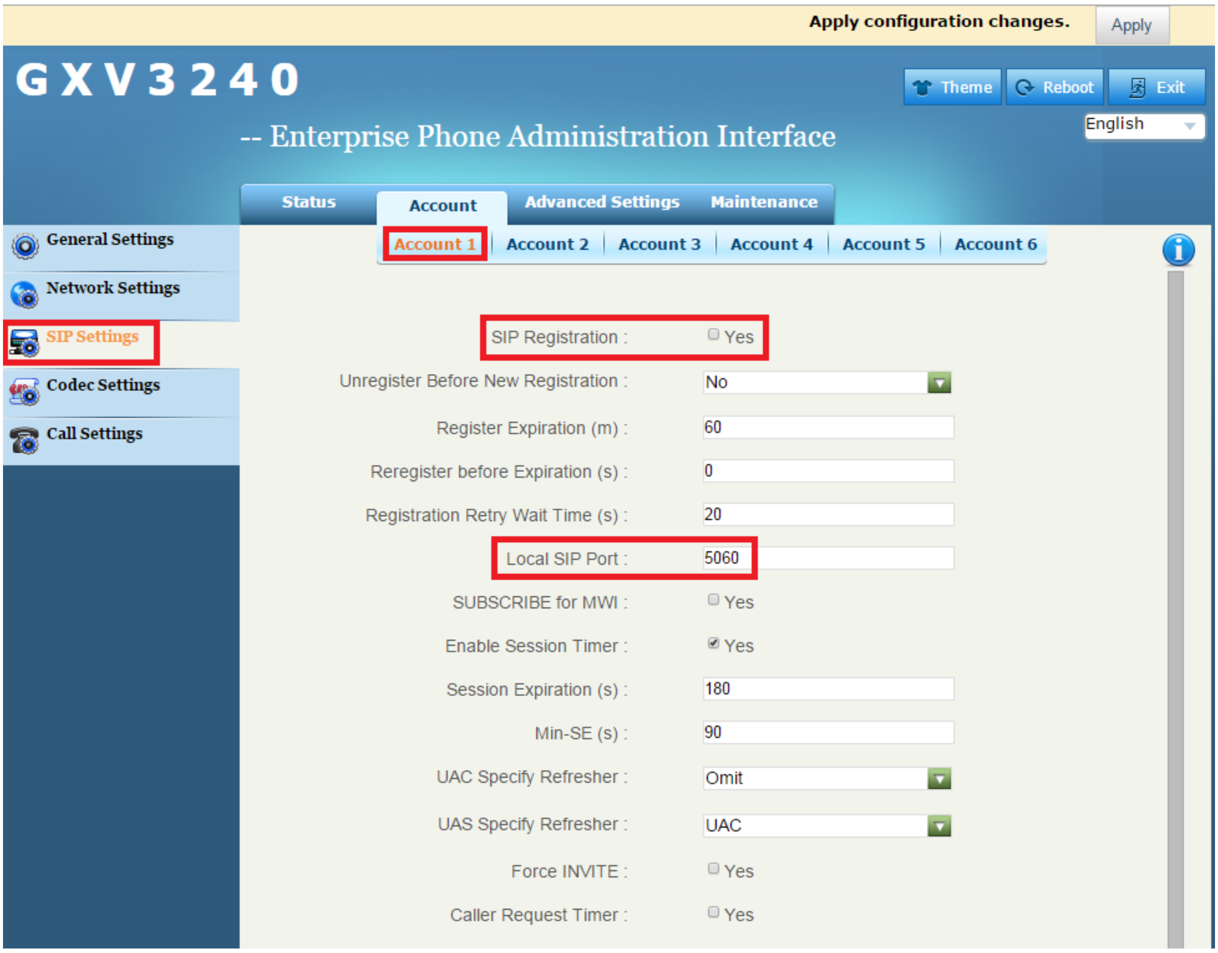
ATTENTION: the SIP user ID is the number you have to dial from your Grandstream in order to call the AXIS SIP device!!!



Account Active : ☑ Yes
Account Name : AXIS A8004-VE
SIP Server : 192.168.0.110
SIP User ID : 111
SIP Authentication ID :
SIP Authentication Password :
Voice Mail UserID :
Name :
Show Account Name Only : □ Yes
Tel URI : Disable

Go to the "SIP Settings" section and disable/uncheck the "SIP Registration" field

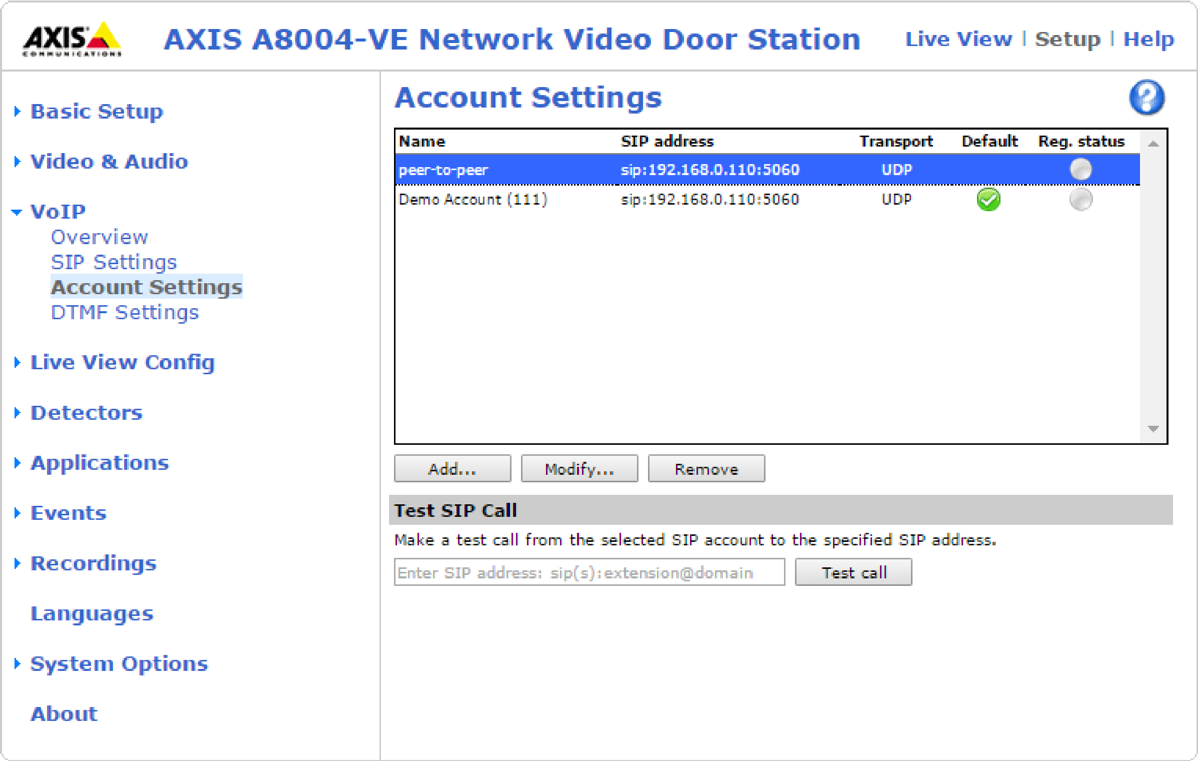
Verify that the **Local SIP Port** is set to **5060**
Click **Save** at the bottom
Click **Apply** to apply the configuration changes



SIP Registration : □ Yes
Unregister Before New Registration : No
Register Expiration (m) : 60
Reregister before Expiration (s) : 0
Registration Retry Wait Time (s) : 20
Local SIP Port : 5060
SUBSCRIBE for MWI : □ Yes
Enable Session Timer : ☑ Yes
Session Expiration (s) : 180
Min-SE (s) : 90
UAC Specify Refresher : Omit
UAS Specify Refresher : UAC
Force INVITE : □ Yes
Caller Request Timer : □ Yes

Navigate to VoIP > Account Settings. The account settings for the demo account that was created earlier in the A8004-VE will need to match the account settings added in the GXV3240.

Select the account and click on Modify. It should the account that is checked as default.



Account Settings

Name	SIP address	Transport	Default	Reg. status
peer-to-peer	sip:192.168.0.110:5060	UDP		○
Demo Account (111)	sip:192.168.0.110:5060	UDP	✓	○

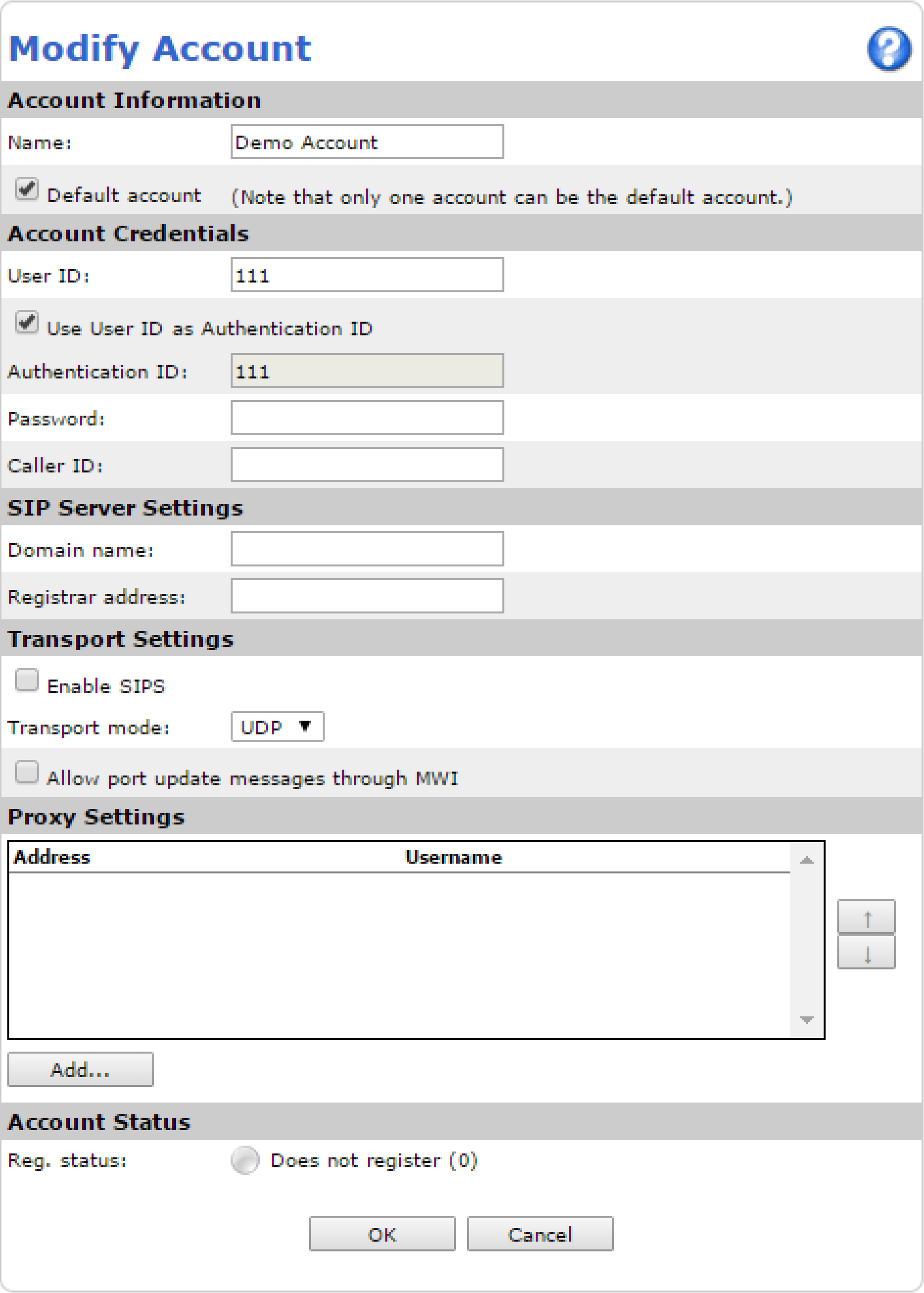
Test SIP Call

Make a test call from the selected SIP account to the specified SIP address.

Enter SIP address: sip(s):extension@domain

Name: no need to change it

User ID: **111** *(this should match the user ID added in the GXV3240 account)*
Password: should remain blank *(unless you added a password in the GXV3240 account)*
Click OK



Modify Account

Account Information

Name: Demo Account

☑ Default account (Note that only one account can be the default account.)

Account Credentials

User ID: 111

☑ Use User ID as Authentication ID

Authentication ID: 111

Password:

Caller ID:

SIP Server Settings

Domain name:

Registrar address:

Transport Settings

☐ Enable SIPS

Transport mode: UDP ▼

☐ Allow port update messages through MWI

Proxy Settings

Address	Username

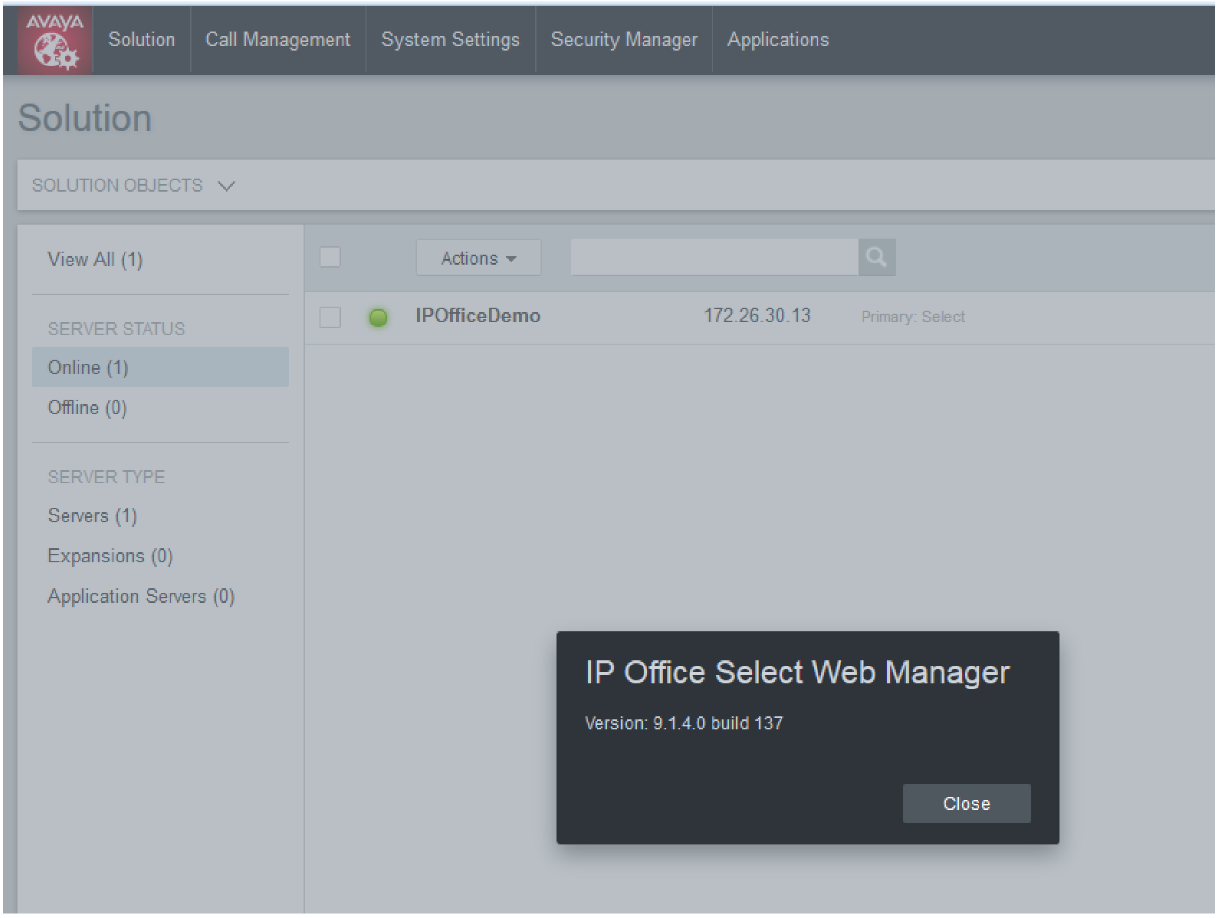
Account Status

Reg. status: ○ Does not register (0)

If you now dial 111 from your Grandstream the A8004-VE should take the call.

