



SCS 4.0

Remote Worker Configuration

Task Based Guide

**Copyright © 2010 Avaya Inc.
All Rights Reserved.**

Notices

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>

Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/ LICENSEINFO/](http://support.avaya.com/LICENSEINFO/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER.

UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

<http://support.avaya.com/Copyright>.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support. Web site: <http://www.avaya.com/support>

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>

Copyright © 2010 ITEL, All Rights Reserved

The copyright in the material belongs to ITEL and no part of the material may be reproduced in any form without the prior written permission of a duly authorised representative of ITEL.

Table of Contents

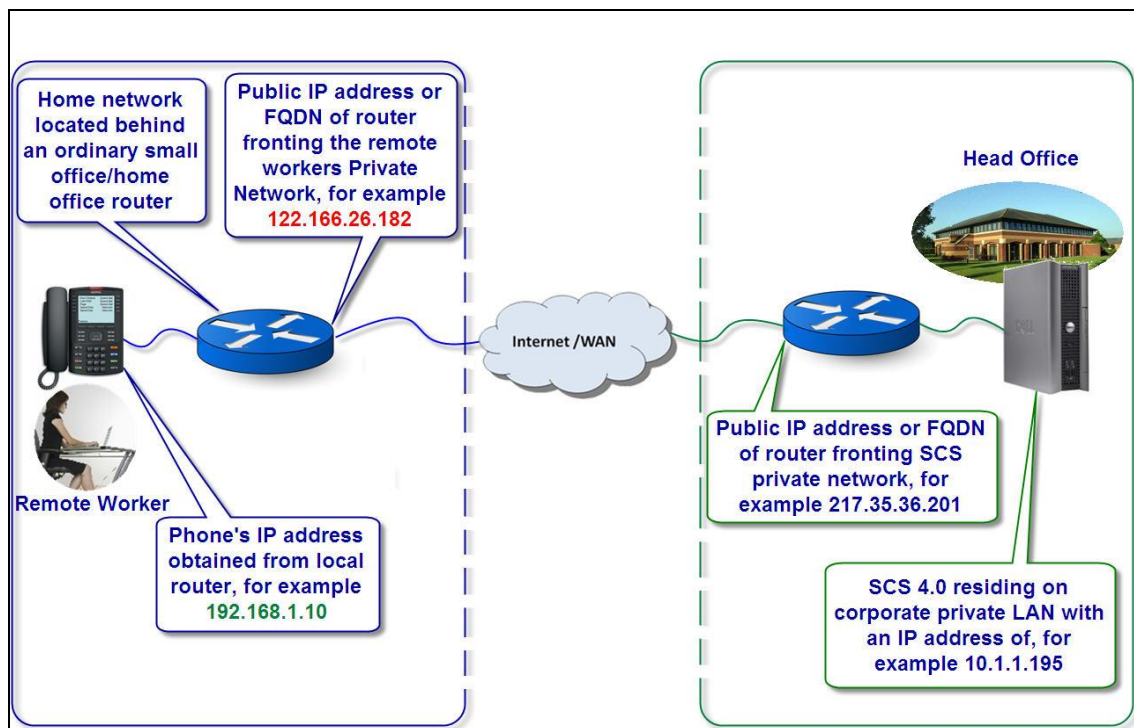
Overview	5
Network Topology Example	5
Required Information	6
 Administrators	 8
Step 1 – SCS STUN Configuration	8
Step 2 - Configuring an SCS User Account for the Remote Worker.....	13
Step 3- Firewall & Router Configuration.....	15
 Remote Workers – Configuring IP Phones	 20
Avaya 12xx Series IP Phones.....	21
Avaya IP Softphone 3456	28
Installation	29
Starting the 3456	31
Licensing.....	32
Disabling the Provisioning Server.....	32
Configuring Remote Settings	36
Polycom SoundPoint (Administrators Only).....	41
User Accounts and Phone Profiles	41
Configure DHCP and FTP on the Phone.....	48
 Avaya Documentation Links.....	 52

Overview

SCS 4.0 includes a NAT traversal solution to enable SIP traffic from remote workers to access the SCS system without the requirement for a VPN.

The SCS 4.0 system can be configured for remote workers to utilize both near end and far end NAT traversal. This enables the SCS system to be deployed behind a 'non SIP aware' firewall. Remote users can connect from their home networks behind small office/home office routers and communicate with the SCS deployed at for example, their head office.

