



# CONNECTING A REMOTE EXTENSION IN 3CX

## 1. Introduction

### 1.1 General

This guide will cover the configuration of a 3CX PBX in respect to server and client configurations in order to setup staff members to work from home.

It will cover different methods to connect to 3CX remotely regardless if 3CX is hosted in the cloud or on premise.

It has been written for 3CX version 16, however some components may be relevant for versions 15.5 and version 15.0

The following scenarios will be covered;

- Remote extensions using 3CX Webclient
- Remote extensions using 3CX Softclient
- Remote extensions using 3CX SBC
- Remote extensions using 3CX mobile client
- Remote extensions using STUN provisioning
- Remote extensions using manual provisioning
- Using Jabra cordless Headsets with 3CX Webclient

## Contents

1. Introduction .....	1
1.1 General.....	1
2. General preparation.....	4
2.1 Prerequisites .....	4
2.2 Data consumption – 3CX Server side .....	4
3. Configuration .....	5
3.1 3CX Webclient .....	5
3.1.1 Prerequisites .....	5
3.1.2 Server side.....	5
3.1.3 Client side.....	7
3.2 3CX Softclient .....	9
3.2.1 Prerequisites .....	9
3.2.2 Server side.....	9
3.2.3 Client side.....	10
3.3 3CX SBC .....	15
3.3.1 Prerequisites .....	15
3.3.2 Server Side .....	15
3.3.3 Client Side .....	16
3.4 3CX Mobile client .....	23
3.4.1 Prerequisites .....	23
3.4.2 Server Side .....	23
3.4.3 Client side.....	23
3.5 Remote connection using STUN.....	26
3.5.1 Prerequisites .....	26
3.5.2 Preparing the RPS server.....	26
3.6 Remote connection using manual provisioning.....	31
3.6.1 Prerequisites .....	31
3.6.2 Server side.....	31
3.6.3 Client side.....	32
4. Using the 3CX Web-Client with Jabra headset.....	33
4.1 General.....	33
4.1 Preparation: .....	33
4.2 Option 1: .....	35
4.2.1 Step 1: .....	35

4.2.2 Step 2: .....	35
4.2.3 Step 3: .....	35
4.2.4 Step 4: .....	36
4.3 Option 2: .....	37

## 2. General preparation

### 2.1 Prerequisites

To have these solutions implemented properly the following points should be followed;

- Proper port preservation/port forwarding setup for all the required ports (**SIP (Default Port 5060)**, **RTP (Default 9000-10999)**, **Tunnel (Default 5090)** and **HTTPS (Default 5001)**) on the firewall on the 3CX-Server side.
  - If using STUN or manual provisioning a configurable firewall must be on the remote end.
  - If the 3CX is on premise and remote workers also must access the LAN in the Office, ensure that there is enough bandwidth on the WAN connection of the office side.
  - Setup 3CX on an OS you are familiar with.
  - Ensure that QoS is enabled on all necessary network components
  - SIP ALG is **disabled** on any possible border device (Router/Firewall) on the server side!

### 2.2 Data consumption – 3CX Server side

Having remote extensions, creates an additional layer of traffic that you would not experience if extensions were in the same office. For example calls between local extensions will now take extra bandwidth as they will be traversing over the internet.

Please find the data usage on 3CX with different codecs:

- <https://www.3cx.com/blog/docs/bandwidth-utilised-for-voip/>
- <https://www.3cx.com/blog/docs/bandwidth-dsl-atm-isp/>

Additional traffic will also be generated by using SIP-Notify messages on port 5001 for BLF keys.

- ➔ The more extensions that use BLF, the more SIP-Notify traffic is generated
- ➔ The more BLF keys every single extension uses, the more SIP-Notify traffic is generated

## 3. Configuration

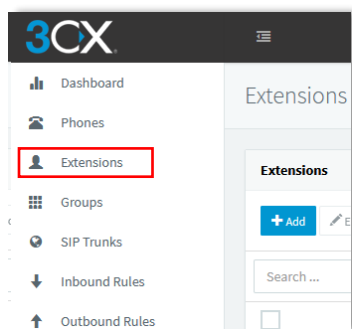
### 3.1 3CX Webclient

#### 3.1.1 Prerequisites

- Port forwarding on the firewall is implemented and configured properly on the 3CX server side.
- Chrome is default browser on clients.
- Corded or cordless headset configured as main audio device on the remote computer.

#### 3.1.2 Server side

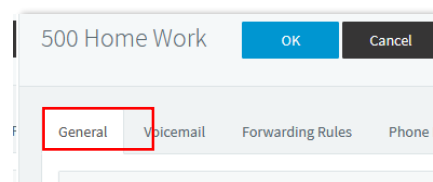
By default, every extension has Webclient enabled. To ensure it is enabled go on the Navigation pane to **Extensions – mark the Ext. – General tab** – scroll down to **‘Web Authentication’** – Tick **‘Enable Web Client’**



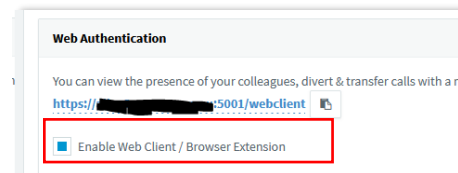
Click on the extension



Choose the **‘General’** tab



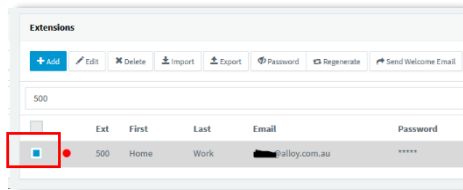
Scroll down to **‘Web Authentication’** and ensure **‘Enable Web Client’** is ticked.



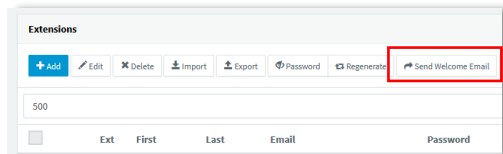
Also make sure that every extension that should receive the Webclient login has an e-mail address inside the **‘User Information’** under the **‘General’** tab inside the extension.

Once this is all checked and confirmed, simply choose either all extensions from the top of the list or only the ones that need the credentials and choose **‘Send Welcome Email’**.

Highlight the extension



Choose '**Send Welcome Email**'



The users credentials will be sent now to the e-mail address entered inside the extension.

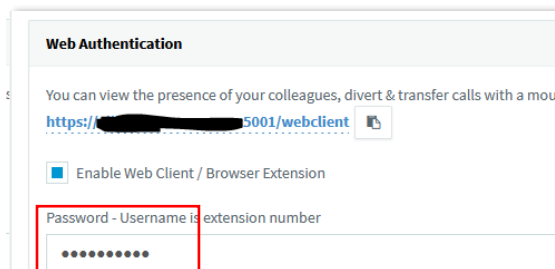
The welcome e-mail contains the following information:

- Config-file for the 3CX Softclient
- QR code for the 3CX mobile client
- Number of the extension
- Personal VM PIN
- Number of the VM System
- 3CX Webclient login link and credentials
- Link for the Chrome 'click2call' plugin
- Links to download the Softclient and Mobile client

*Optional: Password change*

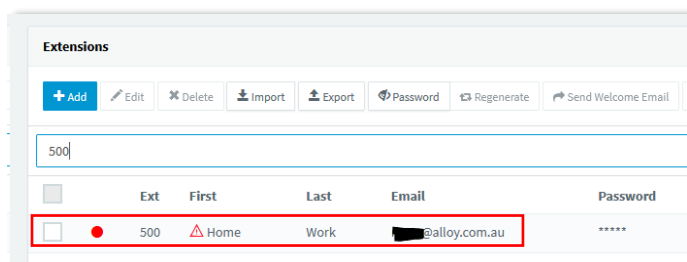
In the '**Password**' field a random password is entered by default. This can be found in the welcome e-mail.

However, a new password can be entered there.

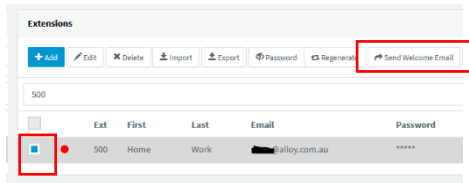


If you enter a new password, make sure the password is strong enough!

Once done, scroll to the extension or search for it by entering the extension number, highlight the extension



and press 'Send Welcome Email'. A welcome mail with the ne login credentials will be sent to the user.

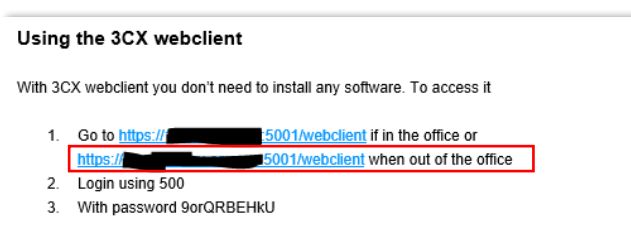


### 3.1.3 Client side

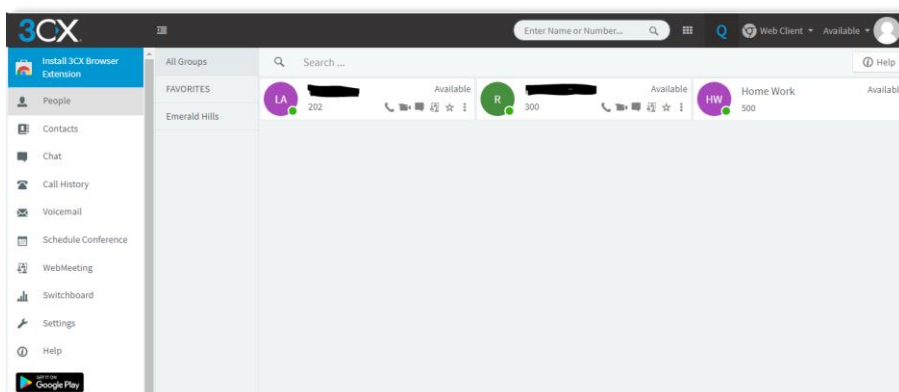
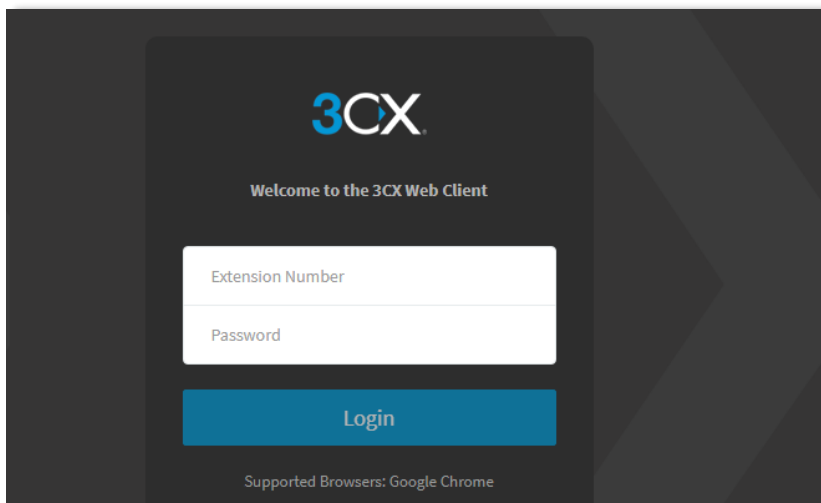
The e-mail has been successfully received by the user.