5 Configuring the Avaya Office Manager Vers. 9.1.4.0

To be able to use the system you have to create a user and an extension.



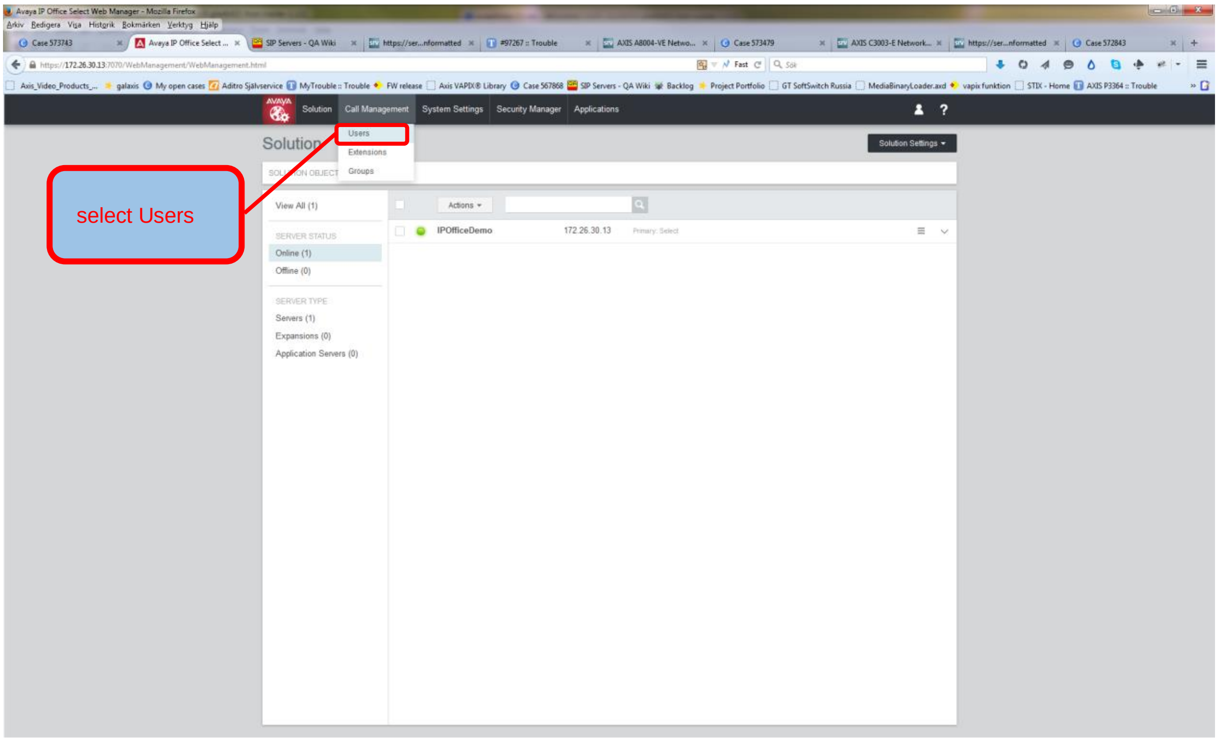
IPOfficeDemo 172.26.30.13 Primary: Select

IP Office Select Web Manager

Version: 9.1.4.0 build 137

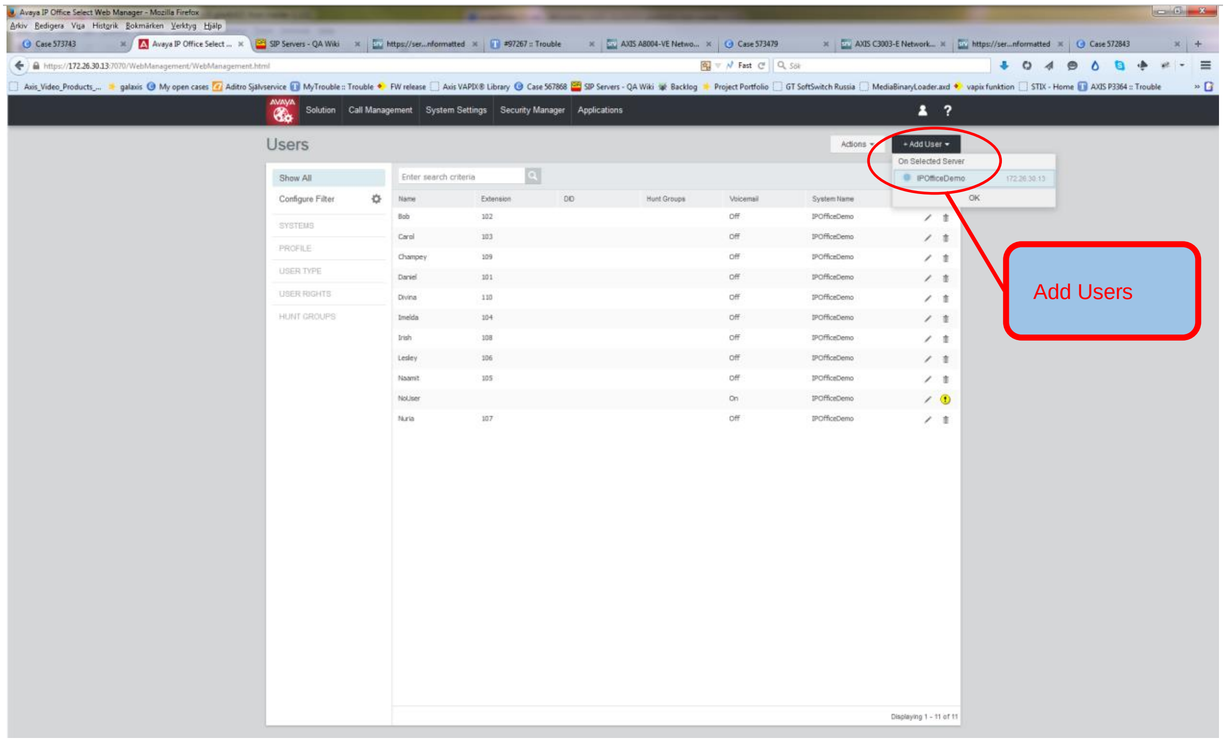
First you have to create a user

Go to Call Management → Users



select Users

In the new view click Add Users choose the server instance you like to create the user on



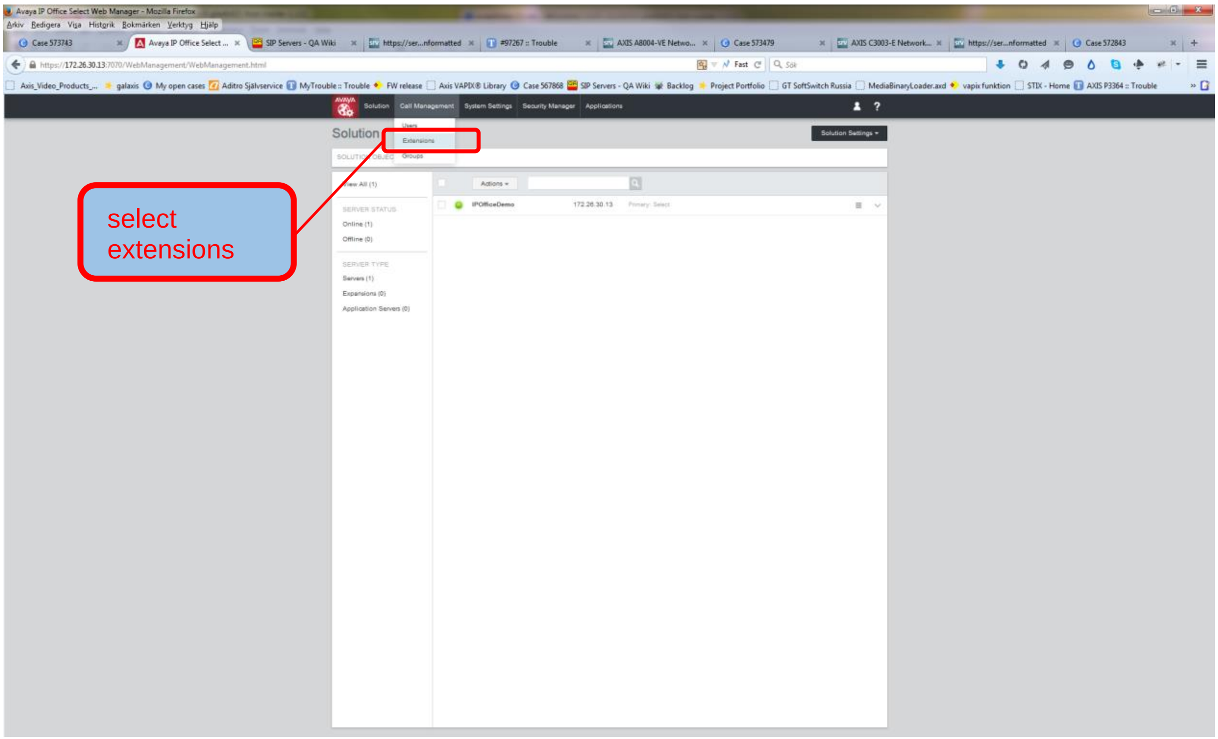
Users

Name	Extension	DID	Hunt Groups	Voicemail	System Name
Bob	102			Off	IPOfficeDemo
Carol	103			Off	IPOfficeDemo
Champey	109			Off	IPOfficeDemo
Daniel	101			Off	IPOfficeDemo
Divina	110			Off	IPOfficeDemo
Imelda	104			Off	IPOfficeDemo
Irish	108			Off	IPOfficeDemo
Lesley	106			Off	IPOfficeDemo
Naamit	105			Off	IPOfficeDemo
NoUser				On	IPOfficeDemo
Nuria	107			Off	IPOfficeDemo