Network Topology Example



AVAYA Tue, 18 May 2010 8:52 AM Home ? Help Logout Search

Users Devices Features System Diagnostics

Active Registrations

[Show Primary Registrar](#)
☒ Refresh every 30 seconds

Total Registrations : 1
 Active Registrations : 1
 Load Balance : 1.00

URI	Contact
*7030@sip:2030@scsite2.teluk.com	<sip:7010@122.166.26.182:5060:sip5060.x.sipx.privcontact=192.168.1.10%345060>

Refresh

The remote worker's phone will be configured with an extension from the SCS. Depending on the phone model, the extension will either be configured manually or from a managed configuration file created by the SCS

The registration details will include the **Public IP Address** of the remote worker's router along with **Private IP Address** of the registered phone

The Primary Registrar column displays the name of the server that handled the initial registration for that phone. This is useful in high-availability mode where the initial registration can be handled by either server in the system. This page will refresh automatically. You can switch automatic refreshing off by clearing the Refresh checkbox. You can also modify the refresh interval by clicking on the current interval and then enter a new value.

Required Information

Before the Remote Worker configuration can take place, obtain the answers to the following questions:

- What is the IP address of the SCS system to which remote workers will be assigned?
- Will STUN be utilised to determine the routers Public IP address?
- Is the public IP address of the router fronting the SCS static or can it change over time?
 - If static, what is the public IP address of the router fronting the SCS?
 - If not static, a STUN server will need to be used to determine the router's public IP address.
- What is the model of the router fronting the SCS?
- Is the router running the latest f/w version?
- What is the private LAN Subnet(s) to which the SCS is connected?
- Which models of IP phones will be used by remote workers?
- Are the phones running the latest firmware?
- What is the SCS Domain Name or Fully Qualified Domain Name?
- What are the SIP passwords of remote worker's SCS user accounts?
- What is the Outbound Proxy address. This is the public IP address of the router fronting the SCS system that is used to access the Internet or a WAN.
- What is the SCS voicemail extension number?
- What is the Music-on-hold URI?
- What is the BLF URI if speed dials have been configured?

In order to successfully register a remote worker with the SCS, there are four main configuration steps that must be undertaken:

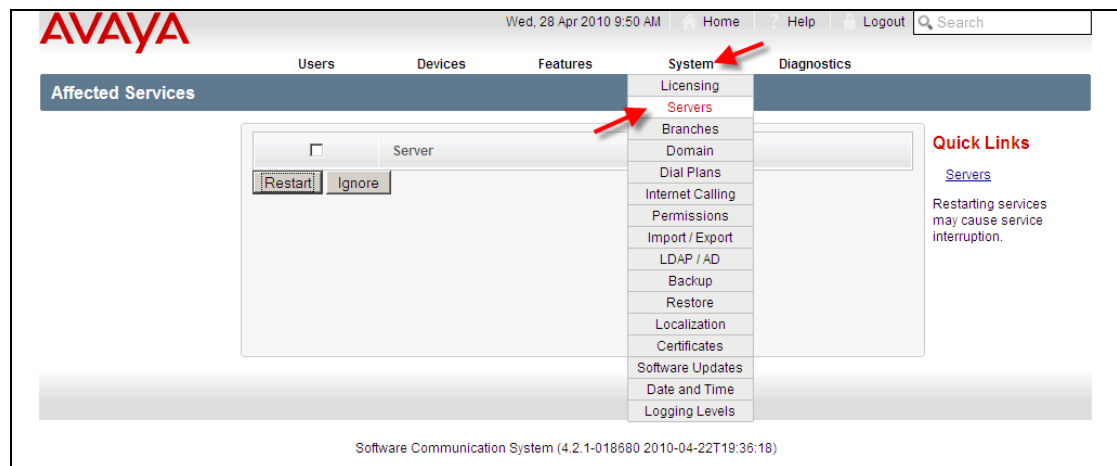
1. The SCS must be configured for NAT Traversal and remote user access.
2. A user account must be configured on the SCS for the remote user.
3. Firewall, NAT, and Port Forwarding rules must be set on the router fronting the SCS system (the right-hand router in the diagram above).
4. Configure remote IP and VoIP settings on the phone set that the user will use.