Open the email and scroll to '**Using the 3CX Webclient**'.

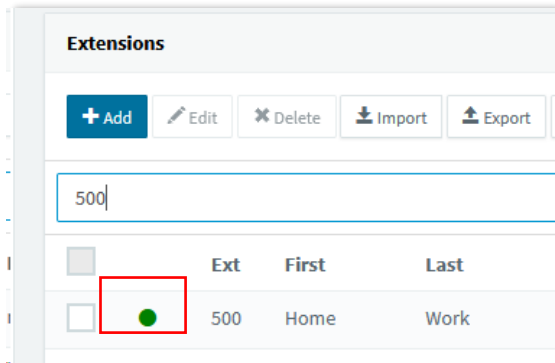
Click on the 2<sup>nd</sup> link 'when out of office' that contains the FQDN.



Enter the extension number and the password from the welcome e-mail.



In the 3CX Management console we can see the extension now as being registered.



Detailed description on how to use the Webclient can be found in the Alloy 3CX Webclient user guide. To view the 3CX Webclient user guide please click [here](#).



## 3.2 3CX Softclient

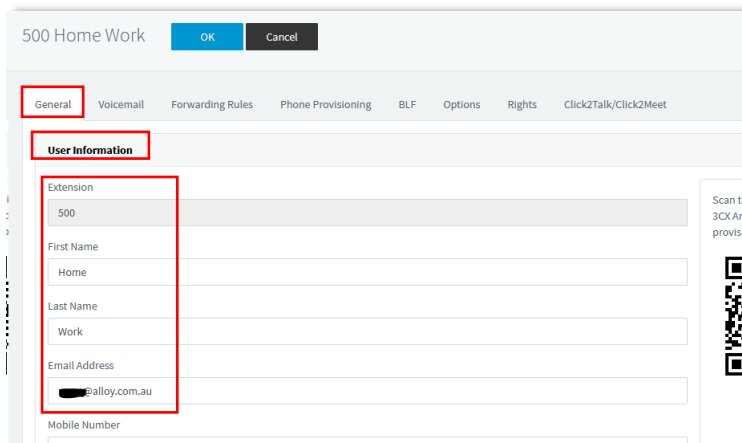
### 3.2.1 Prerequisites

- Port forwarding is setup on the firewall properly on the 3CX server side.
- Corded or cordless headset configured as main audio device on the computer.

### 3.2.2 Server side

**By default, every extension has the Softclient pre-configured by already.**

All that needs to be setup is the email address inside the **'User Information'** under the **'General'** tab inside the extension.



500 Home Work

OK Cancel

General Voicemail Forwarding Rules Phone Provisioning BLF Options Rights Click2Talk/Click2Meet

**User Information**

Extension: 500

First Name: Home

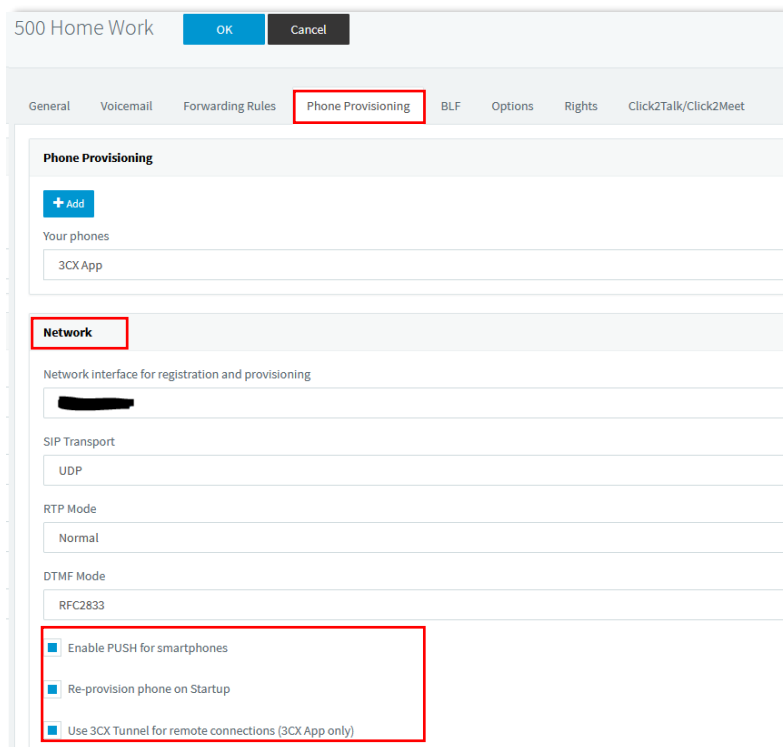
Last Name: Work

Email Address: 500@alloy.com.au

Mobile Number:

Scan the 3CX App QR code to provision

Then head over to the **'Phone Provisioning'** tab and ensure under **'Network'** all boxes are ticked: **'Enable PUSH for smartphones'**, **'Re-provision phone on Startup'** and **'Use 3CX Tunnel for remote connections (3CX App only)'**



500 Home Work

OK Cancel

General Voicemail Forwarding Rules **Phone Provisioning** BLF Options Rights Click2Talk/Click2Meet

**Phone Provisioning**

+ Add

Your phones

3CX App

**Network**

Network interface for registration and provisioning

SIP Transport: UDP

RTP Mode: Normal

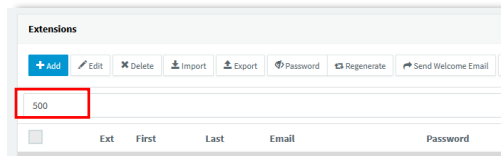
DTMF Mode: RFC2833

☒ Enable PUSH for smartphones

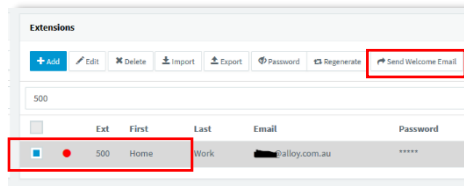
☒ Re-provision phone on Startup

☒ Use 3CX Tunnel for remote connections (3CX App only)

Once this is all checked and confirmed, simply choose either all extensions from the top of the list or only the ones that need the credentials



and choose 'Send Welcome Email'.



The users credentials will be sent now to the e-mail address entered inside the extension.

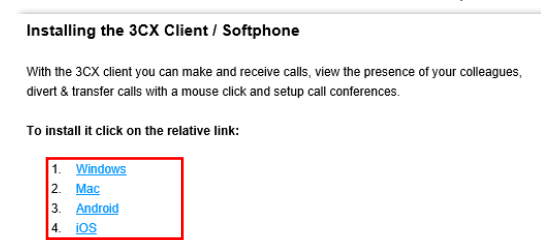
The welcome e-mail contains the following information:

- Config-file for the 3CX Softclient
- QR code for the 3CX mobile client
- Number of the extension
- Personal VM PIN
- Number of the VM System
- 3CX Webclient login link and credentials
- Link for the Chrome 'click2call' plugin
- Links to download the Softclient and Mobile client

### 3.2.3 Client side

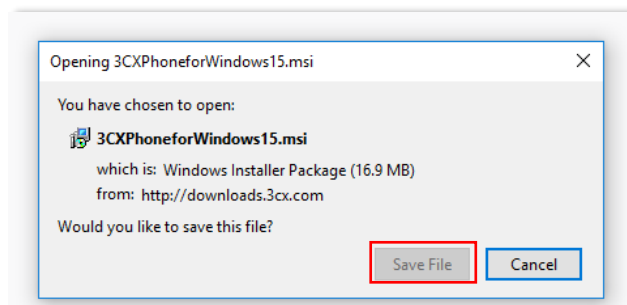
The e-mail has been successfully received by the user.

Open the email and scroll to '**Installing the 3CX Client/Softphone**' and click on the correct link, f.e. Windows and save the file on the computer.

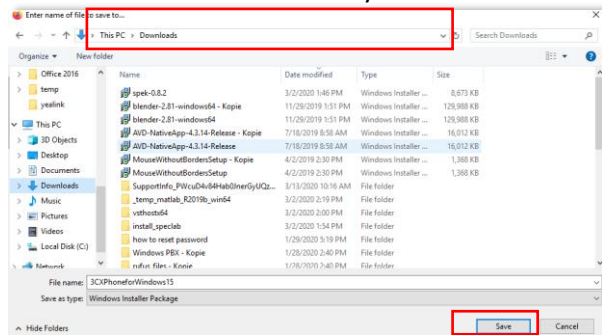


Once the link is clicked the file download starts.

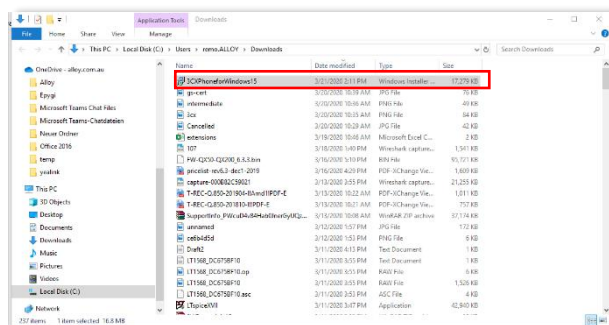
Choose '**Save File**'



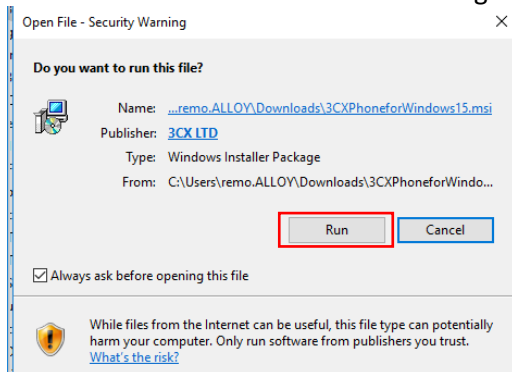
Choose the download directory and hit 'Save'



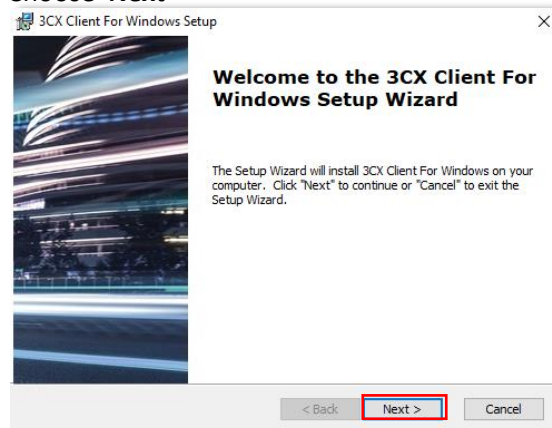
Open the containing folder and find the downloaded file.



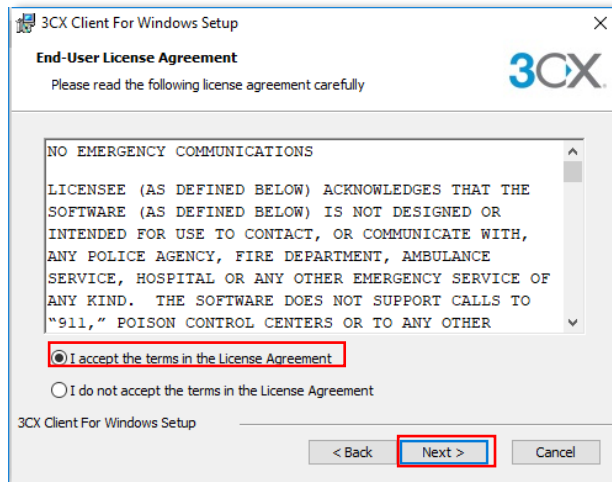
Double click on the installation file or right click on it and choose 'Install' and then click 'Run'.