Add Users

Second step:
You have to create an extension

Go to Call Management → Extensions

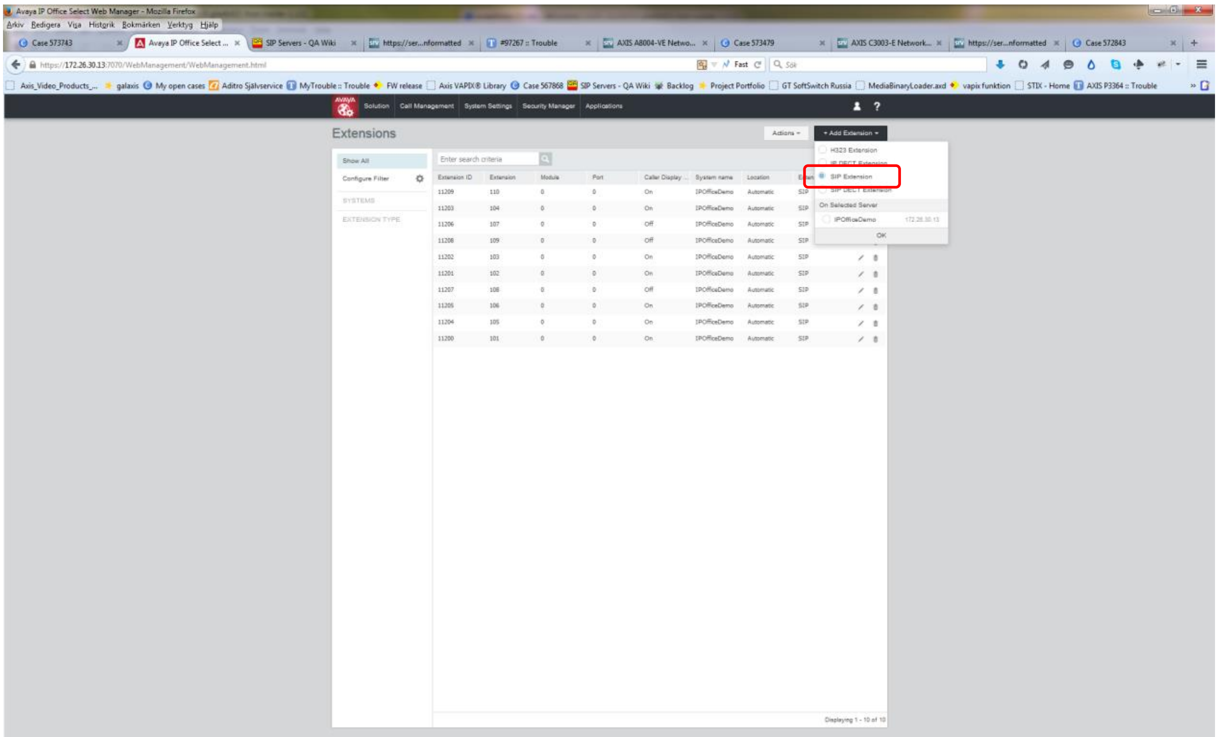


Solution

IPOfficeDemo 172.26.30.13 Primary: Select

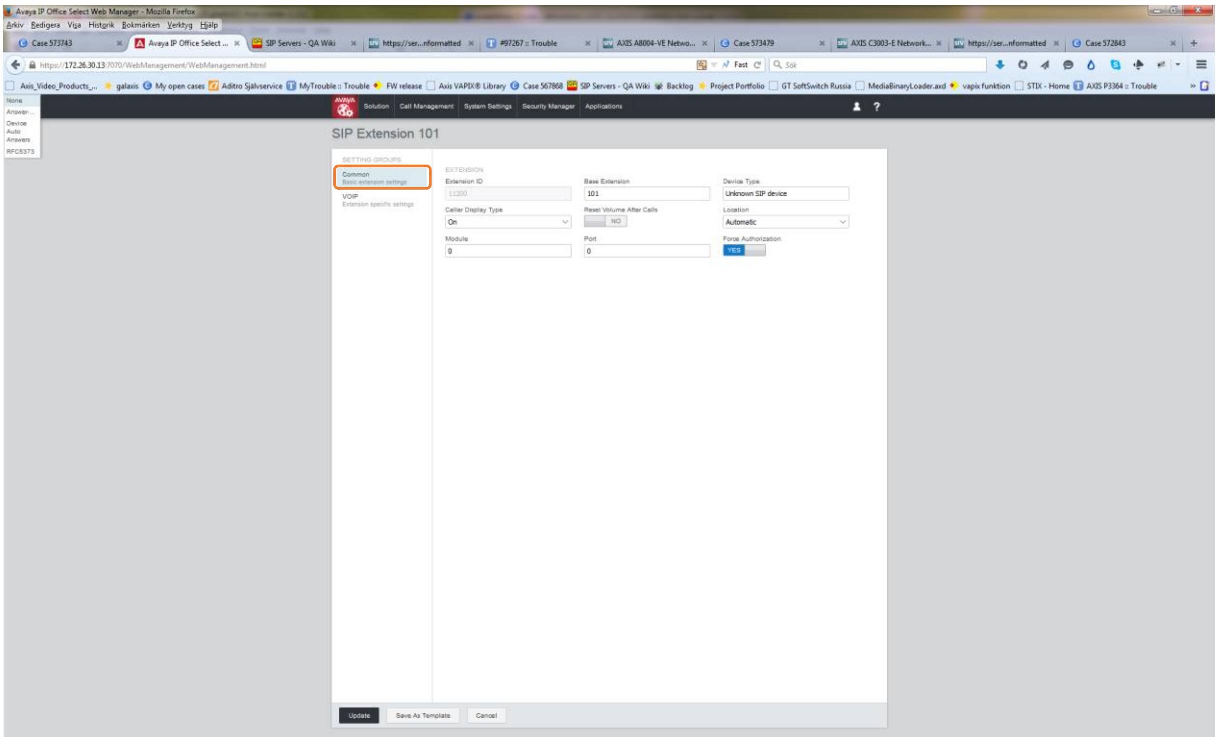
select extensions

In the new view click Add Extensions choose the server instance you like to create the user on



Extension ID	Extension	Module	Port	Caller Display ...	System name	Location	E
11209	110	0	0	On	IPOfficeDemo	Automatic	SIP
11203	104	0	0	On	IPOfficeDemo	Automatic	SIP
11206	107	0	0	Off	IPOfficeDemo	Automatic	SIP
11208	109	0	0	Off	IPOfficeDemo	Automatic	SIP
11202	103	0	0	On	IPOfficeDemo	Automatic	SIP
11201	102	0	0	On	IPOfficeDemo	Automatic	SIP
11207	108	0	0	Off	IPOfficeDemo	Automatic	SIP
11205	106	0	0	On	IPOfficeDemo	Automatic	SIP
11204	105	0	0	On	IPOfficeDemo	Automatic	SIP
11200	101	0	0	On	IPOfficeDemo	Automatic	SIP

Please choose “Common” and configure the extension and press update



Extension ID: 11200

Base Extension: 101

Device Type: Unknown SIP device

Caller Display Type: On

Reset Volume After Calls: NO

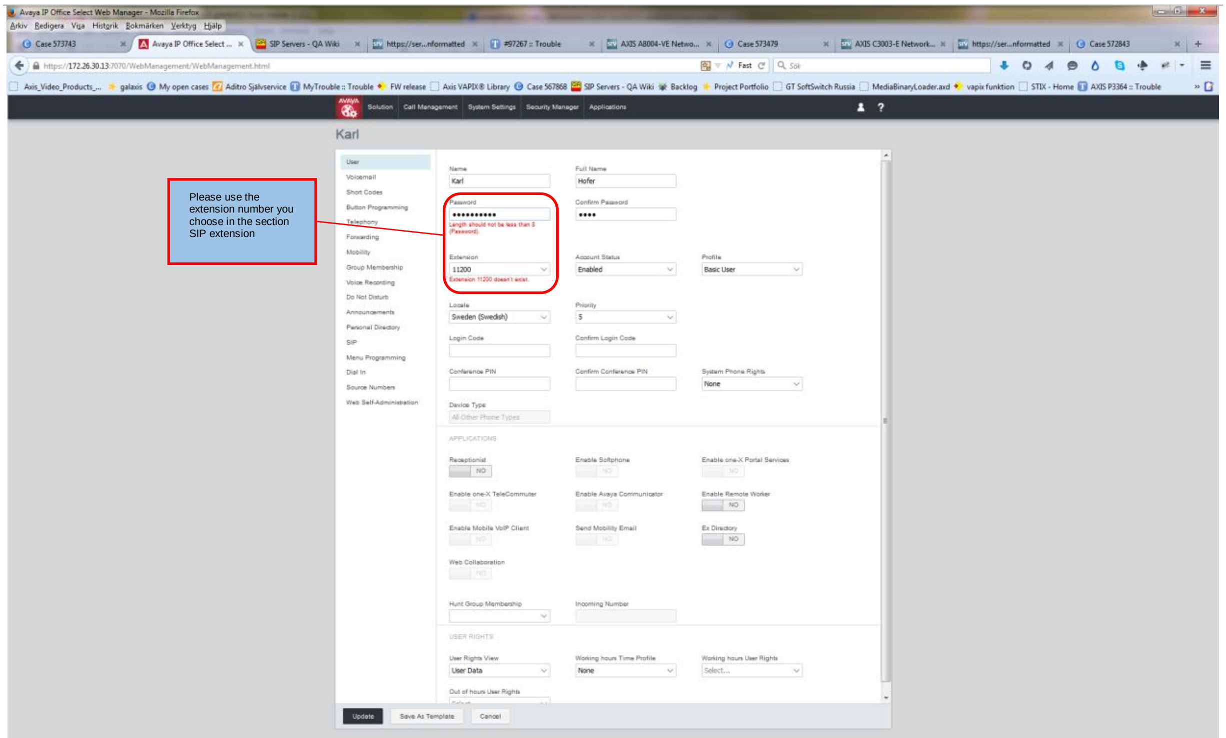
Location: Automatic

Module: 0

Port: 0

Force Authorization: YES

Now assign a USER and a PASSWORD to the extension



Please use the extension number you choose in the section SIP extension

Karl

Name: Karl

Full Name: Hofer

Password: ●●●●●●●●●●●

Length should not be less than 8 (Password).

Confirm Password: ●●●●

Extension: 11200

Extension 11200 doesn't exist.

Account Status: Enabled

Profile: Basic User

Locale: Sweden (Swedish)

Priority: 5

System Phone Rights: None

Device Type: All Other Phone Types

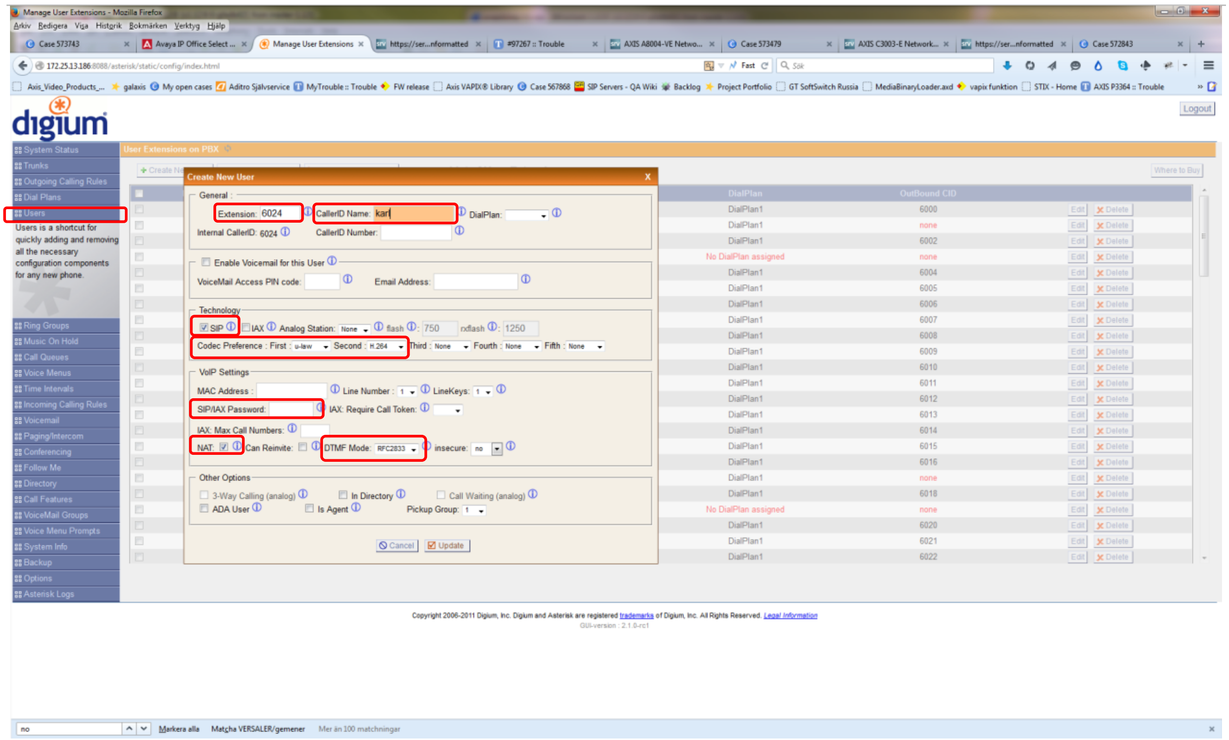
User Rights View: User Data

Working hours Time Profile: None

Now you can register your AXIS SIP DEVICE with the Avaya PBX.

6 Creating an extension and SIP USER on Asterisk PBX version 1.8.x

Create a user and assign an extension to the user



Users is a shortcut for quickly adding and removing all the necessary configuration components for any new phone.

Create New User

General :
Extension: 6024
CallerID Name: karl
DialPlan:
Internal CallerID: 6024
CallerID Number:

□ Enable Voicemail for this User
VoiceMail Access PIN code:
Email Address:

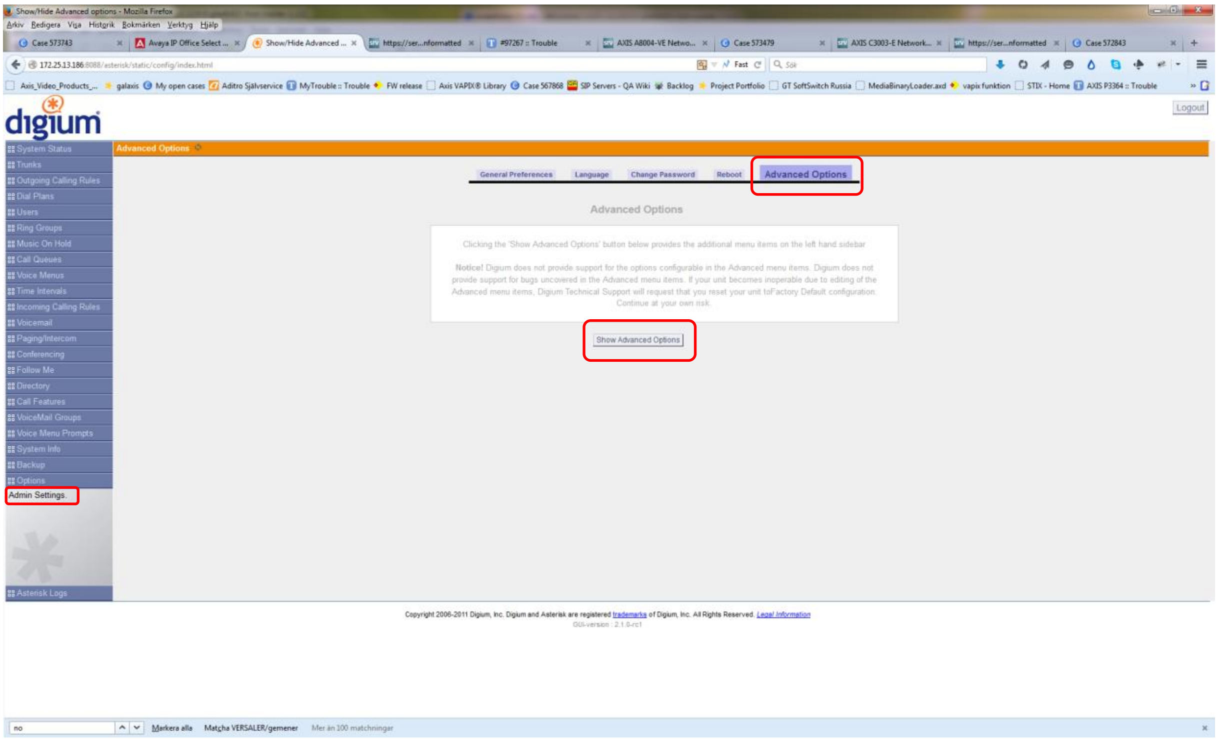
Technology
☑ SIP □ IAX Analog Station: None flash: 750 rxflash: 1250
Codec Preference : First : u-law Second : H.264 Third : None Fourth : None Fifth : None

VoIP Settings
MAC Address : Line Number : 1 LineKeys: 1
SIP/IAX Password:
IAX: Require Call Token:
IAX: Max Call Numbers:
NAT: ☑ Can Reinvite: □ DTMF Mode: RFC2833 insecure: no

Other Options
□ 3-Way Calling (analog) □ In Directory □ Call Waiting (analog)
□ ADA User □ Is Agent Pickup Group: 1

Copyright 2006-2011 Digium, Inc. Digium and Asterisk are registered trademarks of Digium, Inc. All Rights Reserved. Legal Information
GUI-version : 2.1.0-rc1

If your AXIS SIP device needs Video Support it’s important to choose H264.
In the displayed section you have to configure all account settings, create a password, choose SIP, if your SIP device is part of a NAT network choose NAT, and use the right DTMF mode, RFC2833 is recommended.