Administrators

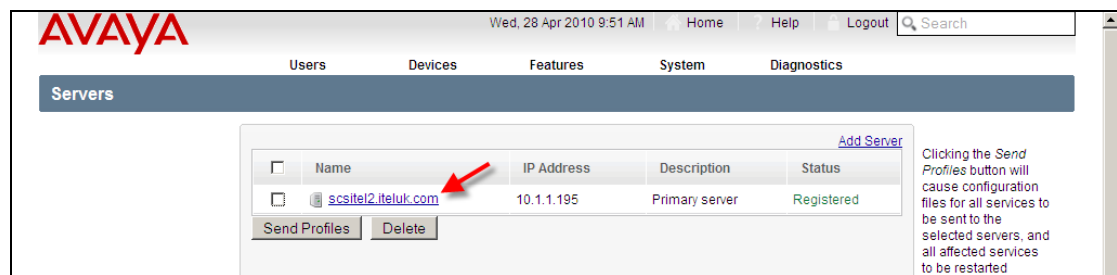
Step 1 – SCS STUN Configuration

The options to 'Enable NAT Traversal' and 'Server Behind NAT' are enabled by default within the SCS 4.0, as is the STUN (Simple Traversal of UDP through NAT) protocol. STUN assists devices behind a NAT firewall or router with packet routing. STUN enables a device to determine its public IP address and the type of NAT service utilised on the router it is located behind. To configure the STUN setting:

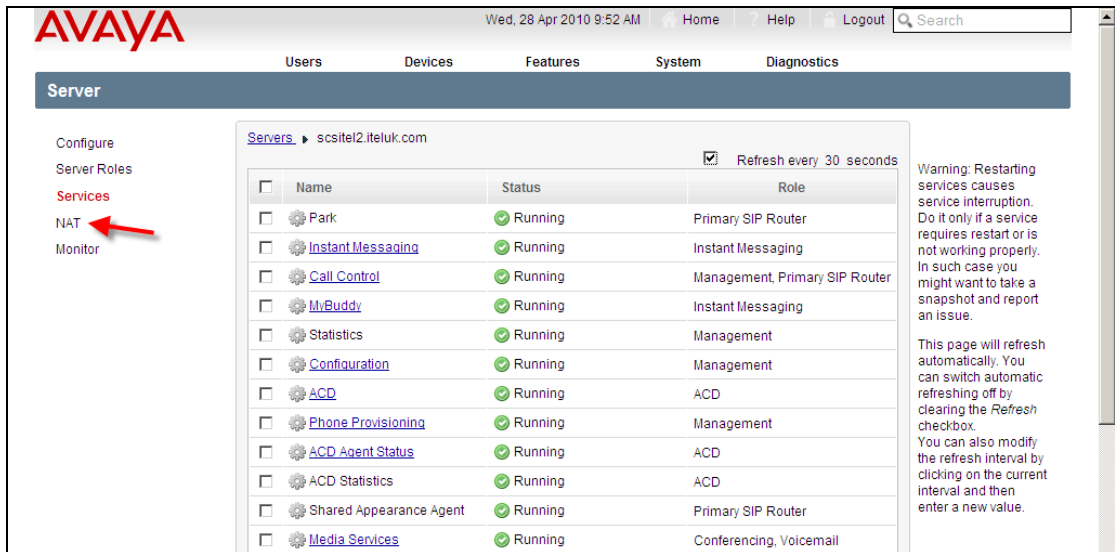
1. Navigate to the **Servers** page under the **System** menu.