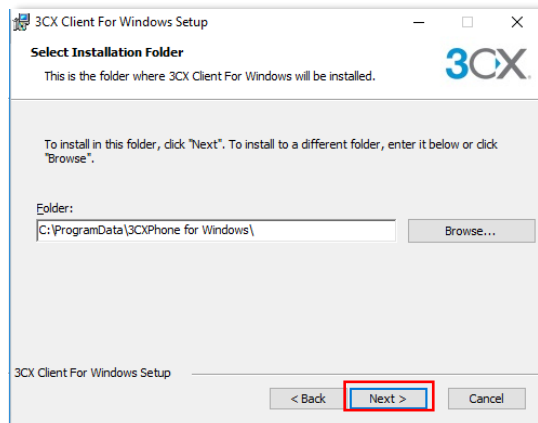
Choose 'Next'



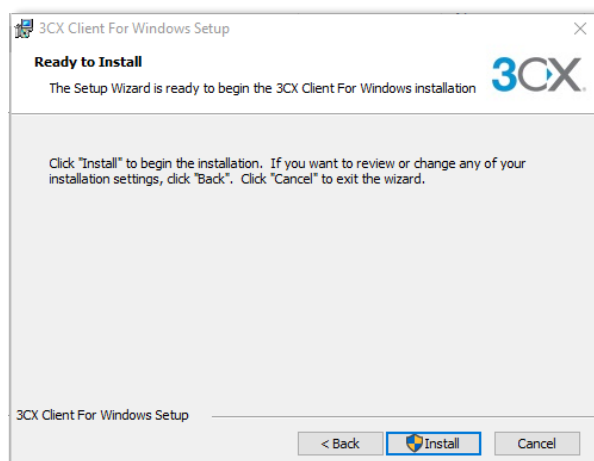
Accept '**Terms and Conditions**' and click '**Next**'.



Keep the installation path and choose '**Next**'.

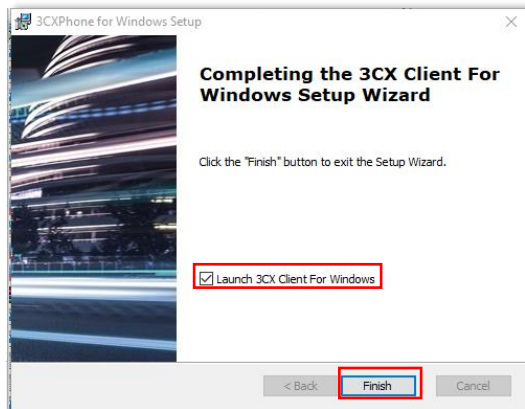


Then choose '**Install**'.

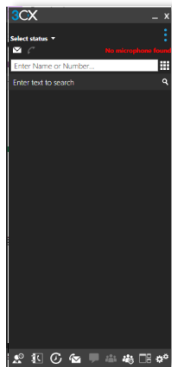


Accept the 'User Account Control' from Windows with Yes.

Leave '**Launch 3CX Client for Windows**' ticked and click '**Finish**'.

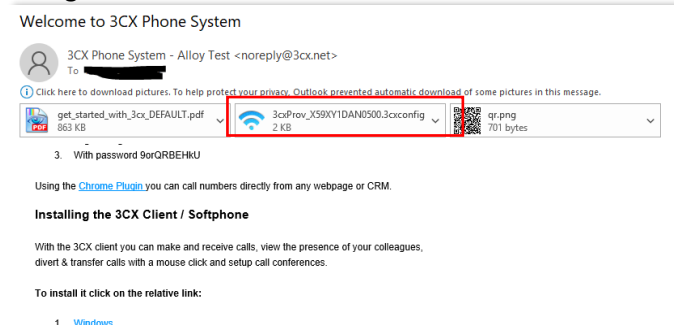


The client was installed successfully.

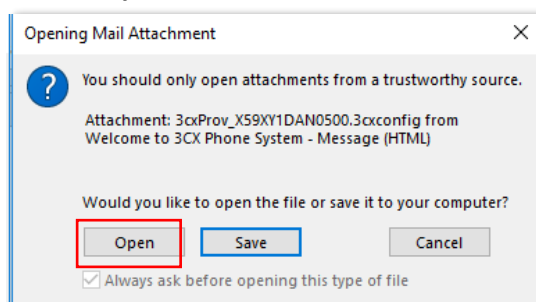


➔ If you are asked to install an update from the phone system accept with Yes/ok.

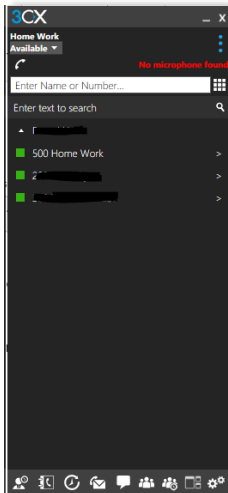
Now go back to the welcome e-mail and double click on the '**3CX config file**'.



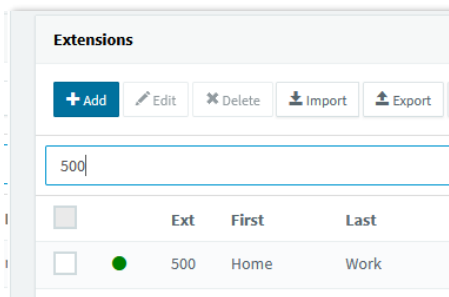
Choose '**Open**'.



The file is opened with the 3CX Softclient.  
The Softclient gets provisioned and is registered automatically.



In the 3CX Management console we can see the extension now as being registered



Detailed description on how to use the Softclient can be found in the following userguides:

- [Windows](#)
- [Mac](#)

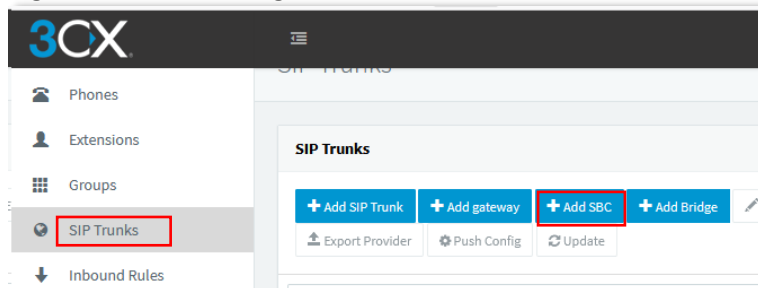
## 3.3 3CX SBC

### 3.3.1 Prerequisites

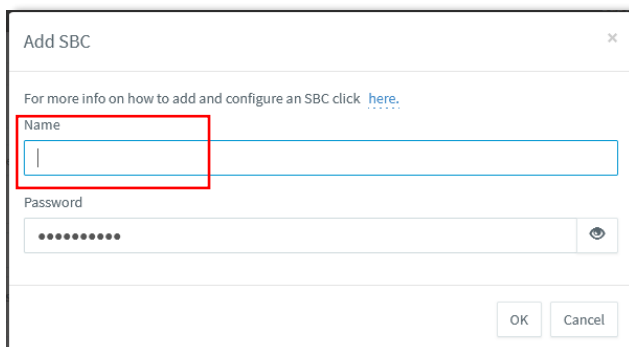
- Port forwarding is setup on the firewall properly on the 3CX server side.
- Single/unused Windows10 computer or supported raspberry Pi with supported hardware Specifications. Link here : [Hardware specifications](#)
- IP Deskphone on remote site

### 3.3.2 Server Side

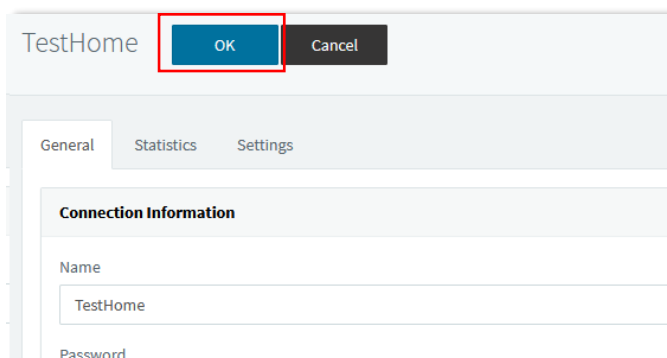
Log into the 3CX Management Console, '**SIP Trunks**' and choose '**Add SBC**'.



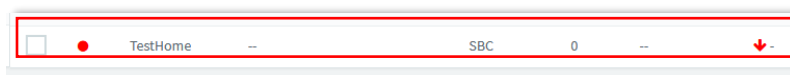
Enter a '**Name**' for the SBC



Choose '**OK**' to save the SBC



On the Trunk overview we can see now the SBC as 'Down'.



Go back into the configuration and keep the window open, as certain information will be needed.  
Now we log into the remote machine:

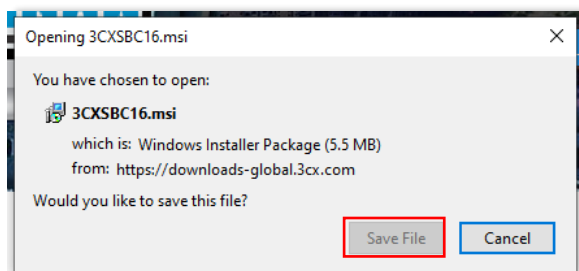
### 3.3.3 Client Side

#### 3.3.3.1 Installing and connecting the SBC

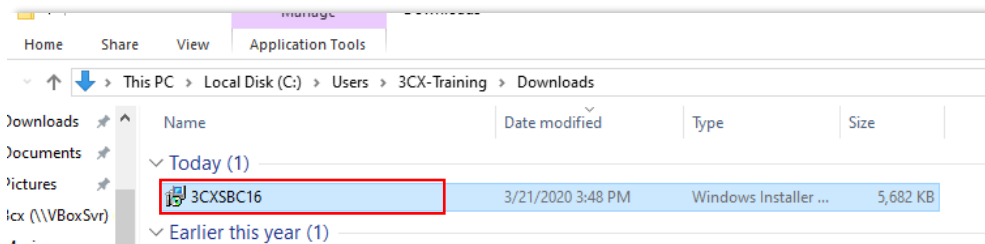
Open this [link](#) to come to the download page of 3CX to download the 3CX SBC unto the remote machine.