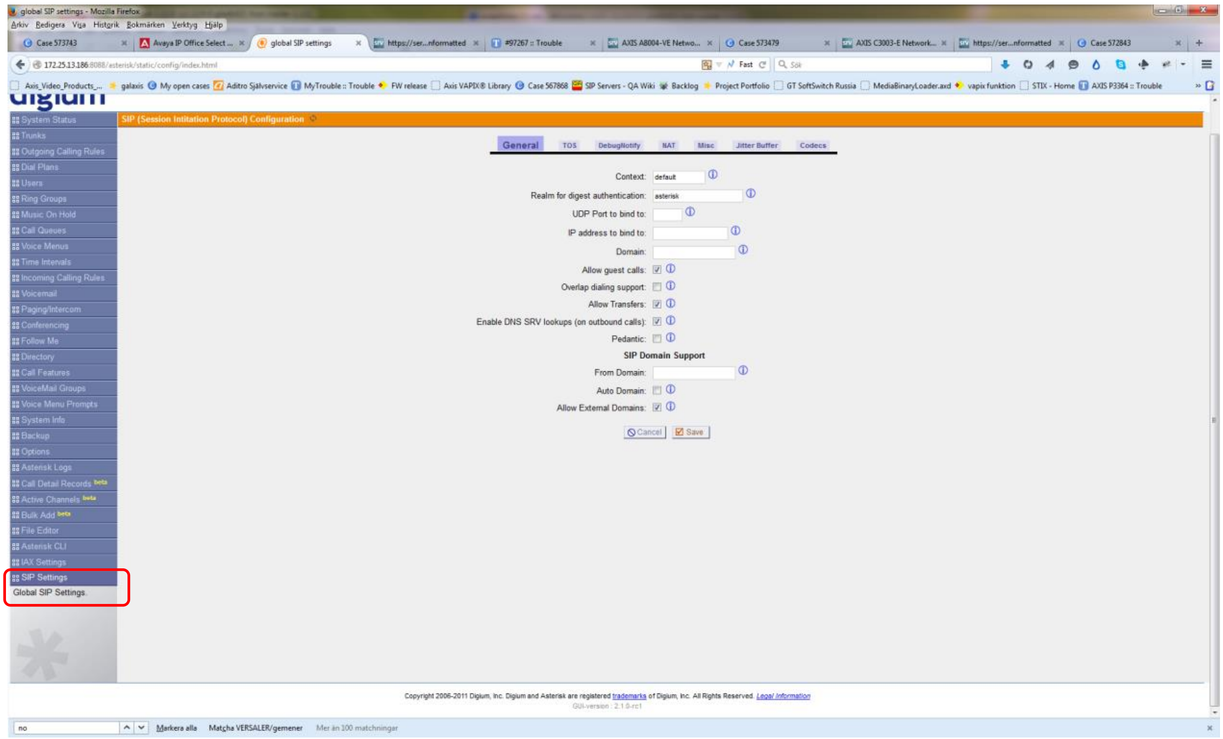
Advanced Options

Clicking the 'Show Advanced Options' button below provides the additional menu items on the left hand sidebar

Notice! Digium does not provide support for the options configurable in the Advanced menu items. Digium does not provide support for bugs uncovered in the Advanced menu items. If your unit becomes inoperable due to editing of the Advanced menu items, Digium Technical Support will request that you reset your unit toFactory Default configuration. Continue at your own risk.

Copyright 2006-2011 Digium, Inc. Digium and Asterisk are registered trademarks of Digium, Inc. All Rights Reserved. Legal Information
GUI-version : 2.1.0-rc1

In the left hand menu choose Admin Settings →Advanced Options →click Show Advanced Options



Context: default

Realm for digest authentication: asterisk

UDP Port to bind to:

IP address to bind to:

Domain:

Allow guest calls: ☑

Overlap dialing support: □

Allow Transfers: ☑

Enable DNS SRV lookups (on outbound calls): ☑

Pedantic: □

SIP Domain Support

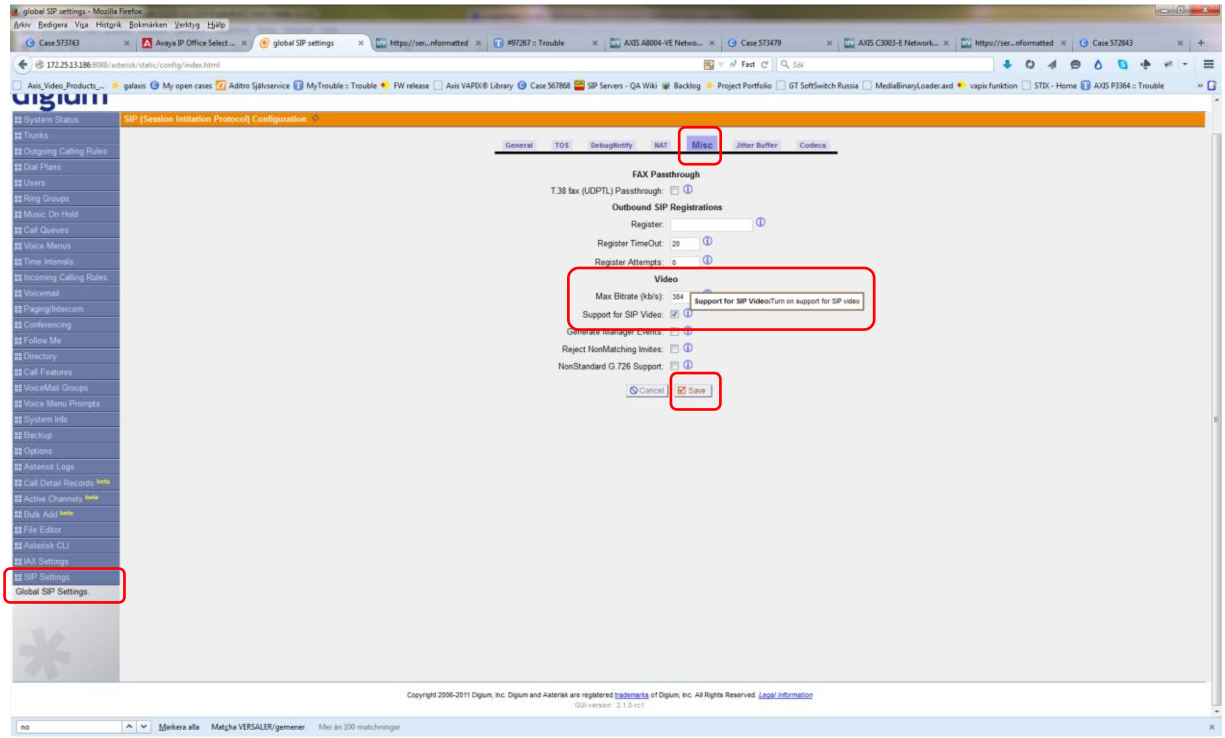
From Domain:

Auto Domain: □

Allow External Domains: ☑

Copyright 2006-2011 Digium, Inc. Digium and Asterisk are registered trademarks of Digium, Inc. All Rights Reserved. Legal Information

GUI-version : 2.1.0-rc1



FAX Passthrough

T.38 fax (UDPTL) Passthrough: □

Outbound SIP Registrations

Register:

Register TimeOut: 20

Register Attempts: 0

Video

Max Bitrate (kb/s): 384

Support for SIP Video: ☑

Support for SIP Video:Turn on support for SIP video

Generate Manager Events: □

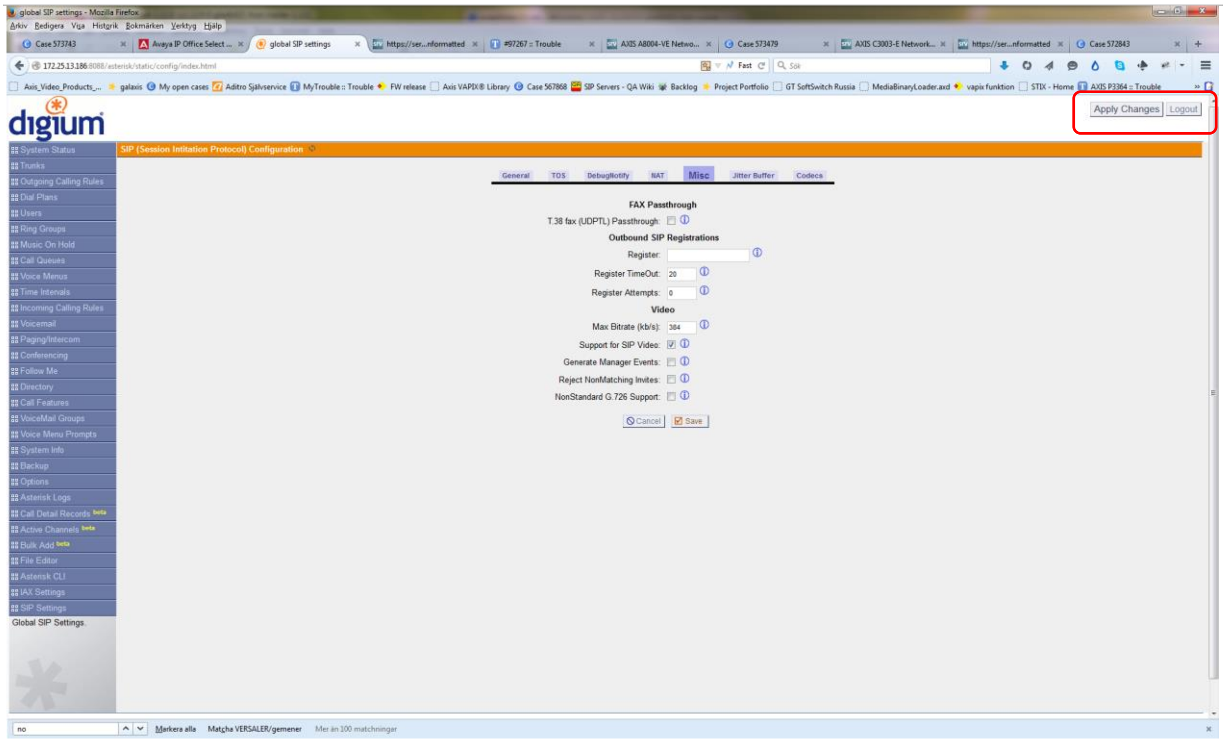
Reject NonMatching Invites: □

NonStandard G.726 Support: □

Copyright 2006-2011 Digium, Inc. Digium and Asterisk are registered trademarks of Digium, Inc. All Rights Reserved. Legal Information

GUI-version : 2.1.0-rc1

In the middle menu choose MISC and do your Video settings, check the Support for SIP Video box, and press Save and then press “Apply Changes”



FAX Passthrough

T.38 fax (UDPTL) Passthrough: □

Outbound SIP Registrations

Register:

Register TimeOut: 20

Register Attempts: 0

Video

Max Bitrate (kb/s): 384

Support for SIP Video: ☑

Generate Manager Events: □

Reject NonMatching Invites: □

NonStandard G.726 Support: □

Cancel Save

Now your Axis SIP device can register with the PBX

7 Common problem descriptions regarding sound quality

Problem	Intermittently	Periodically	Continuously
Conversational difficulty	High levels of jitter cause large numbers of packets to be discarded by the jitter buffer in the receiving IP phone or gateway. This may result in severe degradation in call quality or large increases in delay.		Echo becomes a problem when combined with a significant amount of delay. For example, if an IP phone was connected over wide area IP network to a VoIP Gateway then the delay would be large – echo that occurred on the trunk side of the Gateway would be audible in the IP Phone. If a user reports an echo problem then the source of this problem is

			likely to be on the other end of the connection. In the presence of high levels of delay the normal "protocol" of conversation breaks down. In addition, delay can make echo problems more obvious and annoying.
Gaps in speech	Voice Activity This may be due to a high rate of packet loss or packet discard due to jitter, or to a problem, with Detection associated with an echo canceller. Users report that words are being clipped - similar in effect to a lower quality speakerphone.		If users report that the start and end of words are being “clipped” then this is typically due to the Voice Activity Detector in the VoIP hardware. Voice Activity Detectors are used for silence suppression in packet voice systems, for echo suppression in echo cancellers and for echo suppression or directional control in speakerphones. Clipping can be the result of the sound level settings in the VoIP hardware being incorrectly configured.

Tick or Pop Sounds	Access link problems can be reduced by • Using priority queuing for delay sensitive voice and video traffic • Reducing the maximum MTU size on low speed links (512 kbits/s or less) • Increasing the capacity of the access link • If multiple links are used, then applying load sharing to maximize use of capacity • Applying call admission control to limit the number of calls • Using fragmentation and interleaving.	Low rates of **timing drift** may cause a periodic audible "tick". VoIP systems can sometimes hide this by doing necessary timing adjustments during silence periods. If an NTP timing server is used then VoIP systems may resynchronize or adjust their clock speed automatically. High rates of drift can be much more problematic, and may be symptomatic of hardware problems. These can be caused by high temperatures in end systems such as PCs or due to the use of cheap ceramic resonators instead of crystals in low cost IP phones.	Access link problems can be reduced by • Using priority queuing for delay sensitive voice and video traffic • Reducing the maximum MTU size on low speed links (512 kbits/s or less) • Increasing the capacity of the access link • If multiple links are used, then applying load sharing to maximize use of capacity • Applying call admission control to limit the number of calls • Using fragmentation and interleaving.
Audio quality poor or noisy, level too low or high			Generally if a connections sounds "dead" then the level of background noise is too low. This can be due to an echo canceller being mis-configured or to a poor loss plan. Other causes are mis-configuration of the background noise level in a Voice Activity Detection / Silence Elimination or Line Echo Canceller function. Voice sounds hollow, this is generally due to a high level of echo with a small amount of delay. For example, if an

			IP phone was connected over a LAN to a VoIP Gateway then the delay would be very small – echo that occurred on the trunk side of the Gateway may cause “hollowness” in the IP Phone. Distortion: Users may report that calls sound "noisy", "dead", "hollow", "cavelike" or "tunnel-like", have echo, sound slightly distorted, sound robotic, or be very choppy or garbled (see also Packet Loss)
Speech broken up or distorted	Access link problems can be reduced by • Using priority queuing for delay sensitive voice and video traffic • Reducing the maximum MTU size on low speed links (512 kbits/s or less) • Increasing the capacity of the access link • If multiple links are used, then applying load sharing to maximize use of capacity • Applying call admission control to limit the number of calls • Using fragmentation and interleaving.		Access link problems can be reduced by • Using priority queuing for delay sensitive voice and video traffic • Reducing the maximum MTU size on low speed links (512 kbits/s or less) • Increasing the capacity of the access link • If multiple links are used, then applying load sharing to maximize use of capacity • Applying call admission control to limit the number of calls • Using fragmentation and interleaving.

8 How to troubleshoot SIP

Preliminary remarks:

Before you start trouble shooting please ask for the following information
For SIP devices that are registered to a PBX/SIP registrar:
If the SIP endpoint is registered to a pubic VOIP Network ask the customer if Axis can use the SIP account for test purposes.