2. Click the link that identifies the server.



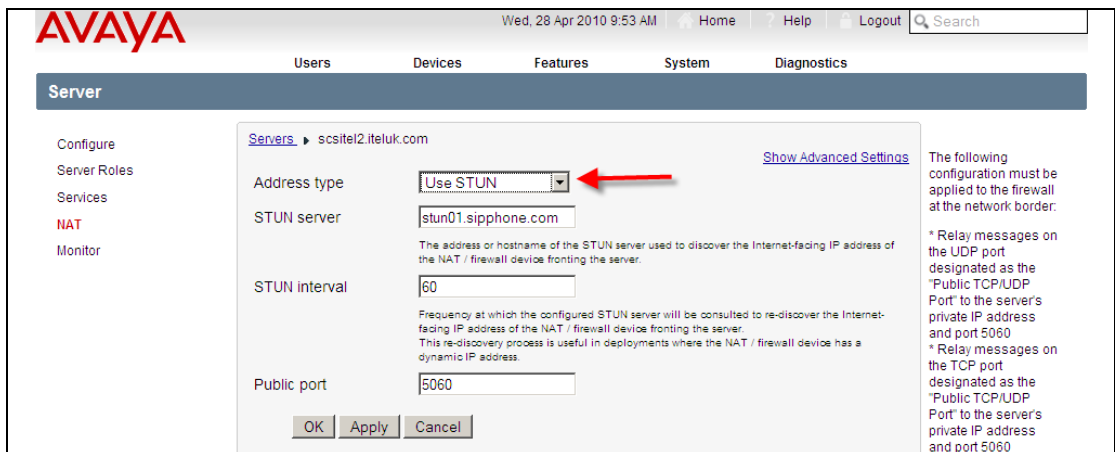
3. From the **Server** page, click the **NAT** link.



The screenshot shows the Avaya Server configuration interface. The left sidebar contains a tree view with 'Configure', 'Server Roles', 'Services', 'NAT', and 'Monitor'. The 'NAT' link is highlighted with a red arrow. The main content area displays a table of services for the server 'scsitel2.iteluk.com'. The table has columns for Name, Status, and Role. The services listed are Park, Instant Messaging, Call Control, MyBuddy, Statistics, Configuration, ACD, Phone Provisioning, ACD Agent Status, ACD Statistics, Shared Appearance Agent, and Media Services. All services are running. A warning message on the right states: 'Warning: Restarting services causes service interruption. Do it only if a service requires restart or is not working properly. In such case you might want to take a snapshot and report an issue.' Below the warning, it says: 'This page will refresh automatically. You can switch automatic refreshing off by clearing the Refresh checkbox. You can also modify the refresh interval by clicking on the current interval and then enter a new value.'

Name	Status	Role
Park	Running	Primary SIP Router
Instant Messaging	Running	Instant Messaging
Call Control	Running	Management, Primary SIP Router
MyBuddy	Running	Instant Messaging
Statistics	Running	Management
Configuration	Running	Management
ACD	Running	ACD
Phone Provisioning	Running	Management
ACD Agent Status	Running	ACD
ACD Statistics	Running	ACD
Shared Appearance Agent	Running	Primary SIP Router
Media Services	Running	Conferencing, Voicemail

4. By default, the **Address type** will be set to **Use STUN** with a default address of `stun01.sipphone.com`. If required, this may be changed with the address of the STUN server you will utilise.



The screenshot shows the Avaya NAT configuration interface. The left sidebar contains a tree view with 'Configure', 'Server Roles', 'Services', 'NAT', and 'Monitor'. The 'NAT' link is highlighted with a red arrow. The main content area displays the NAT configuration for the server 'scsitel2.iteluk.com'. The 'Address type' dropdown is set to 'Use STUN'. The 'STUN server' field contains 'stun01.sipphone.com'. The 'STUN interval' field contains '60'. The 'Public port' field contains '5060'. A 'Show Advanced Settings' link is visible. The bottom of the form has 'OK', 'Apply', and 'Cancel' buttons. A warning message on the right states: 'The following configuration must be applied to the firewall at the network border: * Relay messages on the UDP port designated as the "Public TCP/UDP Port" to the server's private IP address and port 5060 * Relay messages on the TCP port designated as the "Public TCP/UDP Port" to the server's private IP address and port 5060'.

In this example it is assumed that the customer will have a static Public IP address.

5. From the **Address Type** drop down box, select **Specify IP address**.

The screenshot shows the AVAYA configuration interface for a server. The 'Address type' dropdown menu is open, and 'Specify IP address' is selected. A red arrow points to this selection. The 'STUN server' field is set to 'Use STUN', and the 'STUN interval' is set to '60'. The 'Public port' is set to '5060'. The interface includes a sidebar with 'Configure', 'Server Roles', 'Services', 'NAT', and 'Monitor'. The top navigation bar shows 'Users', 'Devices', 'Features', 'System', and 'Diagnostics'. The right side of the interface contains a 'Show Advanced Settings' link and a note about configuration requirements.