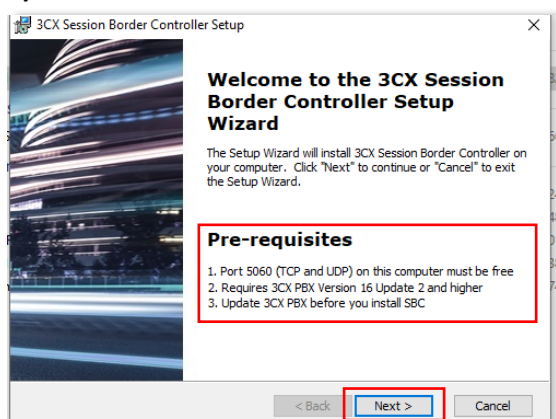
Choose '**Save File**'



Open the file location

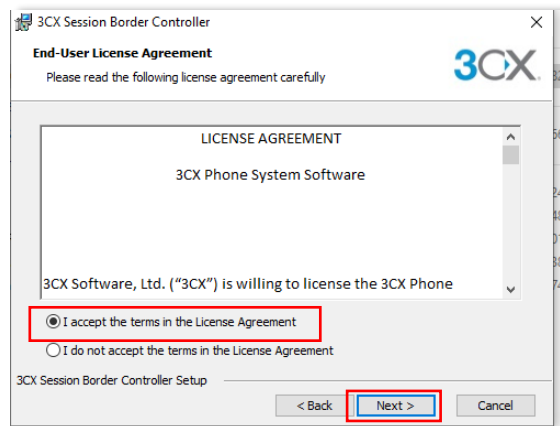


Double click on the installation file or right click on it and choose 'Install', read the lined-out '**Pre-requisites**' and then click '**Next**'.

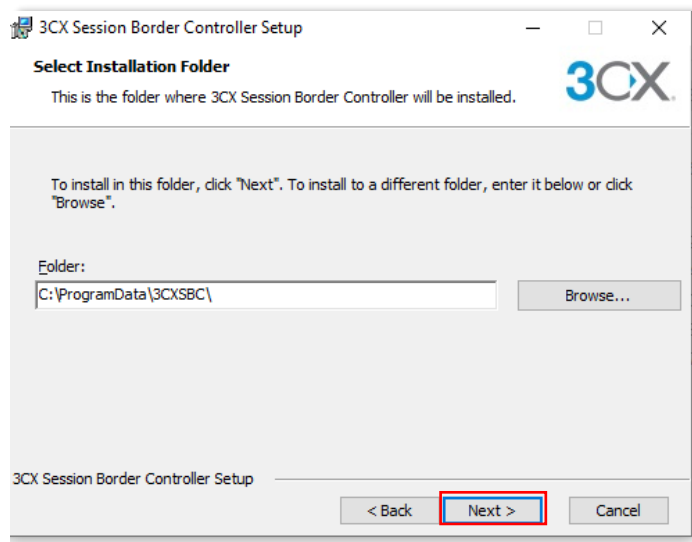




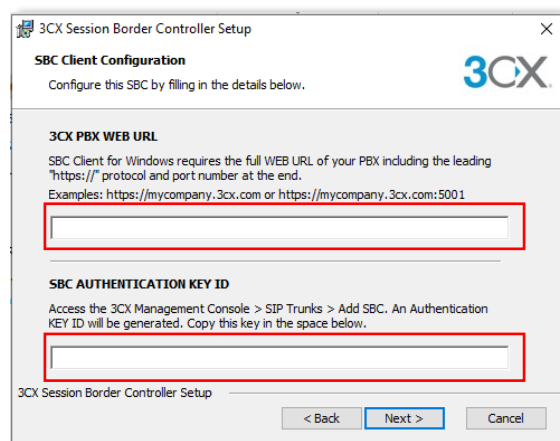
Accept the '**Terms and Conditions**' and choose '**Next**'.



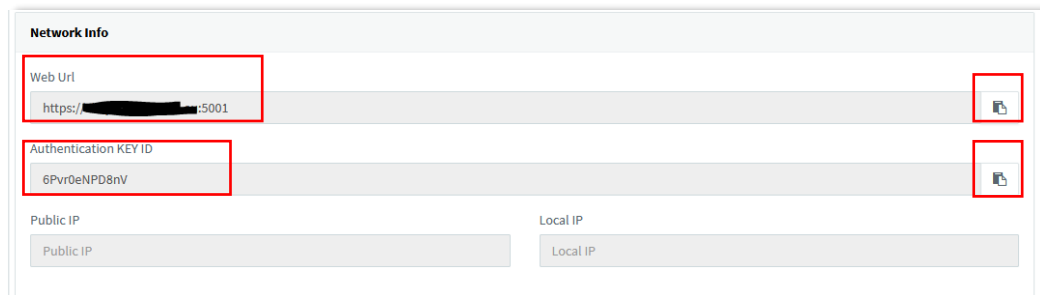
Keep the install path and choose '**Next**'.




Now enter the values from the 3CX Management console into these fields.




Copy the '**Web URL**' incl. Port and '**Authentication KEY ID**' with the help of the copy icons on the right.



**Network Info**

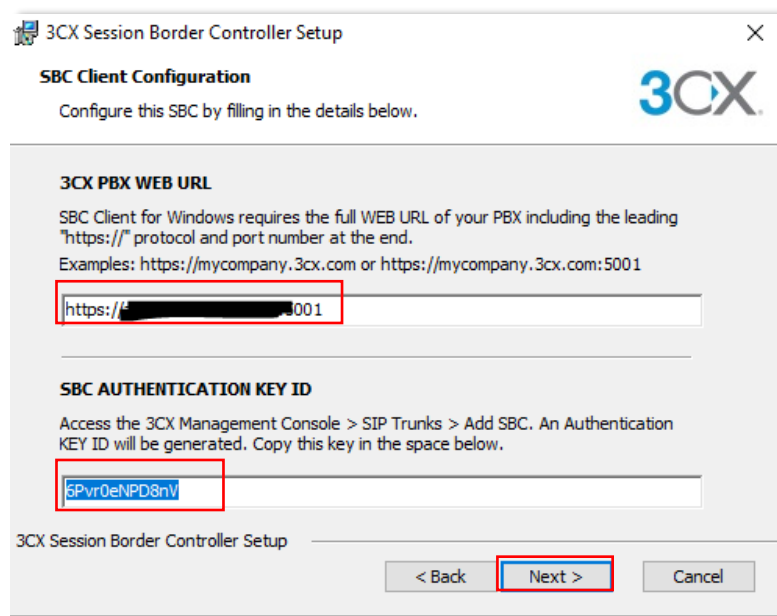
Web Url  
https://[redacted]:5001 

Authentication KEY ID  
6Pvr0eNPD8nV 

Public IP  
Public IP

Local IP  
Local IP

Once done confirm with '**Next**'.



**3CX Session Border Controller Setup**

**SBC Client Configuration**

Configure this SBC by filling in the details below.

**3CX PBX WEB URL**

SBC Client for Windows requires the full WEB URL of your PBX including the leading "https://" protocol and port number at the end.  
Examples: https://mycompany.3cx.com or https://mycompany.3cx.com:5001

https://[redacted]:5001

**SBC AUTHENTICATION KEY ID**

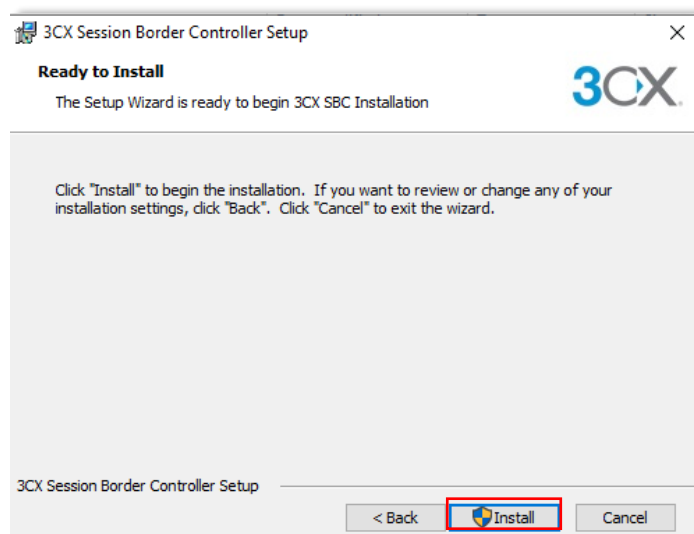
Access the 3CX Management Console > SIP Trunks > Add SBC. An Authentication KEY ID will be generated. Copy this key in the space below.

6Pvr0eNPD8nV

3CX Session Border Controller Setup

< Back **Next >** Cancel

Now choose '**Install**' and accept the 'User Account Control' from Windows with Yes.



**3CX Session Border Controller Setup**

**Ready to Install**

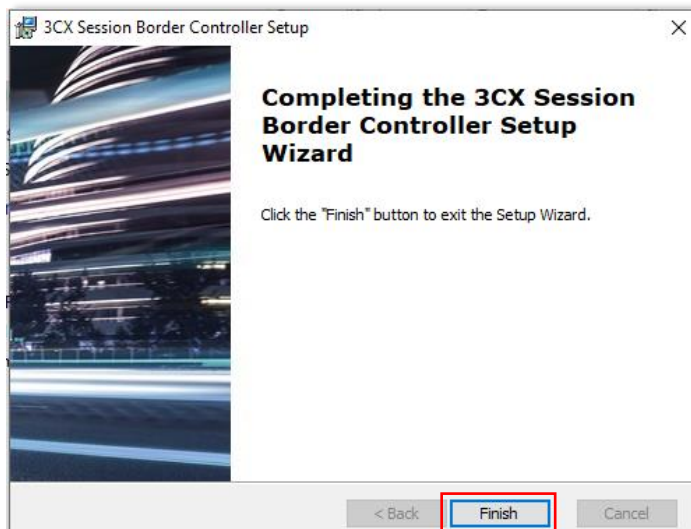
The Setup Wizard is ready to begin 3CX SBC Installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

3CX Session Border Controller Setup

< Back **Install** Cancel

Then click on '**Finish**'.



Done!

Now we can check the status of the SBC from the SIP Trunk list and can see the Trunk is already up.

<input type="checkbox"/>	<span style="color: green;">●</span>	TestHome	124.148.172.96	SBC	0	Version: 16.0.390	<span style="color: green;">↑</span> 2 min	03/21/2020 4:05:25 PM	--
--------------------------	--------------------------------------	----------	----------------	-----	---	-------------------	--	-----------------------	----

### 3.3.3.2 Adding the remote Phone

- The following steps are done once the IP-Phone is plugged into the remote network.

We go back into the SBC connection and note down the local IP of the SBC, in our case 192.168.75.112

Network Info

Web Url

https://[REDACTED]:5001

Authentication KEY ID

6Pvr0eNPD8nV

Public IP

[REDACTED]

Local IP

192.168.75.112

We choose the extension we want to configure.

Extensions

+ Add

Edit

Delete

Import

Export

Password

Regenerate

Se

501

	Ext	First	Last	Email	Password
<input type="checkbox"/>	501	Home	Work		*****

Inside the extension we choose the '**Phone Provisioning**' tab.

501 Home Work OK Cancel

General Voicemail Forwarding Rules **Phone Provisioning** BLF Options

Under '**IP Phone**' we change the '**Provisioning Method**' to '**3CX SBC**' and enter the LAN IP of the SBC, in our case 192.168.75.112 and save.