SIP User
SIP Authentication User
SIP Password
SIP Registrar IP address or Domain Name and its port number
DTMF protocol (SIP-Info, RFC2833)
Proxy Server and its port number (if applicable)

For Peer To Peer devices
Make sure both devices are on the same network and both SIP clients do support Peer To Peer calls.

For both cases please always ask for a server report
Ask always for a Wireshark trace
http://IP of the camera/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=120

SIP trouble shooting first steps

We start with the basics of SIP before going through the important message types, all the important responses, call flows and media.

First step should be to determine if you will have a peer to peer connection or if you are going to register your SIP client with a SIP registrar.

To get a peer to peer connection to work you have to ensure that both SIP endpoint are in the same network.

Because when addressing the calling partner you send an invite that looks like SIP:username@ipadress.to be able to reach the target IP address you have to part of the same network.

If you have to register with a Registrar you need some register information from the operator of the SIP registrar/PBX.

The Display name (if you register with a public server this can be a public phone number)

Proxy server / SIP Server /registrar Ip address/FQDN (this can be a domain name or a IP address your client has to register to)

SIP Registrar Port number your client has to register to (default is 5060)

Extension number /User ID (that's your user name)

Authentication ID: this is your authentication Id needed for the challenge request more under "**The SIP registration mechanism**"

Authentication Password: is just your password.

Please install a SIP soft phone (I suggest EKIGA http://www.ekiga.org) to make calls and configure/install an A8004-VE or a C3003-E as peer2peer or as SIP client. In this example here I use a Grandstream phone .

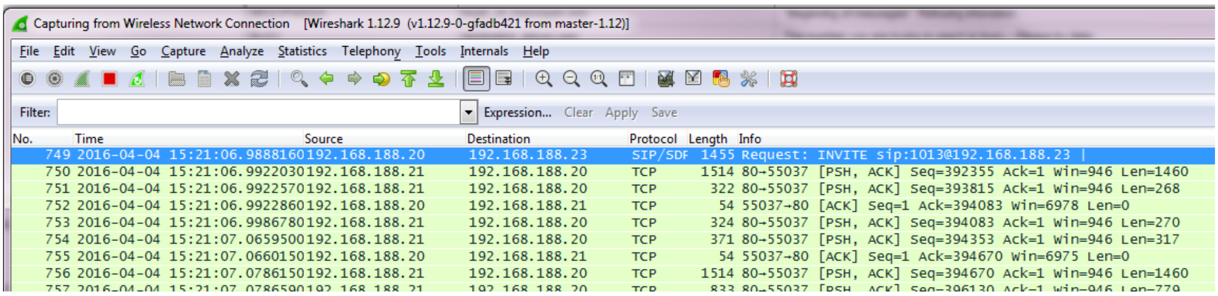
To see those things from a user's standpoint is very important. Then we go to the protocol itself. You can make some calls and then go through the SIP messages to understand what happened.

For dissecting the call flow, **Wireshark(WS) is the preferred tool**. Wireshark is a free and can be found under https://www.wireshark.org/.

Configure WS to capture the packets on a particular interface (e.g. your LAN card). Press "go" and Wireshark will then record every IP packet that comes to or from your PC through this particular interface. Press "stop" when you think you've captured what you need.

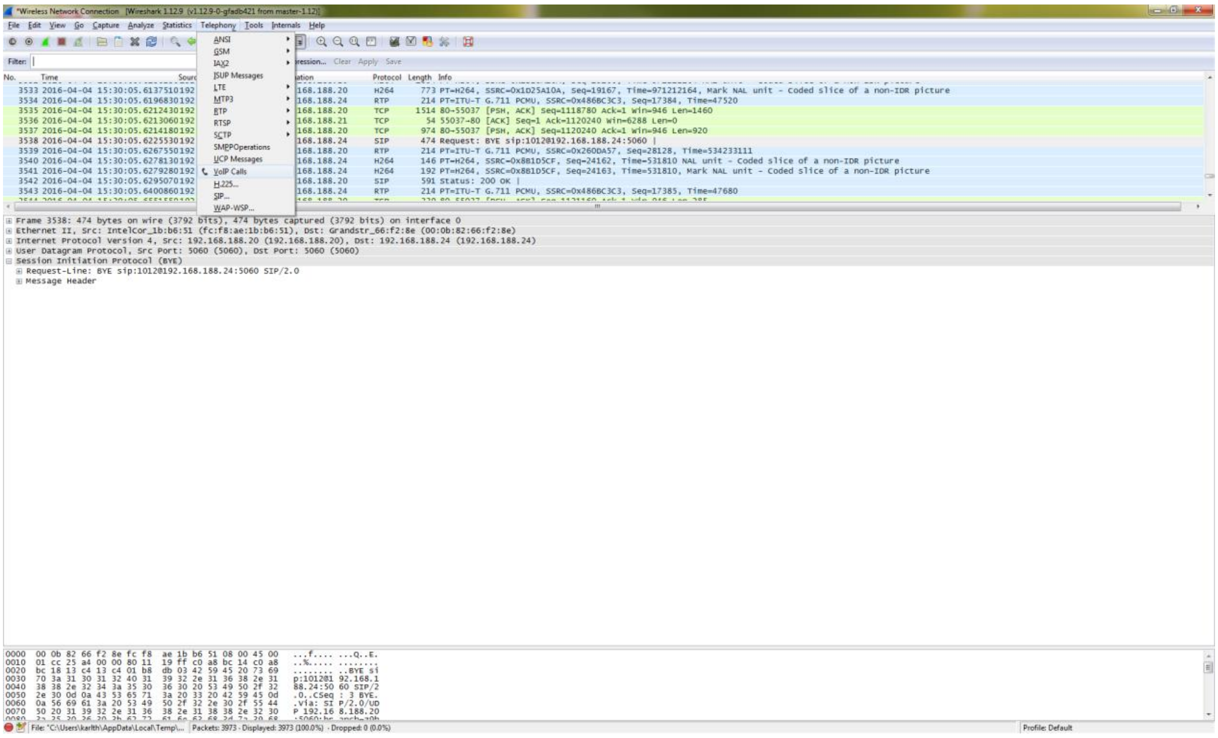
The first step is to make a two-party call. Ext. 1010 (Ekiga) calls Ext. 1012 (Grandstream). Grandstream answers the call. Ekiga hangs up the call. This will cause the Ekiga phone to send INVITE, ACK, and BYE requests. The Grandstream will send 100 Trying, 180 Ringing, and 200 OK response messages.

After capturing the packets you want to look at them.


Capturing from Wireless Network Connection [Wireshark 1.12.9 (v1.12.9-0-gfadb421 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time                          Source          Destination     Protocol Length Info
  749 2016-04-04 15:21:06.9888160192.168.188.20     192.168.188.23  SIP/SDF  1455 Request: INVITE sip:1013@192.168.188.23 |
  750 2016-04-04 15:21:06.9922030192.168.188.21     192.168.188.20  TCP      1514 80→55037 [PSH, ACK] Seq=392355 Ack=1 Win=946 Len=1460
  751 2016-04-04 15:21:06.9922570192.168.188.21     192.168.188.20  TCP       322 80→55037 [PSH, ACK] Seq=393815 Ack=1 Win=946 Len=268
  752 2016-04-04 15:21:06.9922860192.168.188.20     192.168.188.21  TCP        54 55037→80 [ACK] Seq=1 Ack=394083 Win=6978 Len=0
  753 2016-04-04 15:21:06.9986780192.168.188.21     192.168.188.20  TCP       324 80→55037 [PSH, ACK] Seq=394083 Ack=1 Win=946 Len=270
  754 2016-04-04 15:21:07.0659500192.168.188.21     192.168.188.20  TCP       371 80→55037 [PSH, ACK] Seq=394353 Ack=1 Win=946 Len=317
  755 2016-04-04 15:21:07.0660150192.168.188.20     192.168.188.21  TCP        54 55037→80 [ACK] Seq=1 Ack=394670 Win=6975 Len=0
  756 2016-04-04 15:21:07.0786150192.168.188.21     192.168.188.20  TCP      1514 80→55037 [PSH, ACK] Seq=394670 Ack=1 Win=946 Len=1460
```

The easiest way to tell Wireshark to only show you SIP messages and disregard everything else is with the “VoIP Calls” command. This can be invoked as follows.


*Wireless Network Connection [Wireshark 1.12.9 (v1.12.9-0-gfadb421 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
ANSI
GSM
IAX2
ISUP Messages
LTE
MTP3
RTP
RTSP
SCTP
SMPPOperations
UCP Messages
VoIP Calls
H.225...
SIP...
WAP-WSP...
Filter:
Expression... Clear Apply Save

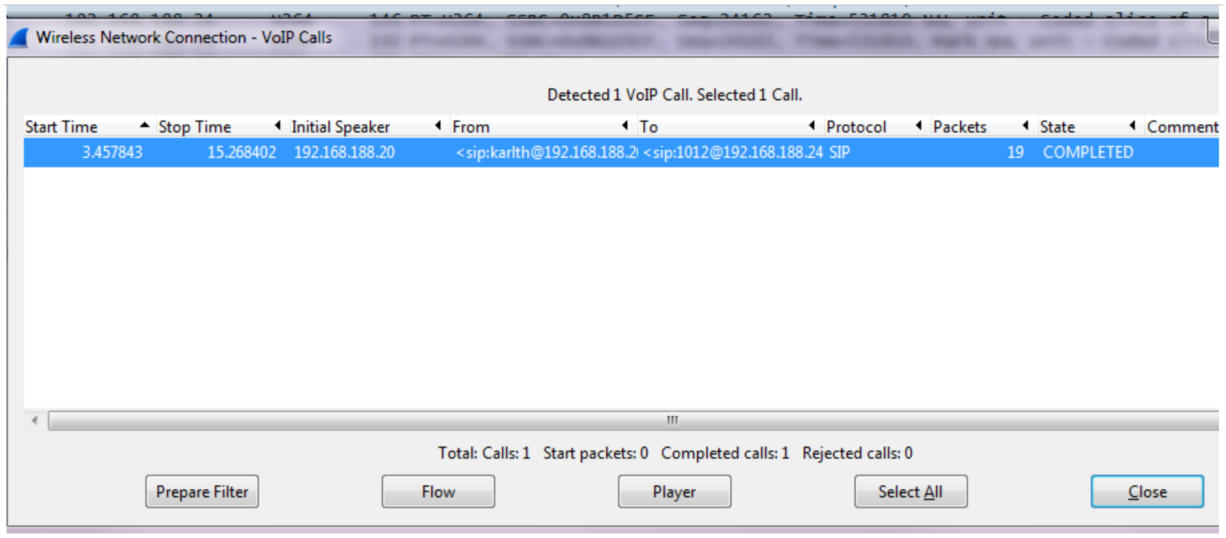
```
No.   Time                          Sourc  ation        Protocol Length Info
 3533 2016-04-04 15:30:05.6137510192  168.188.20   H264      773 PT=H264, SSRC=0x1D25A10A, Seq=19167, Time=971212164, Mark NAL unit - Coded slice of a non-IDR picture
 3534 2016-04-04 15:30:05.6196830192  168.188.24   RTP       214 PT=ITU-T G.711 PCMU, SSRC=0x486BC3C3, Seq=17384, Time=47520
 3535 2016-04-04 15:30:05.6212430192  168.188.20   TCP      1514 80→55037 [PSH, ACK] Seq=1118780 Ack=1 Win=946 Len=1460
 3536 2016-04-04 15:30:05.6213060192  168.188.21   TCP        54 55037→80 [ACK] Seq=1 Ack=1120240 Win=6288 Len=0
 3537 2016-04-04 15:30:05.6214180192  168.188.20   TCP       974 80→55037 [PSH, ACK] Seq=1120240 Ack=1 Win=946 Len=920
 3538 2016-04-04 15:30:05.6225530192  168.188.24   SIP       474 Request: BYE sip:1012@192.168.188.24:5060 |
 3539 2016-04-04 15:30:05.6267550192  168.188.20   RTP       214 PT=ITU-T G.711 PCMU, SSRC=0x260DA57, Seq=28128, Time=534233111
 3540 2016-04-04 15:30:05.6278130192  168.188.24   H264      146 PT=H264, SSRC=0x881D5CF, Seq=24162, Time=531810 NAL unit - Coded slice of a non-IDR picture
 3541 2016-04-04 15:30:05.6279280192  168.188.24   H264      192 PT=H264, SSRC=0x881D5CF, Seq=24163, Time=531810, Mark NAL unit - Coded slice of a non-IDR picture
 3542 2016-04-04 15:30:05.6295070192  168.188.20   SIP       591 Status: 200 OK |
 3543 2016-04-04 15:30:05.6400860192  168.188.24   RTP       214 PT=ITU-T G.711 PCMU, SSRC=0x486BC3C3, Seq=17385, Time=47680
```

```
⊞ Frame 3538: 474 bytes on wire (3792 bits), 474 bytes captured (3792 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_1b:b6:51 (fc:f8:ae:1b:b6:51), Dst: Grandstr_66:f2:8e (00:0b:82:66:f2:8e)
⊞ Internet Protocol Version 4, Src: 192.168.188.20 (192.168.188.20), Dst: 192.168.188.24 (192.168.188.24)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol (BYE)
  ⊞ Request-Line: BYE sip:1012@192.168.188.24:5060 SIP/2.0
  ⊞ Message Header
```