6. In the **Public IP Address** field, enter the Public IP address assigned to the router that is fronting the SCS private network. In this example an address of 217.35.36.201

The screenshot shows the AVAYA configuration interface for a server. The 'Public IP address' field is set to '217.35.36.201'. A red arrow points to this field. The 'Address type' dropdown is set to 'Specify IP address', and the 'Public port' is set to '5060'. The interface includes a sidebar with 'Configure', 'Server Roles', 'Services', 'NAT', and 'Monitor'. The top navigation bar shows 'Users', 'Devices', 'Features', 'System', and 'Diagnostics'. The right side of the interface contains a 'Show Advanced Settings' link and a note about configuration requirements.

7. The **Public Port** should be left as **5060**.

The screenshot shows the AVAYA configuration interface for a server. The 'Public port' field is set to '5060'. A red arrow points to this field. The 'Address type' dropdown is set to 'Specify IP address', and the 'Public IP address' is set to '217.35.36.201'. The interface includes a sidebar with 'Configure', 'Server Roles', 'Services', 'NAT', and 'Monitor'. The top navigation bar shows 'Users', 'Devices', 'Features', 'System', and 'Diagnostics'. The right side of the interface contains a 'Show Advanced Settings' link and a note about configuration requirements.

8. Click the **Apply** button followed by the **OK** button.

The screenshot shows the AVAYA configuration interface for a server. The 'Public IP address' field is set to 217.35.36.201 and the 'Public port' is 5060. The 'Apply' button is highlighted with a red box. The 'OK' button is also visible. The 'Cancel' button is also visible. The 'Show Advanced Settings' link is also visible.

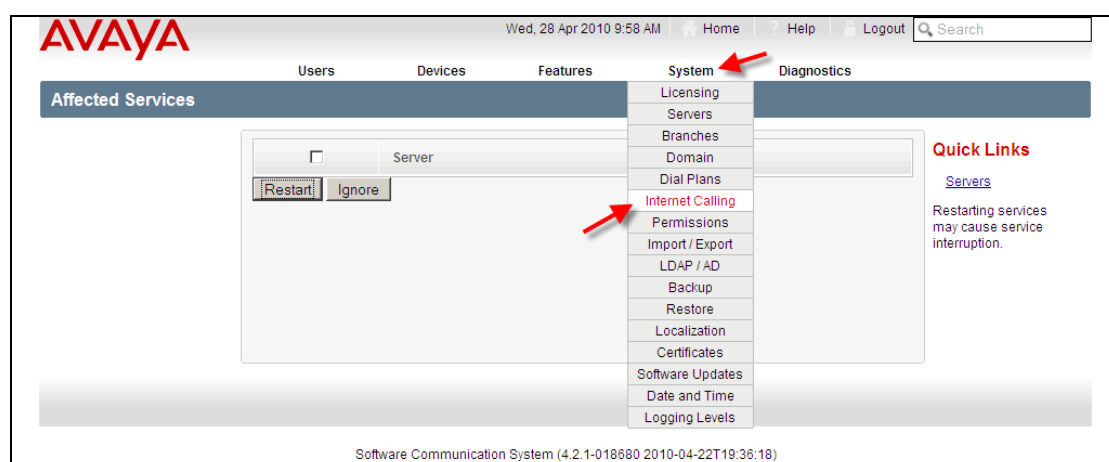
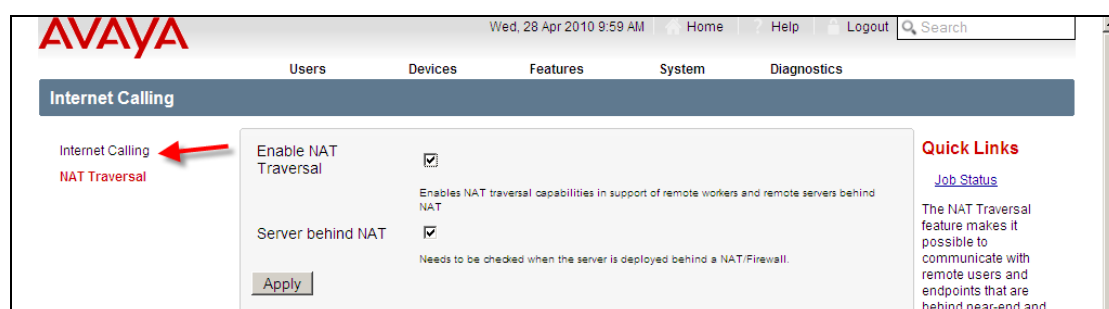
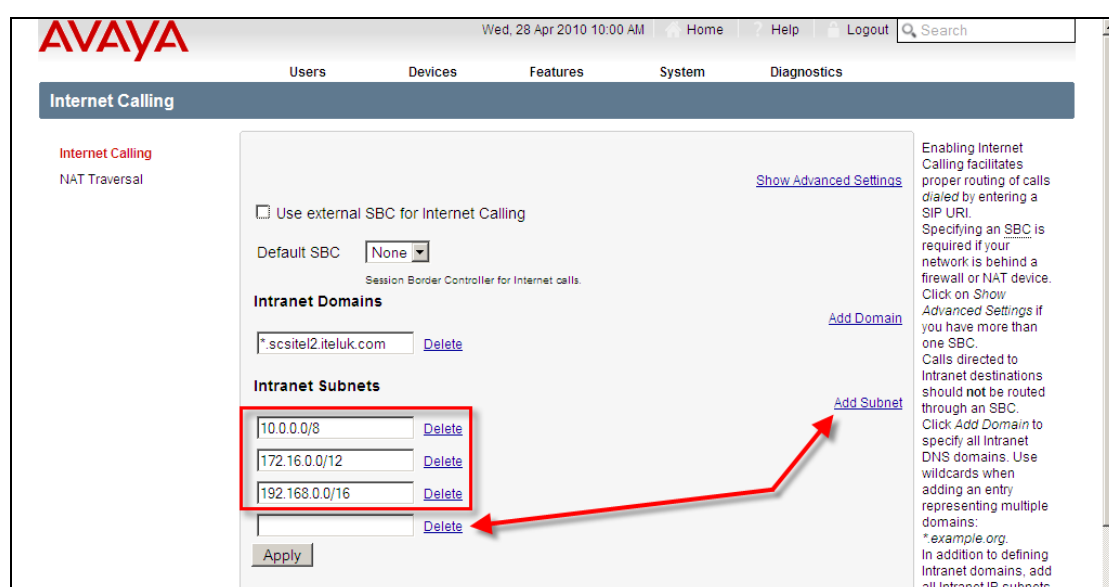
9. You will be notified that services should be restarted. Click the **here** link.