**IP Phone**

Provisioning Method  
3CX SBC (remote)

Provisioning Link: [https://\[redacted\]01/provisioning/mwyh9j00lbu38u](https://[redacted]01/provisioning/mwyh9j00lbu38u)

Mac Address  
001565 [redacted]

Select Interface  
[redacted]

3CX Session Border Controller  
192.168.75.112

Now the IP Phone must be factory reset:

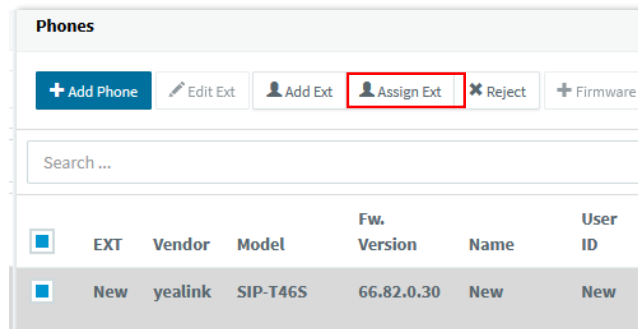
How-to

- [Yealink](#)
- [Snom](#)
- [Grandstream](#)

Once Factory defaulted the phone appears inside the phones node with as a bold entry.

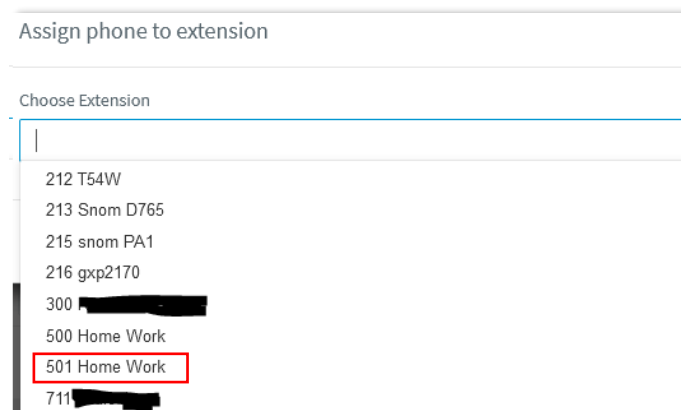
<a href="#">+ Add Phone</a> <a href="#">Edit Ext</a> <a href="#">Add Ext</a> <a href="#">Assign Ext</a> <a href="#">Reject</a> <a href="#">Firmware</a> <a href="#">Reboot</a> <a href="#">Reprovision</a> <a href="#">Phone UI</a> <a href="#">Password</a> <a href="#">+ Config</a>											
Search ...											
<input type="checkbox"/>	EXT	Vendor	Model	Fw. Version	Name	User ID	Password	Phone pwd	PIN	IP	MAC
<input type="checkbox"/>	New	yealink	SIP-T28P	2.73.0.50	New	New	New	New	New	192.168.75.81:5059 via SBC 192.168.75.112:5060	0015
<input type="checkbox"/>	New	yealink	SIP-T22P	7.73.0.50	New	New	New	New	New	192.168.75.80:5059 via SBC 192.168.75.112:5060	0015
<input type="checkbox"/>	New	yealink	SIP-T48G	35.81.0.110	New	New	New	New	New	192.168.75.83:5059 via SBC 192.168.75.112:5060	0015
<input type="checkbox"/>	New	yealink	SIP-T46S	66.82.0.30	New	New	New	New	New	192.168.75.82:5059 via SBC 192.168.75.112:5060	0015

Highlight the required phone and choose '**Assign Ext**'.



EXT	Vendor	Model	Fw. Version	Name	User ID
New	yealink	SIP-T46S	66.82.0.30	New	New

Assign the phone to its original extension, in this case '501'.

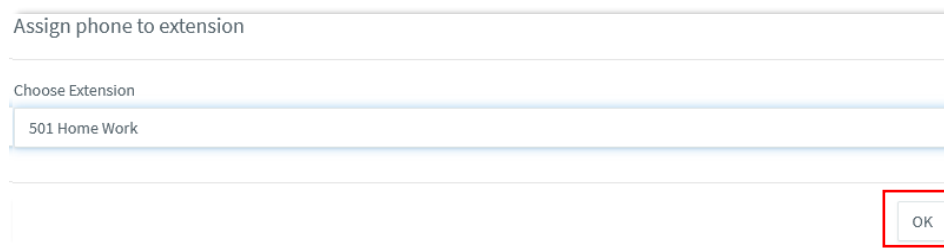


Assign phone to extension

Choose Extension

- 212 T54W
- 213 Snom D765
- 215 snom PA1
- 216 gxp2170
- 300 [REDACTED]
- 500 Home Work
- 501 Home Work**
- 711 [REDACTED]

Then click '**OK**'.



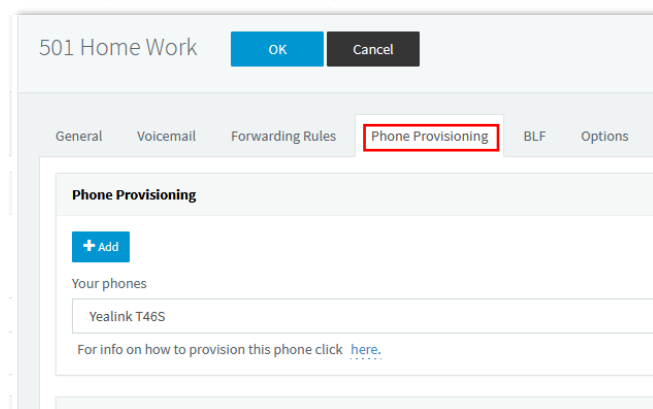
Assign phone to extension

Choose Extension

501 Home Work

OK

The '**Phone Provisioning**' tab opens automatically and lets you choose the settings, change if there is need to (f.e. Timezone, etc.).



501 Home Work

OK Cancel

General Voicemail Forwarding Rules **Phone Provisioning** BLF Options

**Phone Provisioning**

+ Add

Your phones

- Yealink T46S

For info on how to provision this phone click [here](#).

Then choose the '**Options**' tab, scroll down to '**Troubleshooting**' and ensure '**PBX Delivers Audio**' is **unticked** and save.



**Troubleshooting**

Potentially overcome compatibility issues with old/incompatible phones with these options

☐ PBX Delivers Audio

The phone receives the provisioning information and depending on the model either reboots or directly takes over the new settings.

After a few moments the phone is up and running. *(If it was previously used on the same system, it should not line out that it has the wrong firmware!)*

<input type="checkbox"/>	501	Yealink	SIP-T46S	Not Supported 66.82.0.30	Home Work	*****	*****	*****	7079	192.168.75.82:5060 via SBC 192.168.75.112:5060	 001565F59C89
<input type="checkbox"/>		501	Home	Work	*****						

The Deskphone can now be used as it would be inside the office network. Also in terms of maintenance.

## 3.4 3CX Mobile client

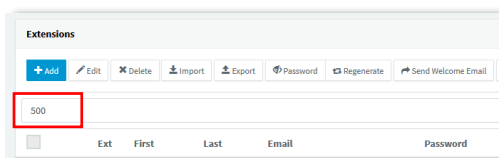
### 3.4.1 Prerequisites

- Port forwarding is setup on the firewall properly on the 3CX server side.
- Mobile device running iOS 13 and higher or Android 7 and higher
- App Store or Google Play Store account

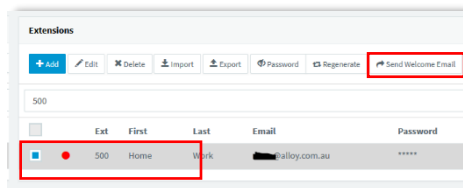
### 3.4.2 Server Side

All that must be done is setup the e-mail address inside the 'User Information' under the General tab inside the extension.

Once this is all checked and confirmed, simply choose either all extensions from the top of the list or only the ones that need the credentials



and choose 'Send Welcome Email'.



The users credentials will be sent now to the e-mail address entered inside the extension.

The welcome e-mail contains the following information:

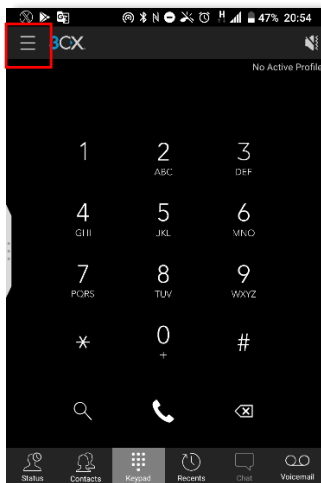
- Config-file for the 3CX Softclient
- QR code for the 3CX mobile client
- Number of the extension
- Personal VM PIN
- Number of the VM System
- 3CX Webclient login link and credentials
- Link for the Chrome 'click2call' plugin
- Links to download the Softclient and Mobile client

### 3.4.3 Client side

The e-mail has been successfully received by the user.

Now open the App Store on the mobile device and search for 3CX Android or 3CX iOS app. Click on it and press the 'Install' button.

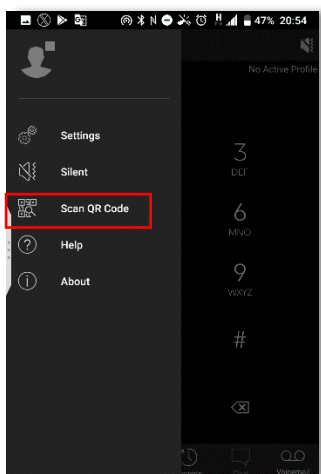
Once the app is installed open the app by clicking on the icon. The 3CX app opens. Choose the '**Menu**' top left.



Open the email and click on the **QR code**.

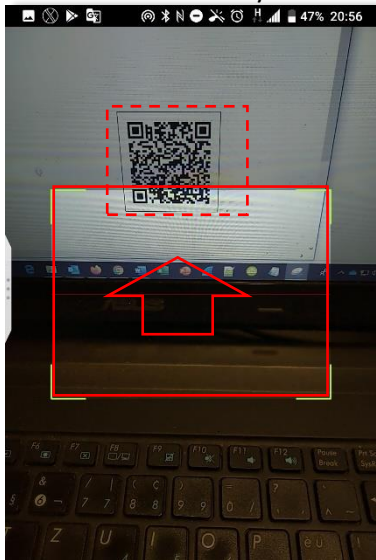


Inside the app choose 'Scan QR code'.

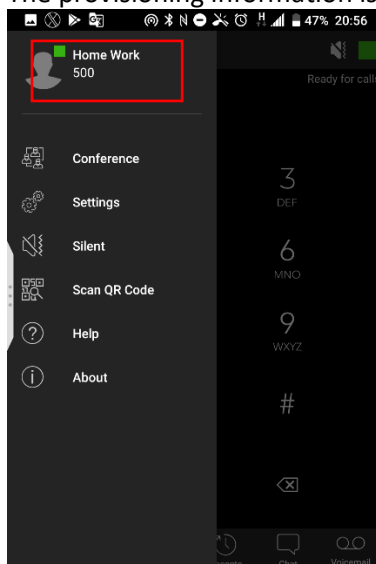




Hold the scanner fully over the QR Code displayed in the mail.



The provisioning information is retrieved and the client is configured.



Done!

Detailed description on how to use the Mobile client can be found in the following userguides:

- [iOS](#)
- [Android](#)

## 3.5 Remote connection using STUN

### 3.5.1 Prerequisites

- Port forwarding is setup on the firewall properly on the 3CX server side.
- SIP ALG is **disabled** on any firewall/router device on the remote side!
- If using port 5060 as a port for a remote device, ensure to lock 5060 down to the public IP of the 3CX server on the remote firewall, else 5060 will be attacked by hacking tools like 'Sipvicious'.
- Port forwarding is setup on the firewall properly on the remote extension side.
  