```
0000  00 0b 82 66 f2 8e fc f8  ae 1b b6 51 08 00 45 00   ...f.... ...Q..E.
0010  01 cc 25 a4 00 00 80 11  19 ff c0 a8 bc 14 c0 a8   ..%..... ........
0020  bc 18 13 c4 13 c4 01 b8  db 03 42 59 45 20 73 69   ........ ..BYE si
0030  70 3a 31 30 31 32 40 31  39 32 2e 31 36 38 2e 31   p:1012@1 92.168.1
0040  38 38 2e 32 34 3a 35 30  36 30 20 53 49 50 2f 32   88.24:50 60 SIP/2
0050  2e 30 0d 0a 43 53 65 71  3a 20 33 20 42 59 45 0d   .0..CSeq : 3 BYE.
0060  0a 56 69 61 3a 20 53 49  50 2f 32 2e 30 2f 55 44   .Via: SI P/2.0/UD
0070  50 20 31 39 32 2e 31 36  38 2e 31 38 38 2e 32 30   P 192.16 8.188.20
```

File: "C:\Users\karlth\AppData\Local\Temp\... Packets: 3973 · Displayed: 3973 (100.0%) · Dropped: 0 (0.0%) Profile: Default

On my PC, one SIP call was made while Wireshark was running in capture mode. Each SIP call has its own entry.



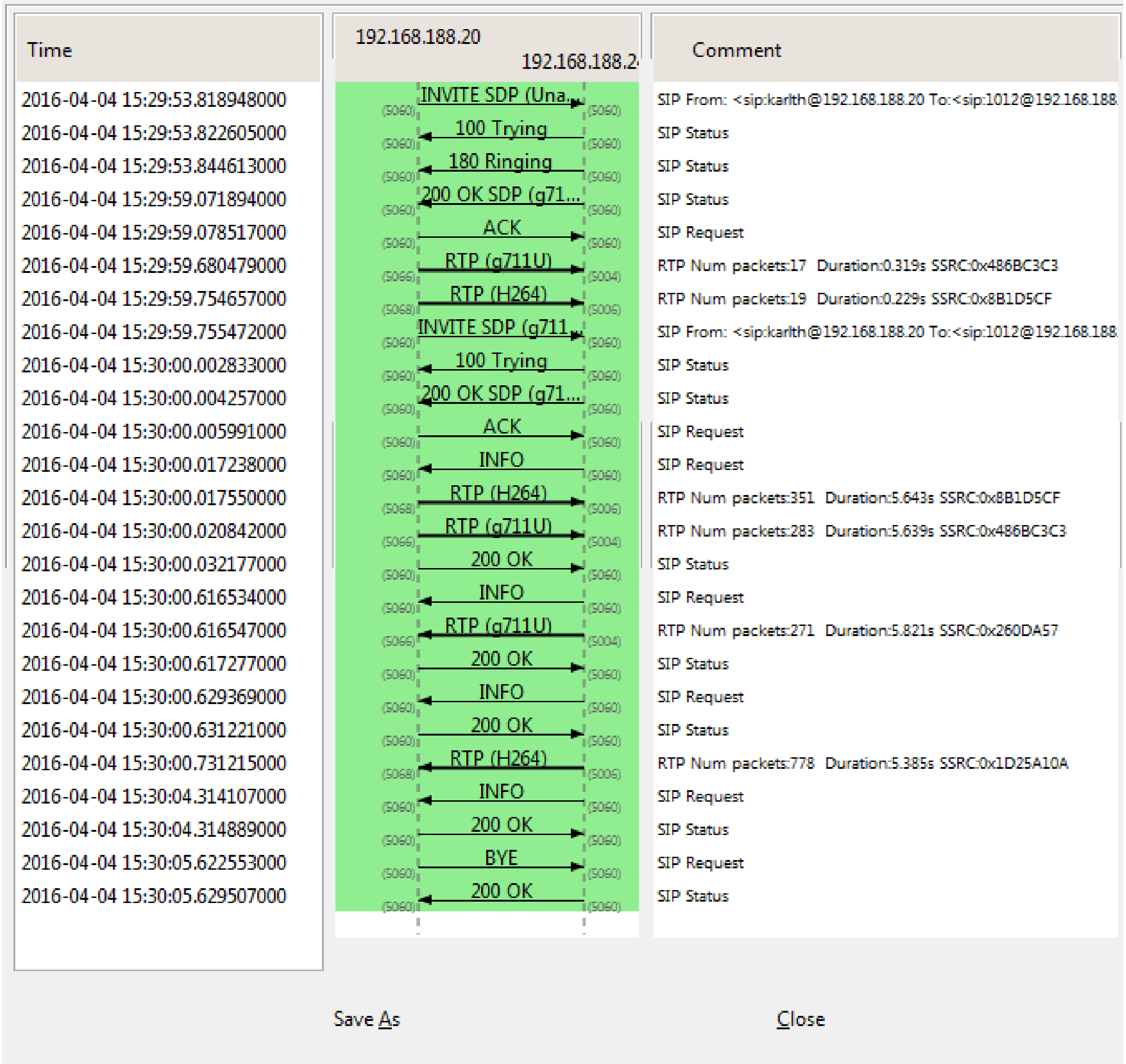
Wireless Network Connection - VoIP Calls

Detected 1 VoIP Call. Selected 1 Call.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comment
3.457843	15.268402	192.168.188.20	<sip:karlth@192.168.188.2(	<sip:1012@192.168.188.24	SIP	19	COMPLETED	

Total: Calls: 1   Start packets: 0   Completed calls: 1   Rejected calls: 0

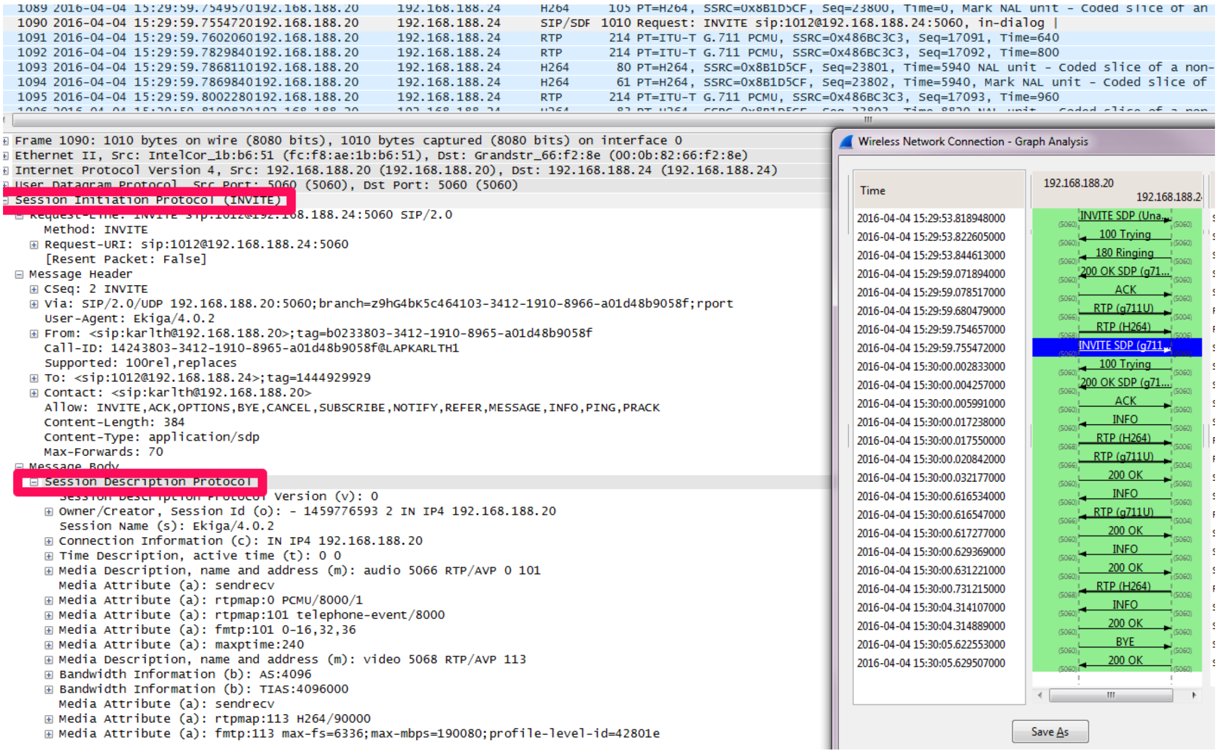
Select the session and click on the “Flow” button to see the following.



Time	192.168.188.20		192.168.188.2	Comment
2016-04-04 15:29:53.818948000	(5060)	INVITE SDP (Una... →	(5060)	SIP From: <sip:karlth@192.168.188.20 To:<sip:1012@192.168.188
2016-04-04 15:29:53.822605000	(5060)	← 100 Trying	(5060)	SIP Status
2016-04-04 15:29:53.844613000	(5060)	← 180 Ringing	(5060)	SIP Status
2016-04-04 15:29:59.071894000	(5060)	← 200 OK SDP (g71...	(5060)	SIP Status
2016-04-04 15:29:59.078517000	(5060)	ACK →	(5060)	SIP Request
2016-04-04 15:29:59.680479000	(5066)	RTP (g711U) →	(5004)	RTP Num packets:17 Duration:0.319s SSRC:0x486BC3C3
2016-04-04 15:29:59.754657000	(5068)	RTP (H264) →	(5006)	RTP Num packets:19 Duration:0.229s SSRC:0x8B1D5CF
2016-04-04 15:29:59.755472000	(5060)	INVITE SDP (g711... →	(5060)	SIP From: <sip:karlth@192.168.188.20 To:<sip:1012@192.168.188
2016-04-04 15:30:00.002833000	(5060)	← 100 Trying	(5060)	SIP Status
2016-04-04 15:30:00.004257000	(5060)	← 200 OK SDP (g71...	(5060)	SIP Status
2016-04-04 15:30:00.005991000	(5060)	ACK →	(5060)	SIP Request
2016-04-04 15:30:00.017238000	(5060)	← INFO	(5060)	SIP Request
2016-04-04 15:30:00.017550000	(5068)	RTP (H264) →	(5006)	RTP Num packets:351 Duration:5.643s SSRC:0x8B1D5CF
2016-04-04 15:30:00.020842000	(5066)	RTP (g711U) →	(5004)	RTP Num packets:283 Duration:5.639s SSRC:0x486BC3C3
2016-04-04 15:30:00.032177000	(5060)	200 OK →	(5060)	SIP Status
2016-04-04 15:30:00.616534000	(5060)	← INFO	(5060)	SIP Request
2016-04-04 15:30:00.616547000	(5066)	← RTP (g711U)	(5004)	RTP Num packets:271 Duration:5.821s SSRC:0x260DA57
2016-04-04 15:30:00.617277000	(5060)	200 OK →	(5060)	SIP Status
2016-04-04 15:30:00.629369000	(5060)	← INFO	(5060)	SIP Request
2016-04-04 15:30:00.631221000	(5060)	200 OK →	(5060)	SIP Status
2016-04-04 15:30:00.731215000	(5068)	← RTP (H264)	(5006)	RTP Num packets:778 Duration:5.385s SSRC:0x1D25A10A
2016-04-04 15:30:04.314107000	(5060)	← INFO	(5060)	SIP Request
2016-04-04 15:30:04.314889000	(5060)	200 OK →	(5060)	SIP Status
2016-04-04 15:30:05.622553000	(5060)	BYE →	(5060)	SIP Request
2016-04-04 15:30:05.629507000	(5060)	← 200 OK	(5060)	SIP Status

Wireshark displays the call flow in an easy-to-understand ladder graph. To get inside one of these message simply click on it. .

For example, if I click on the INVITE, I see the following:



```
1089 2016-04-04 15:29:59.7549570192.168.188.20    192.168.188.24    H264     105 PT=H264, SSRC=0x8B1D5CF, Seq=23800, Time=0, Mark NAL unit - Coded slice of an
1090 2016-04-04 15:29:59.7554720192.168.188.20    192.168.188.24    SIP/SDF 1010 Request: INVITE sip:1012@192.168.188.24:5060, in-dialog |
1091 2016-04-04 15:29:59.7602060192.168.188.20    192.168.188.24    RTP      214 PT=ITU-T G.711 PCMU, SSRC=0x486BC3C3, Seq=17091, Time=640
1092 2016-04-04 15:29:59.7829840192.168.188.20    192.168.188.24    RTP      214 PT=ITU-T G.711 PCMU, SSRC=0x486BC3C3, Seq=17092, Time=800
1093 2016-04-04 15:29:59.7868110192.168.188.20    192.168.188.24    H264      80 PT=H264, SSRC=0x8B1D5CF, Seq=23801, Time=5940 NAL unit - Coded slice of a non-
1094 2016-04-04 15:29:59.7869840192.168.188.20    192.168.188.24    H264      61 PT=H264, SSRC=0x8B1D5CF, Seq=23802, Time=5940, Mark NAL unit - Coded slice of
1095 2016-04-04 15:29:59.8002280192.168.188.20    192.168.188.24    RTP      214 PT=ITU-T G.711 PCMU, SSRC=0x486BC3C3, Seq=17093, Time=960
```