The screenshot shows the AVAYA configuration interface with a notification that services need to be restarted. A red arrow points to the 'here' link in the notification message. The notification text is: 'One or more services need to be restarted. For details click: [here](#)'. The 'Add Server' link is also visible.

10. Select the check boxes adjacent to the affected services then click the **Restart** button.

The screenshot shows the AVAYA configuration interface with a table of affected services. The 'Restart' button is highlighted with a red box and a red arrow points to it. The table has columns for 'Server' and 'Service'. The services listed are Media Relay, SIP Proxy, SIP Registrar, and SIP Trunking. The 'Restart' button is also visible.

Server	Service
☒	Media Relay
☒	SIP Proxy
☒	SIP Registrar
☒	SIP Trunking

11. From the **System** menu select **Internet Calling**.12. Click the **Internet Calling** link.13. The private LAN Subnets to which the SCS is connected, must be defined. Three commonly used Intranet subnets are listed. If the LAN side IP address range is not listed for the network to which the SCS is attached, click the **Add Subnet** link and enter the required subnet details.

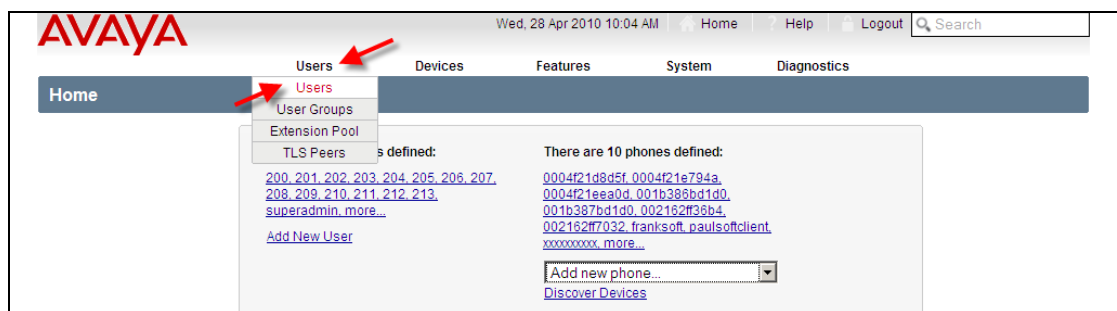
Note: If the default subnets do not apply to your actual subnet, they must be deleted. All you should be left with at the end of this step is a list of one or more subnets that together describe your private LAN subnets.