- The below conditions must be met for each remote phone on at the same location
  - Every remote phone uses a static IP address
  - Every remote phone uses a different SIP port. F.e. 5060, 5065, 5070, ...
  - Every remote phone uses a different RTP port range. f.e. 11000-11005, 11006-11010, ...
  - SIP and RTP port are mapped equally → Source port = outside port and they are forwarded to the static IP address of the matching device.

Using STUN provisioning we show the solution using Yealink RPS. To fully keep control over the remote device we advise to follow our steps as lined out:

### 3.5.2 Preparing the RPS server

#### 3.5.2.1 What is RPS

RPS (Remote Provisioning Server) from Yealink, GAPS from Grandstream or Snom Active are free provisioning services designed to dropship devices to the customer and have them auto configured upon first boot. All that is required is a free account to the respective service.

Free registration for Alloy resellers can be done:

- [Yealink RPS](#)
- [Snom Active](#)
- Grandstream GAPS → send request to: [support@alloy.com.au](mailto:support@alloy.com.au)

#### 3.5.2.2 How does it work

Upon every first boot (after factory default has been performed) the IP Phone contacts the RPS service to see if there is any provisioning information available. If there is no information available, the device skips this step and stays unprovisioned until it will be provisioned via another way.

If there is any data available the device downloads the available information, which is the link to the provisioning server, and downloads the provisioning information from the server.

The link between the device and the provisioning server is the devices' MAC-address that is entered on the RPS with the attached server link.

#### 3.5.2.3 3CX RPS vs own RPS

If an extension on 3CX is created and the 'Provisioning Method' is set to 'STUN' the MAC address of the device is registered along with the provisioning link for 2 weeks on 3CX' RPS account. After this the information will be removed automatically.

Now what happens if the device must be factory defaulted at some stage after these 2 weeks? The extension must be refreshed through the 3CX management console, to have the provisioning MAC and link sent again to the RPS server.

If the own RPS account is used, the MAC address and the assigned provisioning link will not be removed automatically and will stay untouched until changes are made. This means, after a factory

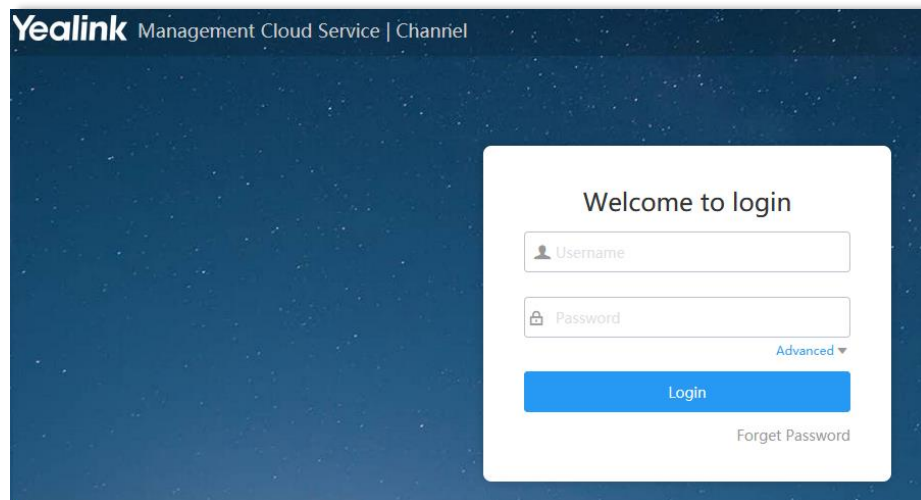
default of the device, the device will be able to retrieve auto provisioning information from the RPS server upon first boot and be up and running automatically in the shortest time.

We therefore strongly advise the following when using RPS provisioning:

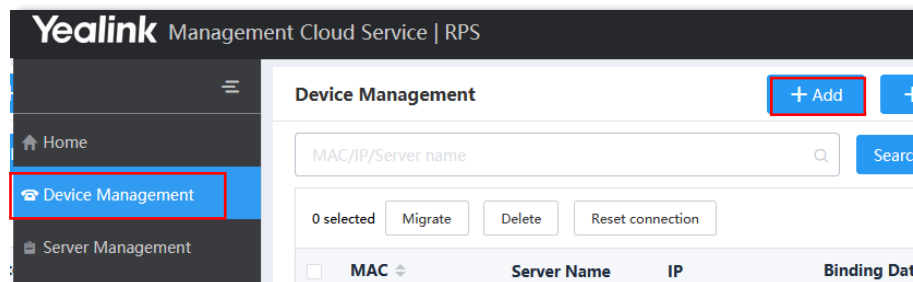
#### 3.5.2.4 Register device on RPS

Before we create an RPS extension, we register the device, the MAC address of the device, on our RPS account.

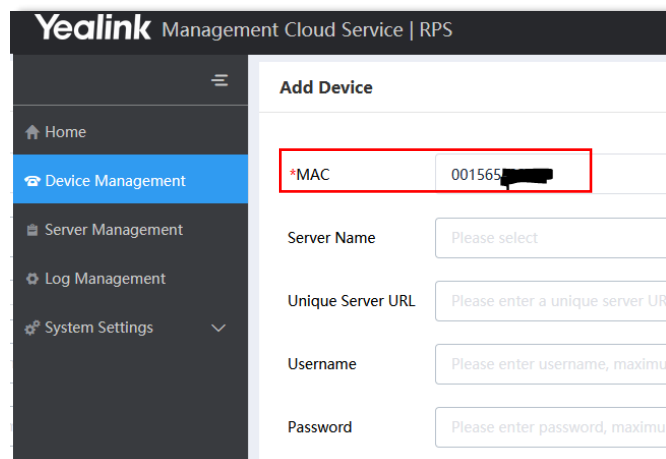
We go to <https://dm.yealink.com/reseller/login> and enter username and password.



Once logged in we choose '**Device Management**' and click on '**Add**'.

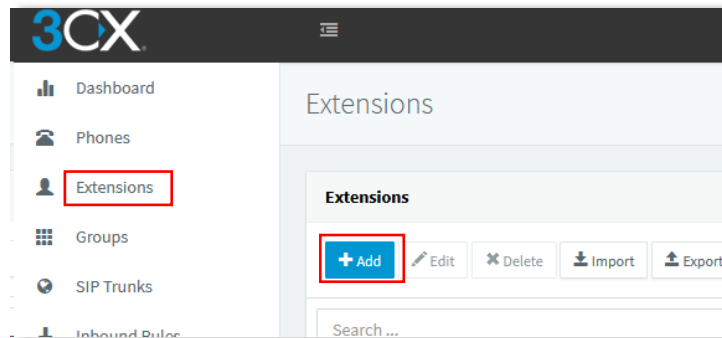


We just enter the **MAC** for this moment and click '**Save**'.

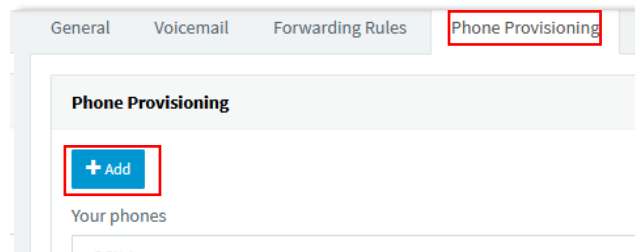


Now the device is bound to our RPS account and can't be used anymore from any other RPS account. We go to the Management Console of the 3CX and create a new extension.

### 'Extensions' – 'Add'



We enter the 'User Information' under the 'General' tab and go to the 'Phone Provisioning' tab and choose 'Add'.



We choose the phone model and enter the MAC address of this device and confirm.

Add Phone

Choose from available models

Yealink T48

Mac Address

001565

We choose the Provisioning Method 'Direct SIP'

IP Phone

Provisioning Method

Direct SIP (STUN - remote)

Note: For a device to work in Direct SIP (STUN - remote) mode, the setting in "Disallow u
unchecked. Uncheck this option before saving for this device to work.

Provisioning Link: https://001/provisioning/mwyh9j00lbu38u

And enter under '**Local SIP Port of Phone**' and '**Local RTP Port Start/End**' the values we have defined on the remote firewall for the device with the matching MAC address.

Local SIP Port of Phone	5065
Local RTP Audio Ports Start	14000
Local RTP Audio Ports End	14019

Further below we enter additional Information like Display language, Time zone, .... Once done we go to the '**Options**' tab and untick '**Disallow use of ....**'.

General	Voicemail	Forwarding Rules	Phone Provisioning	BLF	<b>Options</b>	Rights
<b>Restrictions</b>						
<input type="checkbox"/> Disable Extension						
<input type="checkbox"/> Disable External Calls						
<input type="checkbox"/> Enable PIN Protect For <input type="text" value="0"/> seconds						
<input checked="" type="checkbox"/> Disallow use of extension outside the LAN (Remote extensions using Direct SIP or STUN will be blocked)						

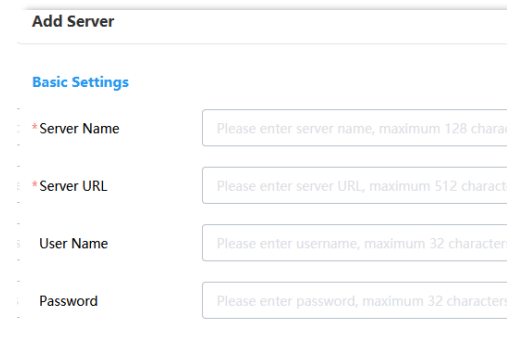
We go back to the '**Phone Provisioning**' tab and copy the provisioning link and press 'OK' at the top to save the extension.

<b>IP Phone</b>
Provisioning Method Direct SIP (STUN - remote)
Provisioning Link: <a href="https://[redacted]5001/provisioning/mwyh9j00lbu38u">https://[redacted]5001/provisioning/mwyh9j00lbu38u</a>

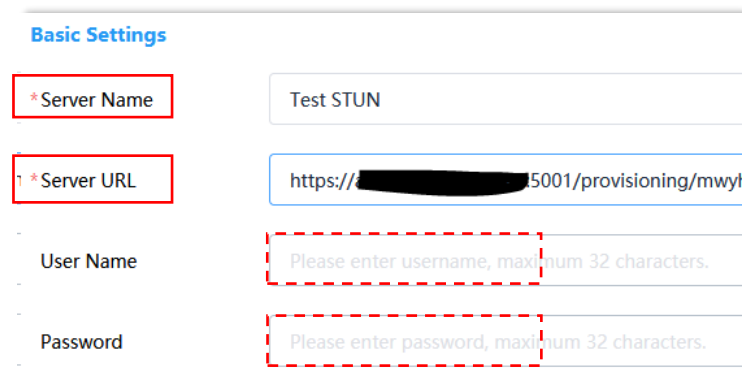
With this link copied we go now back to the RPS management platform and choose '**Server Management**' on the left side.

Home Device Management <b>Server Management</b>	<b>Device Overview</b> <div>12</div>
---	---


There we choose '**Add Server**'.