```
⊞ Frame 1090: 1010 bytes on wire (8080 bits), 1010 bytes captured (8080 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_1b:b6:51 (fc:f8:ae:1b:b6:51), Dst: Grandstr_66:f2:8e (00:0b:82:66:f2:8e)
⊞ Internet Protocol Version 4, Src: 192.168.188.20 (192.168.188.20), Dst: 192.168.188.24 (192.168.188.24)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol (INVITE)
  ⊟ Request-Line: INVITE sip:1012@192.168.188.24:5060 SIP/2.0
      Method: INVITE
    ⊞ Request-URI: sip:1012@192.168.188.24:5060
      [Resent Packet: False]
  ⊟ Message Header
    ⊞ CSeq: 2 INVITE
    ⊞ Via: SIP/2.0/UDP 192.168.188.20:5060;branch=z9hG4bK5c464103-3412-1910-8966-a01d48b9058f;rport
      User-Agent: Ekiga/4.0.2
    ⊞ From: <sip:karlth@192.168.188.20>;tag=b0233803-3412-1910-8965-a01d48b9058f
      Call-ID: 14243803-3412-1910-8965-a01d48b9058f@LAPKARLTH1
      Supported: 100rel,replaces
    ⊞ To: <sip:1012@192.168.188.24>;tag=1444929929
    ⊞ Contact: <sip:karlth@192.168.188.20>
      Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,MESSAGE,INFO,PING,PRACK
      Content-Length: 384
      Content-Type: application/sdp
      Max-Forwards: 70
  ⊟ Message Body
    ⊟ Session Description Protocol
        Session Description Protocol Version (v): 0
      ⊞ Owner/Creator, Session Id (o): - 1459776593 2 IN IP4 192.168.188.20
        Session Name (s): Ekiga/4.0.2
      ⊞ Connection Information (c): IN IP4 192.168.188.20
      ⊞ Time Description, active time (t): 0 0
      ⊞ Media Description, name and address (m): audio 5066 RTP/AVP 0 101
        Media Attribute (a): sendrecv
      ⊞ Media Attribute (a): rtpmap:0 PCMU/8000/1
      ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
      ⊞ Media Attribute (a): fmtp:101 0-16,32,36
      ⊞ Media Attribute (a): maxptime:240
      ⊞ Media Description, name and address (m): video 5068 RTP/AVP 113
      ⊞ Bandwidth Information (b): AS:4096
      ⊞ Bandwidth Information (b): TIAS:4096000
        Media Attribute (a): sendrecv
      ⊞ Media Attribute (a): rtpmap:113 H264/90000
      ⊞ Media Attribute (a): fmtp:113 max-fs=6336;max-mbps=190080;profile-level-id=42801e
```

Wireless Network Connection - Graph Analysis

Time	192.168.188.20		192.168.188.24
2016-04-04 15:29:53.818948000	(5060)	INVITE SDP (Una... →	(5060)
2016-04-04 15:29:53.822605000	(5060)	← 100 Trying	(5060)
2016-04-04 15:29:53.844613000	(5060)	← 180 Ringing	(5060)
2016-04-04 15:29:59.071894000	(5060)	← 200 OK SDP (g71...	(5060)
2016-04-04 15:29:59.078517000	(5060)	ACK →	(5060)
2016-04-04 15:29:59.680479000	(5066)	RTP (g711U) →	(5004)
2016-04-04 15:29:59.754657000	(5068)	RTP (H264) →	(5006)
2016-04-04 15:29:59.755472000	(5060)	INVITE SDP (g711... →	(5060)
2016-04-04 15:30:00.002833000	(5060)	← 100 Trying	(5060)
2016-04-04 15:30:00.004257000	(5060)	← 200 OK SDP (g71...	(5060)
2016-04-04 15:30:00.005991000	(5060)	ACK →	(5060)
2016-04-04 15:30:00.017238000	(5060)	← INFO	(5060)
2016-04-04 15:30:00.017550000	(5068)	RTP (H264) →	(5006)
2016-04-04 15:30:00.020842000	(5066)	RTP (g711U) →	(5004)
2016-04-04 15:30:00.032177000	(5060)	200 OK →	(5060)
2016-04-04 15:30:00.616534000	(5060)	← INFO	(5060)
2016-04-04 15:30:00.616547000	(5066)	← RTP (g711U)	(5004)
2016-04-04 15:30:00.617277000	(5060)	200 OK →	(5060)
2016-04-04 15:30:00.629369000	(5060)	← INFO	(5060)
2016-04-04 15:30:00.631221000	(5060)	200 OK →	(5060)
2016-04-04 15:30:00.731215000	(5068)	← RTP (H264)	(5006)
2016-04-04 15:30:04.314107000	(5060)	← INFO	(5060)
2016-04-04 15:30:04.314889000	(5060)	200 OK →	(5060)
2016-04-04 15:30:05.622553000	(5060)	BYE →	(5060)
2016-04-04 15:30:05.629507000	(5060)	← 200 OK	(5060)

Do you see that little plus sign ("+") next to the words "Session Initiation Protocol"? Click on it and the actual INVITE message will open up.

Do you see that little plus sign ("+") next to the words "Session Description Protocol"? Click on it and the actual INVITE message will open up.

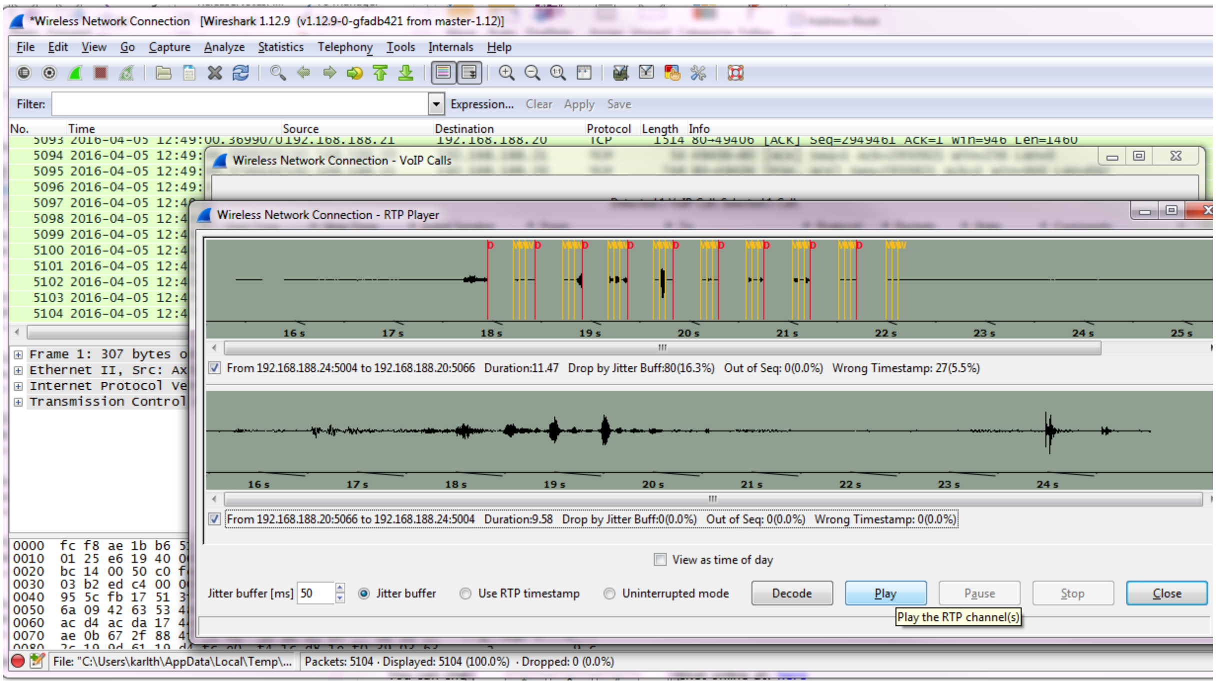
At this point you can examine the SIP URI, headers, and even the message body. Since SIP is fairly easy to read and understand, it doesn't take much to figure out what is happening with each message in a call flow. Later in the document we will have a look at the registration process and the SDP part.

You can save these traces, too. Wireshark saves traces in pcap (packet capture) files. On our AXIS devices you have the possibility to capture such files directly on the device via VAPIX

http://root:pass@IP/AXIS-cgi/debug/debug.tgz?cmd=pcapdump&duration=30

(AXIS device will take 30s network trace)

One last WS feature I want to show you t is how to get/replay to the actual media. As you may know, media is sent in RTP packets and since RTP is just another kind of IP packet, Wireshark captures those, too. Go back to the list of SIP calls, select the one in question, and press “Play” to see the following.


*Wireless Network Connection [Wireshark 1.12.9 (v1.12.9-0-gfadb421 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time                           Source              Destination        Protocol Length Info
 5093 2016-04-05 12:49:00.369907 0192.168.188.21     192.168.188.20     TCP       1514 80→49406 [ACK] Seq=2949461 Ack=1 Win=946 Len=1460
 5094 2016-04-05 12:49:
 5095 2016-04-05 12:49:
 5096 2016-04-05 12:49:
 5097 2016-04-05 12:4
 5098 2016-04-05 12:4
 5099 2016-04-05 12:4
 5100 2016-04-05 12:4
 5101 2016-04-05 12:4
 5102 2016-04-05 12:4
 5103 2016-04-05 12:4
 5104 2016-04-05 12:4

⊞ Frame 1: 307 bytes o
⊞ Ethernet II, Src: Ax
⊞ Internet Protocol Ve
⊞ Transmission Control

0000  fc f8 ae 1b b6 5
0010  01 25 e6 19 40 0
0020  bc 14 00 50 c0 f
0030  03 b2 ed c4 00 0
0040  95 5c fb 17 51 3
0050  6a 09 42 63 53 4
0060  ac d4 ac da 17 4
0070  ae 0b 67 2f 88 4
```

Wireless Network Connection - VoIP Calls

Wireless Network Connection - RTP Player

☑ From 192.168.188.24:5004 to 192.168.188.20:5066 Duration:11.47 Drop by Jitter Buff:80(16.3%) Out of Seq: 0(0.0%) Wrong Timestamp: 27(5.5%)

☑ From 192.168.188.20:5066 to 192.168.188.24:5004 Duration:9.58 Drop by Jitter Buff:0(0.0%) Out of Seq: 0(0.0%) Wrong Timestamp: 0(0.0%)

☐ View as time of day

Jitter buffer [ms] 50 ● Jitter buffer ○ Use RTP timestamp ○ Uninterrupted mode

File: "C:\Users\karlth\AppData\Local\Temp\... Packets: 5104 · Displayed: 5104 (100.0%) · Dropped: 0 (0.0%)

This allows you to “Decode” and “Play” the audio stream between the Softphone and the Grandstream phone.

This is a good way to check the audio quality.

9 UNDERSTANDING SESSION DESCRIPTION PROTOCOL (SDP)

It´s not possible to trouble shoot SIP without having a fairly good understanding of the Session Description Protocol (SDP). SIP only deals with establishing, modifying, and ending sessions but SDP takes care about the media within the session.

SDP is a protocol that describes the media of a session but it doesn't negotiate the media. Instead, one party tells the other party, “here are all the media types I can support — pick one and use it.”

SDP contains a series of <character>=<value> lines, where <character> is a single case-sensitive alphabetic character and <value> is structured text.

SDP has three main sections – session, timing, and media descriptions. Each message may contain multiple timing and media descriptions, but only one session description.

The definition of those sections and their possible contents are as follows. It's important to know that not every character/value may be present in an SDP message.

Session description

v= (protocol version number, currently only 0)

o= (originator and session identifier : username, id, version number, network address)

s= (session name : mandatory with at least one UTF-8-encoded character)

i=* (session title or short information)

u=* (URI of description)

e=* (zero or more email address with optional name of contacts)

p=* (zero or more phone number with optional name of contacts)

c=* (connection information—not required if included in all media)

b=* (zero or more bandwidth information lines)

One or more Time descriptions (“t=” and “r=” lines; see below)

z=* (time zone adjustments)

k=* (encryption key)

a=* (zero or more session attribute lines)

Zero or more Media descriptions (each one starting by an “m=” line; see below)

Time description (mandatory)

t= (time the session is active)

r=* (zero or more repeat times)

Media description (if present)

m= (media name and transport address)

i=* (media title or information field)

c=* (connection information — optional if included at session level)

b=* (zero or more bandwidth information lines)

k=* (encryption key)

a=* (zero or more media attribute lines — overriding the Session attribute lines)

For Example

The following is an example of an actual SDP message.

v=0

o=1011 2890844526 2890844526 IN IP4 192.168.188.21

```
s= SDP Blog

c=IN IP4 192.168.188.23

t=0 0

m=audio 49170 RTP/AVP 0 8 97

a=rtpmap:0 PCMU/8000

a=rtpmap:8 PCMA/8000

a=rtpmap:97 iLBC/8000

m=video 9078 RTP/AVP 96

a=rtpmap:31 H264/90000
```

The following lines are worth to pay attention to in an SDP message

c= This will tell me the IP address where the media will come from and where it should be sent to.

m= There will be an entry for each media type. If your client supports real-time audio there will be an m= audio line. If your client supports real-time video there will be m=video line. Each media line indicates the port number and the type of codecs that will be defined in attribute lines.

a= There will be an attribute line for each codec advertised in the media line.

Looking at the example above we can see the following:

The client will use IP version 4 with an address of 192.168.188.21. It can support three audio codecs and one video codec. The audio codecs are G.711 uLaw (PCMU), G.711 aLaw (PCMA), and iLBC. The audio codecs will use port 49170 and all have a sample rate of 8000 Hz. The video codec is H.264 on port 51327.

After receiving the SIP message (Invite with SDP) with the above SDP content, the recipient will respond with a SDP packet identifying its IP address, ports, and codec values. The recipient will also pick from the list of the sender's codecs which ones it will use and potentially start real-time media flows.

If you like take some Wireshark traces and try to figure out how media is being described and used.

10 Traversal of UDP through NAT

STUN is an industry standard approach for traversal of NAT and the technical details are published as RFC 3489. It requires that your IP phone has access to a STUN server somewhere on the Internet. Your VoIP service provider should be able to give you the address details of their STUN server, but don't despair if they cannot. See the section below that explains how to make your phone use STUN. **A simple explanation of how STUN works**, it sends a number of queries to the specified STUN server. The STUN server carries out a few simple tests to determine things like: Is the IP phone behind a NAT device? What is the external IP address of the NAT device? How tightly does the NAT device enforce rules for blocking inbound UDP connections? Does it make a difference to inbound connections if an outbound connection has already been established to that remote address? It then reports the results back to the AXIS device. The AXIS device is now able to use this information to modify the SIP messages it sends when it registers and, if you are lucky, everything will now work perfectly.

STUN does not include an authentication dialogue so generally any phone can use any STUN server. Here are some addresses that might work if you in need of a STUN Server: stun.xten.com, stun.SIPgate.net, stunserver.org

11 Introduction to ICE (from http://www.pjSIP.org)

Interactive Connectivity Establishment (ICE) is the ultimate weapon a client can have in its NAT traversal solution arsenals, as it promises that if there is indeed one path for two clients to communicate, then ICE will find this path. And if there are more than one paths which the clients can communicate, ICE will use the best/most efficient one.

ICE works by combining several protocols (such as STUN and TURN) altogether and offering several candidate paths for the communication, thereby maximising the chance of success, but at the same time also has the capability to prioritize the candidates, so that the more expensive alternative (namely relay) will only be used as the last resort when else fails. ICE negotiation process involves several stages:

- candidate gathering, where the client finds out all the possible addresses that it can use for the communication. It may find three types of candidates: host candidate to represent its physical NICs, server reflexive candidate for the address that has been resolved from STUN, and relay candidate for the address that the client has allocated from a TURN relay.
- prioritizing these candidates. Typically the relay candidate will have the lowest priority to use since it's the most expensive.
- encoding these candidates, sending it to remote peer, and negotiating it with offer-answer.
- pairing the candidates, where it pairs every local candidates with every remote candidates that it receives from the remote peer.
- checking the connectivity for each candidate pairs.

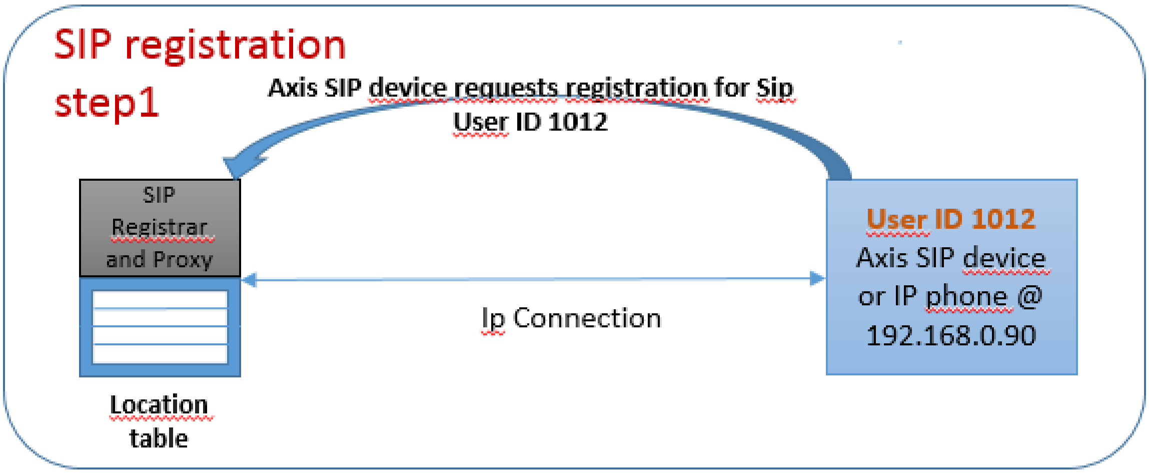
- concluding the result. Since every possible path combinations are checked, if there is a path to communicate ICE will find it.