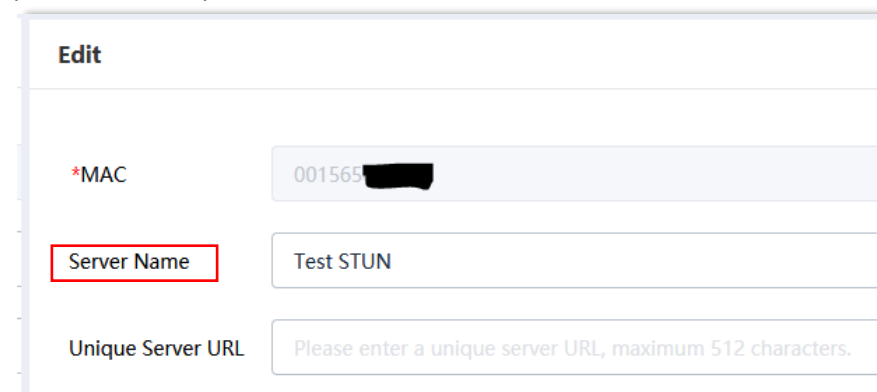
We enter a Server Name and the provisioning URL that we have copied from the 3CX. Additionally, we can enter a Username and password for higher security. The user will be asked to enter these values once the phone is connected to the server. When finished we 'Save'.



Go back to '**Device Management**' and click the '**Edit**' symbol on the right side of the matching MAC address.

<input type="checkbox"/>	MAC	Server Name	IP	Binding Date	Last Report Ti...	IP Status	Operation
<input type="checkbox"/>	001565 [redacted]	--	--	2020/03/21 22:5...	--	Unbound	

Under '**Server Name**' choose the Server that contains the link to the install you want to add this phone to. Then press '**Save**'.



The user can now plug in the factory defaulted device or factory default it in the remote network. The device will get the provisioning link, get provisioned and reboot.

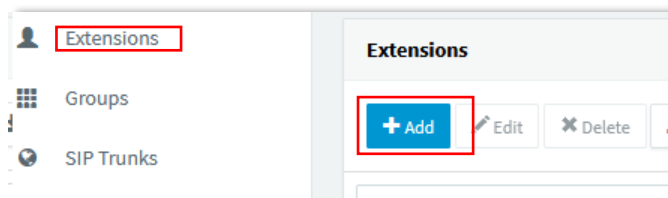
## 3.6 Remote connection using manual provisioning

### 3.6.1 Prerequisites

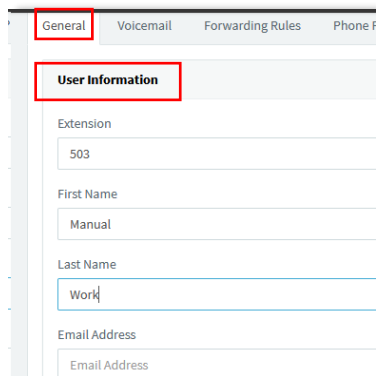
- Port forwarding is setup on the firewall properly on the 3CX server side.
- SIP ALG may or may not be enabled on the remote site. This depends on the situation.
- If using port 5060 as a port for a remote device, ensure to lock 5060 down to the public IP of the 3CX server on the remote firewall, else 5060 will be attacked by hacking tools like 'Sipvicious'.
- Port forwarding is setup on the firewall properly on the 3CX remote side.
- The below conditions must be met for each remote phone on at the same location
  - Every remote phone uses a static IP address
  - Every remote phone uses a different SIP port. F.e. 5060, 5065, 5070, ...
  - Every remote phone uses a different RTP port range. f.e. 11000-11005, 11006-11010, ...
  - SIP and RTP port are mapped equally → Source port = outside port and they are forwarded to the static IP address of the matching device

### 3.6.2 Server side

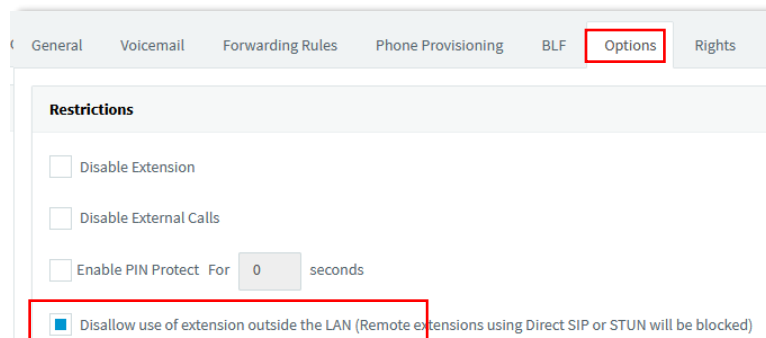
Log into the 'Management Console' of the 3CX, choose '**Extensions**' on the left and choose '**Add**'.



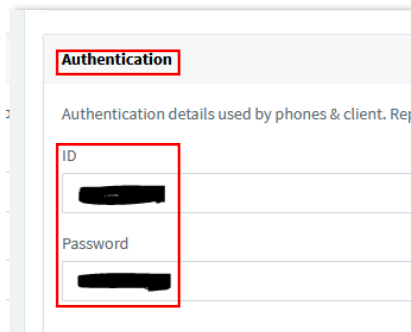
Enter all the necessary '**User Information**' (Extension number, First and Last name, ...) in the '**General**' tab.



Once done we go to the '**Options**' tab and untick '**Disallow use of ....**'. Choose 'OK' at the top.



Go back into the extension, '**General**' tab and scroll down to '**Authentication**' and either keep the tab like this or copy the values under '**ID**' and '**Password**' into a notepad.

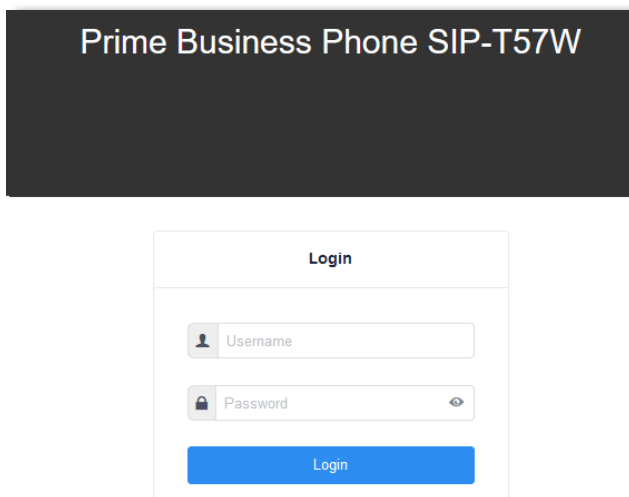


The screenshot shows the 'Authentication' tab with the following fields:

- ID**: [Redacted]
- Password**: [Redacted]

### 3.6.3 Client side

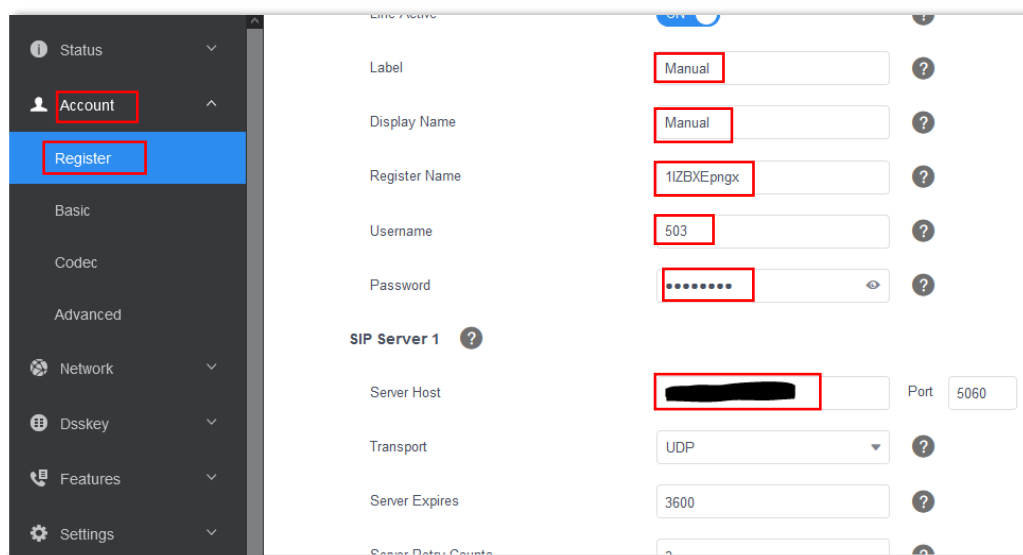
No log unto the client network and enter the phones' local IP into the browser



The screenshot shows the 'Prime Business Phone SIP-T57W' login screen. The 'Login' tab is selected, showing the following fields:

- Username**: [Redacted]
- Password**: [Redacted]
- Login** button

Login to the phone and choose '**Register**' under '**Account**' or the tab where the account settings are to be entered. Enter the values from the 3CX.



The screenshot shows the 'Register' tab with the following fields:

- Label**: Manual
- Display Name**: Manual
- Register Name**: 11ZBXEpngx
- Username**: 503
- Password**: [Redacted]
- SIP Server 1**: [Redacted]
- Port**: 5060
- Transport**: UDP
- Server Expires**: 3600

Confirm the changes and then setup the phone settings like keys, time zones, language, etc.



## 4. Using the 3CX Web-Client with Jabra headset

### 4.1 General

This section lines out which hardware and software should be used to successfully implement Jabra headsets with the 3CX Web-Client.

Mandatory software:

- Google Chrome browser
- 3CX Enterprise v.16

Advised Software:

- [Jabra Direct](#)

**We have tested this integration with 3CX professional v.16 and enterprise v.16. it seems to work with both versions.**

Tested hardware:

Jabra Pro 925: 925-15-508-208 **Not OK**

Jabra Pro 930: 930-29-509-103 **OK**

Jabra Pro 9450: 9450-25-507-103 **OK**

Jabra Engage 65: 9553-553-117 **OK**

Jabra Evolve 65: 6593-823-499 **OK**

Jabra Evolve 30: 5399-829-309 **OK**

This lines out that the Jabra Engage and Evolve series fully work with the 3CX Web-Client. As well as the Pro 930 and the Pro 94xx Series.

However, elder series like the Pro 920/925 won't work with that anymore.

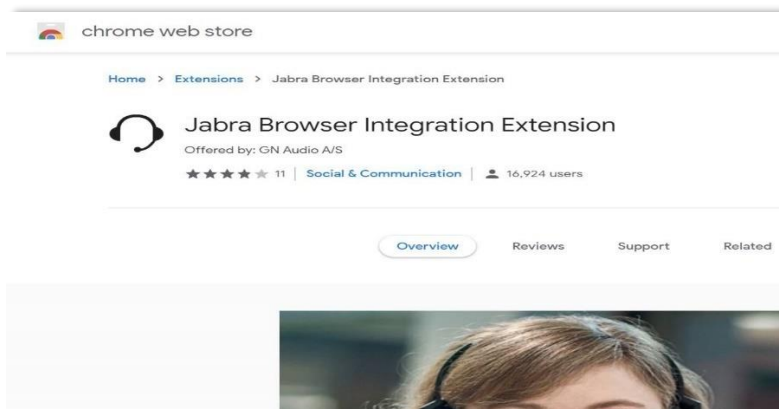
### 4.1 Preparation:

**To successfully integrate the Jabra headset into the 3CX Web-client please follow the steps below:**

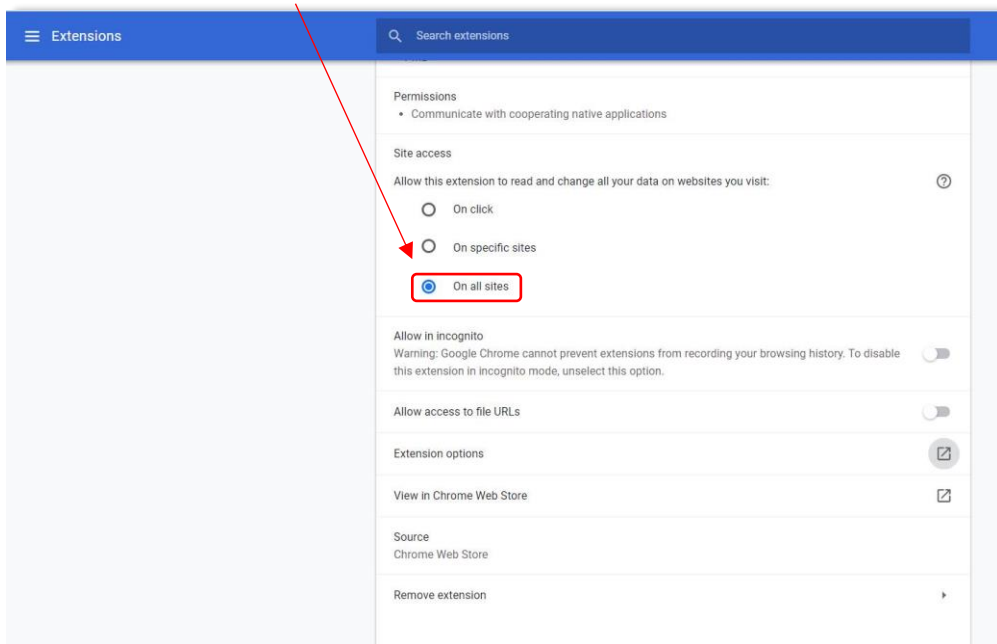
Download and install the Jabra Direct software from [here](#).

If necessary, perform a Firmware update through the Jabra Direct.

Open Chrome and search for '**Jabra Browser Integration Extension**' in Google, download and install it.



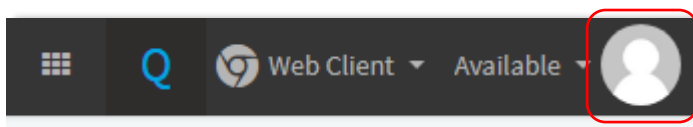
Let the extension access all sites:



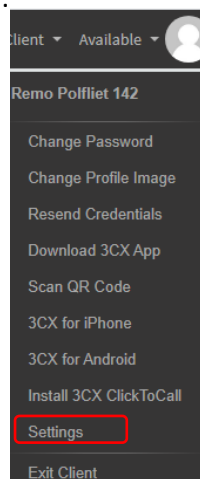
A headset now appears beside the address-bar in Chrome.



Log into the web-client and Click on the user icon top left



Once you click on the user icon a list comes down.  
Choose '**Settings**'.

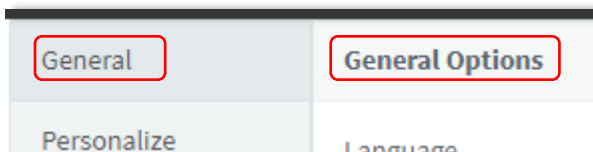


Now we come to 2 possible options. We have realized that there are 2 different settings possible. Based on what the browser shows different options is not known to us now.

## 4.2 Option 1:

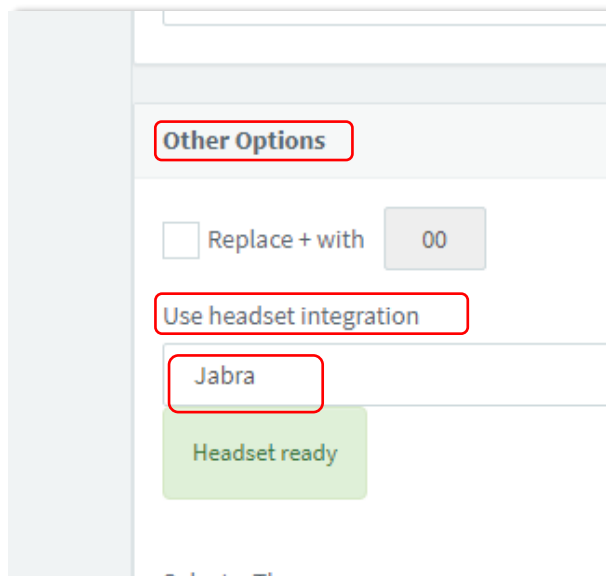
### 4.2.1 Step 1:

Inside '*Settings*' stay on the '**General**' node, '**General Options**' and scroll down.



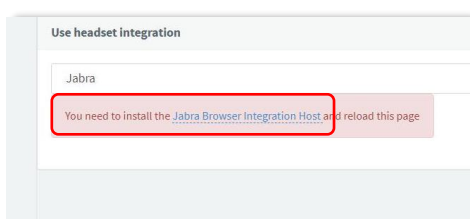
### 4.2.2 Step 2:

At the bottom you will find a section called '**Other Options**', under '**Use headset integration**' choose '**Jabra**'.



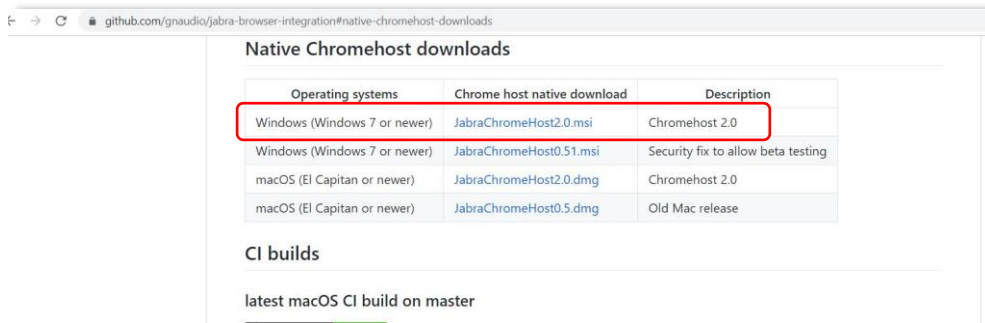
### 4.2.3 Step 3:

This will bring up a new message underneath that advises the install of the 'Jabra browser Integration Host'.



#### 4.2.4 Step 4:

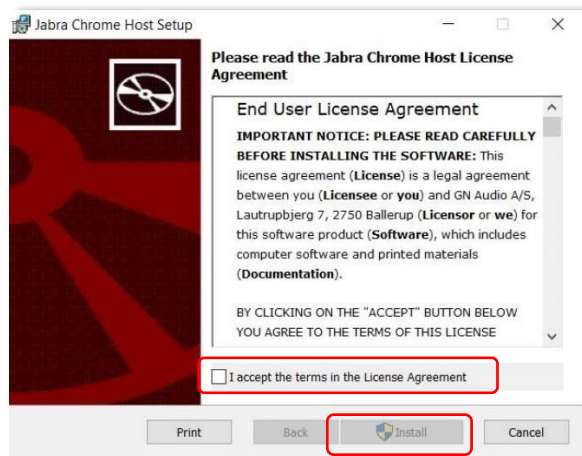
Right click on the link above and choose **'Open link in new Tab'**, choose the **'Chromehost 2.0'** file and install the file.



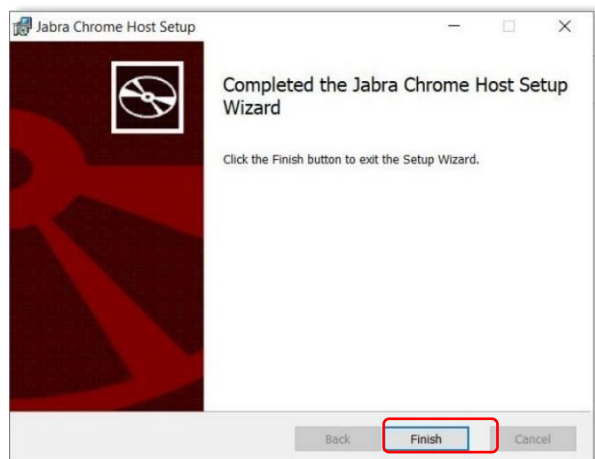
Save the file on the local machine and execute it.



Accept the **'Accept the Terms and Conditions'** and then choose **'Install'**.



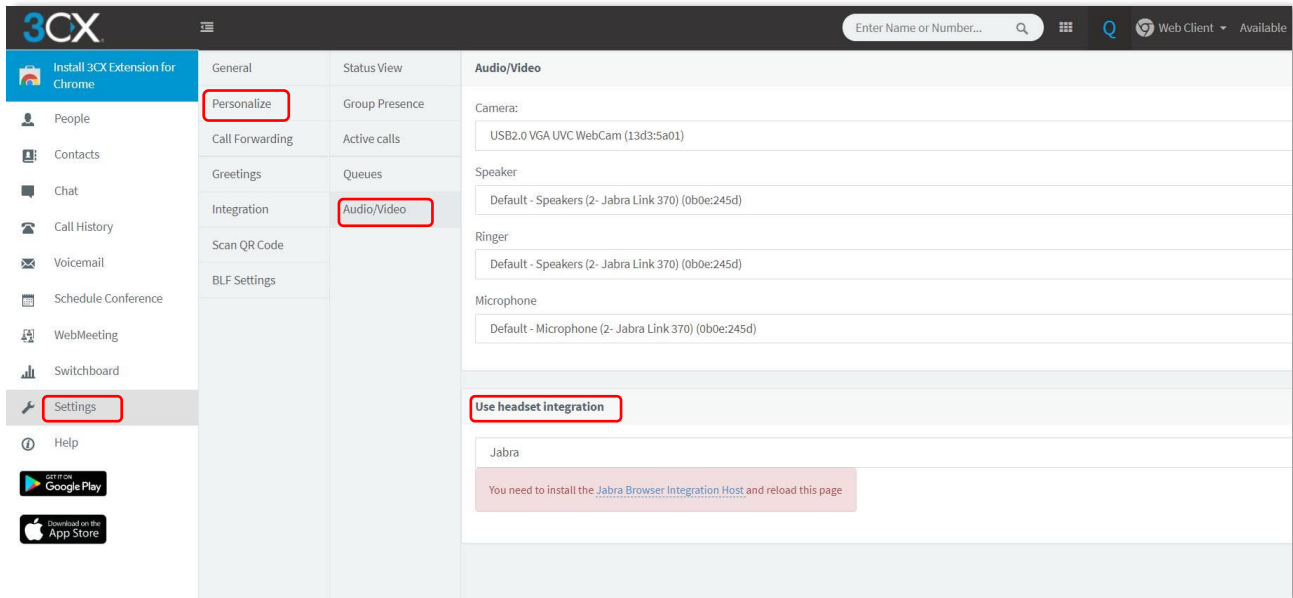
Once the installation is done, choose **'Finish'**



Now reload the 3CX web-client page and allow the Jabra plugin the requested access.

#### 4.3 Option 2:

While the first option must be enabled through the 'General' Node, the 2. Option can be enabled through **'Settings' – 'Personalize' – 'Audio/Video'**



After this follow the [Steps 2 – 4](#) from option 1.

If you have any additional questions or would like further support please contact Alloy on 03 862 9040 or via email at [support@alloy.com.au](mailto:support@alloy.com.au)