12 The SIP registration and how it works

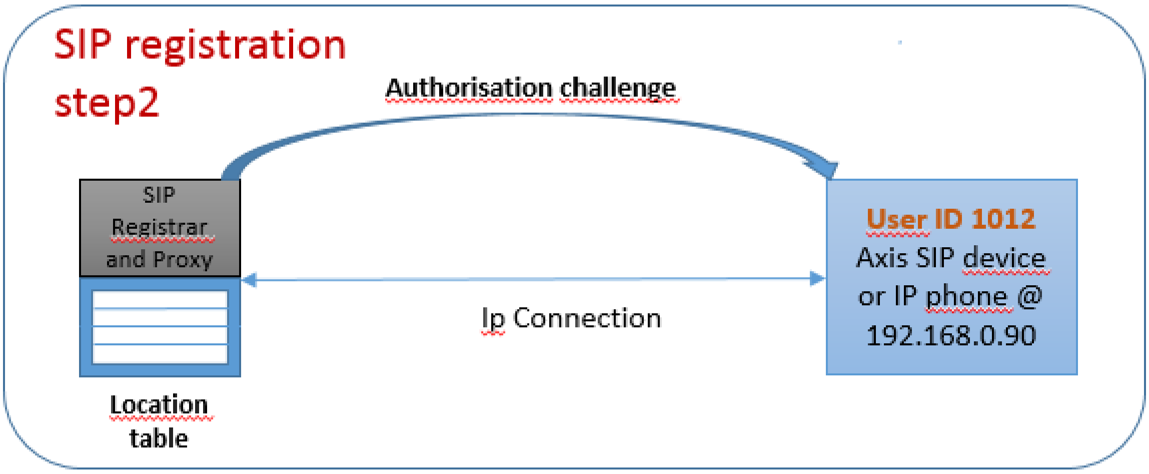
It is normal for SIP registrations to be authenticated by a challenge process. The SIP device sends a REGISTER request with minimal credentials and the Registrar server sends back a “401 Unauthorised” response. The device then re-sends the registration request, but this time it adds an “Authorization” header containing a digest of user information and an encrypted version of the password.

If the information matches with a known user, the registration will be accepted and a record is written to the location table.

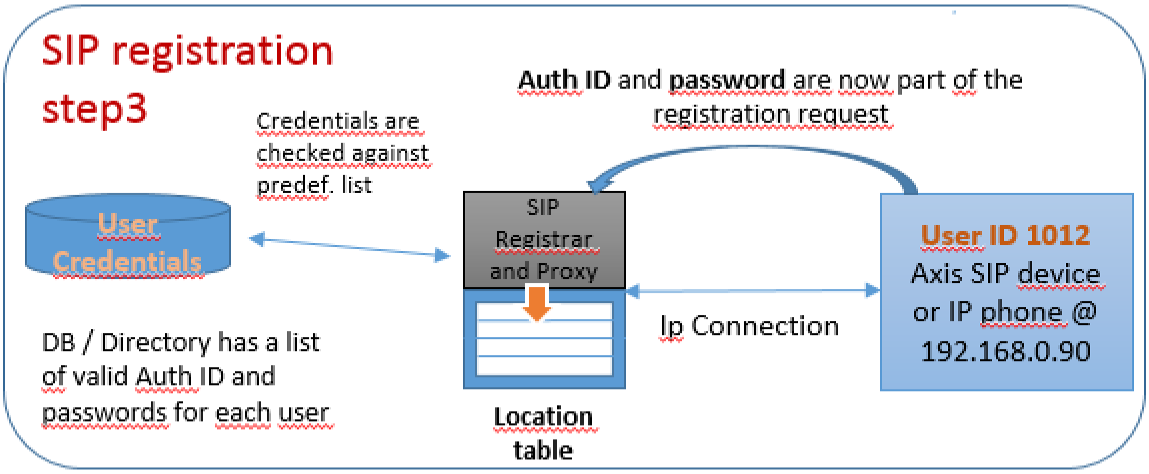
In case you have or your customer are having trouble to register a AXIS SIP device please have a look at the illustrated steps:


SIP registration
step1
Axis SIP device requests registration for Sip User ID 1012
SIP Registrar and Proxy
Location table
Ip Connection
User ID 1012
Axis SIP device or IP phone @ 192.168.0.90

SIP registration step2

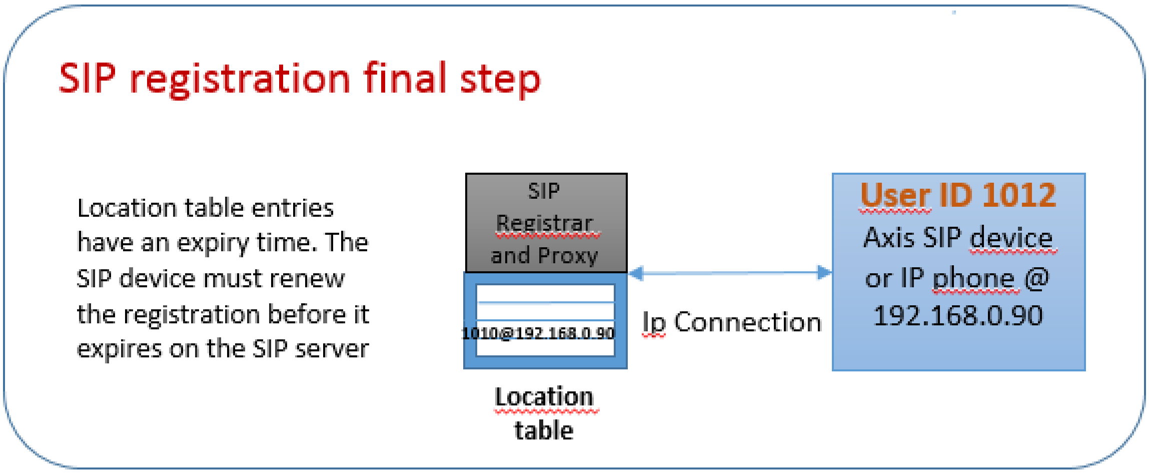


SIP registration step3


Auth ID and password are now part of the registration request
Credentials are checked against predef. list
User Credentials
SIP Registrar and Proxy
Location table
Ip Connection
User ID 1012
Axis SIP device or IP phone @ 192.168.0.90

DB / Directory has a list of valid Auth ID and passwords for each user

SIP registration final step



Location table entries have an expiry time. The SIP device must renew the registration before it expires on the SIP server

13 Appendix

SIP Error Messages (this is an extract of https://en.wikipedia.org/wiki/List_of_SIP_response_codes, be aware of that most of the SIP servers do have the possibility to change the codes and that they can have totally different meaning.)

Informational(1xx)
Informational responses are used to indicate call progress. Normally the responses are end to end (except 100 Trying). The main objective of informational responses is to stop retransmission of INVITE requests.
Informational responses include the following responses:

100 Trying
-This special case response is only a hop-by-hop request.
-It is never forwarded and may not contain a message body.
-It is used to avoid the retransmission of INVITE requests.

180 Ringing
-This response is used to indicate that an INVITE has been received by the user agent and alerting is taking place.

181 Call is Being Forwarded
-This response is used to indicate that the call has been forwarded to another endpoint.
-It is sent when the information may be of use to the caller.
-It gives the status of the caller, as a forwarding operation may result in the call taking longer to be answered.

182 Call Queued
-This response is used to indicate that the INVITE has been received and will be processed in a queue.

183 Session Progress
-It indicates that information about the progress of a session may be present in a message body or media stream.
-Unlike a 100 Trying response, a 183 is an end-to-end response and establishes a dialog.
-A typical use of this response is to allow a UAC to hear a ringtone, busy tone, or recorded announcement in calls through a gateway into the PSTN.

Success(2xx)
This class of responses is meant for indicating that a request has been accepted. It includes the following responses:

200 OK
-200 OK is used to accept a session invitation.
-It indicates a successful completion or receipt of a request.

202 Accepted
-202 Accepted indicates that the UAS has received and understood the request, but that the request may not have been authorized or processed by the server.
-It is commonly used in responses to SUBSCRIBE, REFER methods.

Redirection(3xx)
Generally these class responses are sent by redirect servers in response to INVITE. They are also known as redirect class responses. It includes the following responses:

300 Multiple Choices
-It contains multiple Contact header fields to indicate that the location service has returned multiple possible locations for the SIP URI in the Request-URI.

301 Moved Permanently
-This redirection response contains a Contact header field with the new permanent URI of the called party.
-The address can be saved and used in future INVITE requests.

302 Moved Temporarily
-This redirection response contains a URI that is currently valid but is not permanent.
-That is, the location is valid for the duration of the time specified.

305 Use Proxy
-This response contains a URI that points to a proxy server having authoritative information about the calling party.
-This response could be sent by a UAS issuing a proxy for incoming call screening.

380 Alternative Service
-This response returns a URI that indicates the type of service the called party would like.
-For example, a call could be redirected to a voicemail server.

Client Error(4xx)
Client error responses indicate that the request cannot be fulfilled as some errors are identified from the UAC side. The response codes are generally sent by UAS. Upon receiving an error message, the client should resend the request by modifying it based on the response. Discussed below are some of the important client error responses.

400 Bad Request
-It indicates that the request was not understood by the server.
-Request might be missing required header fields such as To, From, Call-ID, or CSeq.

401 Unauthorized
-It indicates that the request requires the user to perform authentication.
-401 Unauthorized is normally sent by a registrar server for REGISTER request.
-The response contains WWW-Authenticate header field which requests for correct credentials from the calling user agent.
-A subsequent REGISTER will trigger from the User Agent with correct credentials.

403 Forbidden
-403 Forbidden is sent when the server has understood the request, found the request to be correctly formulated, but will not service the request.
-This response is not used when authorization is required.

404 Not Found
-404 Not Found indicates that the user identified by the SIP URI in the Request-URI cannot be located by the server or that the user is not currently signed on with the user agent.

405 Method Not Allowed
-It indicates that the server or user agent has received and understood a request but is not willing to fulfil the request.
-Example: A REGISTER request might be sent to a user agent.
-An Allow field must be present to inform the UAC as to what methods are acceptable.

406 Not Acceptable
-This response indicates that the request cannot be processed due to a requirement in the request message.

-The Accept header field in the request did not contain any options supported by the UAS.

407 Proxy Authentication Required
-This request sent by a proxy indicates that the UAC must first authenticate itself with the proxy before the request can be processed.
-The response should contain information about the type of credentials required by the proxy in a Proxy-Authenticate header field.
-The request can be resubmitted with the proper credentials in a Proxy-Authorization header field.

408 Request Timeout
-This response is sent when an Expires header field is present in an INVITE request and the specified time period has passed.
-It could be sent by a forking proxy or a user agent.
-The request can be retried at any time by the UAC.

422 Session Timer Interval Too Small
-The response is used to reject a request containing a Session-Expires header field.
-The minimum allowed interval is indicated in the required Min-SE header field.
-The calling party may retry the request without the Session-Expires header field or with a value less than or equal to the specified minimum.

423 Interval Too Brief
-The response is returned by a registrar that is rejecting a registration request because the requested expiration time on one or more Contacts is too brief.
-The response must contain a Min-Expires header field listing the minimum expiration interval that the registrar will accept.

480 Temporarily Unavailable
-This response indicates that the request has reached the correct destination, but the called party is not available for some reason.
-The response should contain a Retry-After header indicating when the request may be able to be fulfilled.

481 Dialog/Transaction Does Not Exist
-This response indicates that a response referencing an existing call or transaction has been received for which the server has no records or state information.

483 Too Many Hops
-This response indicates that the request has been forwarded the maximum number of times as set by the Max-Forwards header in the request.
-This is indicated by the receipt of a Max-Forward: 0 header in a request.

486 Busy Here
-This indicates the user agent is busy and cannot accept the call.

487 Request Terminated
-This response can be sent by a UA that has received a CANCEL request for a pending INVITE request.
-A 200 OK is sent to acknowledge the CANCEL, and a 487 is sent to cancel the INVITE transaction.

Server Failure (5xx)
This class response is used to indicate that the request cannot be processed because of an error with the server. The server failed to fulfil an apparently valid request. The response may contain a Retry-After header field. The request can be tried at other locations because there are no errors indicated in the request. Some of the important server failure responses are discussed below.

500 Server Internal Error
-500 indicates that the server has experienced some kind of error that is preventing it from processing the request.

-It is one kind of server failure that indicates the client to retry the request again at this server after several seconds.

501 Not Implemented
-It indicates that the server is unable to process the request because it is not supported.
-This response can be used to decline a request containing an unknown method.

502 Bad Gateway
-This response is sent by a proxy that is acting as a gateway to another network.
-It indicates some problem in the other network is preventing the request from being processed.

503 Service Unavailable
-This response indicates that the requested service is temporarily unavailable at that time.
-The request can be retried after a few seconds, or after the expiration of the Retry-After header field.

504 Gateway Timeout
-This response comes when the request failed due to a timeout occurred in the other network to which the gateway connects.
-It is a server error class response because the call is failing due to a failure of the server in accessing resources outside the SIP network.

505 Version Not Supported
-The server denies a request when it comes with a different SIP version number. The denial is indicated in this message.
-Currently SIP version 2.0 is the only version implemented.

513 Message Too Large
-This response is used by a UAS to indicate that the request size was too large for it to process.
580 Preconditions Failure
-This response is used to reject an SDP offer in which required preconditions cannot be met.

Global Error (6xx)
This response class indicates that the server knows that the request will fail wherever it is tried. As a result, the request should not be sent to other locations.
Only a server having definitive knowledge of the user identified by the Request-URI in every possible instance should send a global error class response. Otherwise, a client error class response should be sent.
A Retry-After header field can be used to indicate when the request might be successful. Some of the important responses are discussed below:
600 Busy Everywhere
-This response indicates that the call to the specified Request-URI could be answered in other locations.

603 Decline
-This response could indicate the called party is busy, or simply does not want to accept the call.

604 Does Not Exist Anywhere
-This response is similar to the 404 Not Found response but indicates that the user in the Request-URI cannot be found anywhere.
-This response should only be sent by a server having access to all the information about the user.

606 Not Acceptable
-This response indicates that some aspect of the desired session is not acceptable to the UAS, and as a result, the session cannot be established.
-The response may contain a Warning header field with a numerical code describing exactly what was not acceptable.
-The request can be retried with different media session information.