14. If any changes have been made, click the **Apply** button.

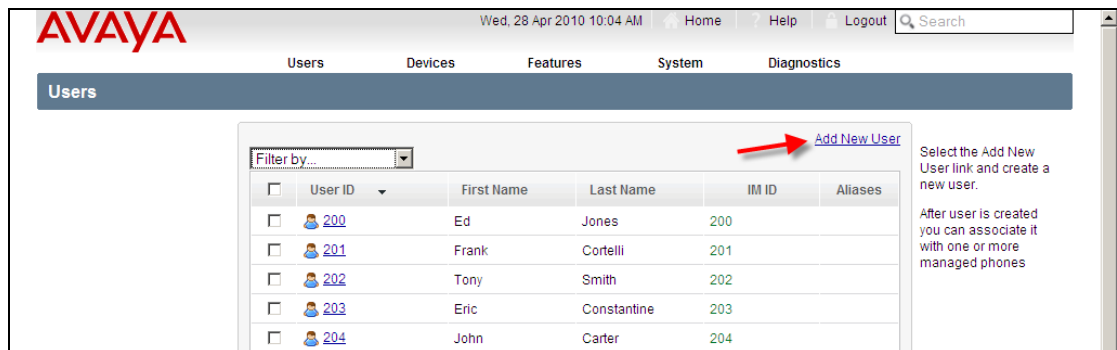
Step 2 - Configuring an SCS User Account for the Remote Worker

An SCS user account is required for the Remote Worker.

1. From the SCS home page, navigate to the **Users** page.



2. Click the **Add User** link.



- You will be presented with the **New User** page. Enter the configuration details for the remote worker.

AVAYA Wed, 28 Apr 2010 10:06 AM Home ? Help Logout Search

Users Devices Features System Diagnostics

New User

User ID

The User ID can be a numeric extension like 123 or a name like janith. The User ID is displayed by the phone and it is therefore recommended to use the internal extension as the User ID. If using DID configure the DID number (or its DNIS portion) as an alias.

Last name

First name

PIN

Confirm PIN

The PIN is a password used to log in to voicemail or to the user portal. Numeric PINs are recommended, since only numbers can be dialed.

SIP password

The SIP password is used by the user's phone to register with the SIP proxy. For phones managed by this system, the SIP password entered here will be configured automatically on the phone. For unmanaged phones, the SIP password is needed when manually configuring lines on the phone. The security of this password is very important and that is why a secure password is auto-generated.

Groups

List all groups for this user. If a group does not exist, it will be created. When entering multiple groups, separate them with spaces.

Branch

Quick Links

[Extension Pool](#)

Existing Groups:
administrators,
Phonebook,
InternalPhonebook,
member,
InternalGroup, IM,
Sales, Conferencing,
conf, im, Confe

New Groups: You can create new groups simply by adding the new group name to the Groups form value.

- Make a note of the **User ID** and the **SIP Password** as these are required when the phone is configured for the Remote User.

Note: For user configuration details, please refer to the SCS 4.0 Configuring User Profiles Task Based Guide.

- Click the **Apply** button followed by the **OK** button.

The PIN is a password used to log in to voicemail or to the user portal. Numeric PINs are recommended, since only numbers can be dialed.

SIP password

The SIP password is used by the user's phone to register with the SIP proxy. For phones managed by this system, the SIP password entered here will be configured automatically on the phone. For unmanaged phones, the SIP password is needed when manually configuring lines on the phone. The security of this password is very important and that is why a secure password is auto-generated.

Groups

List all groups for this user. If a group does not exist, it will be created. When entering multiple groups, separate them with spaces.

Branch

Aliases

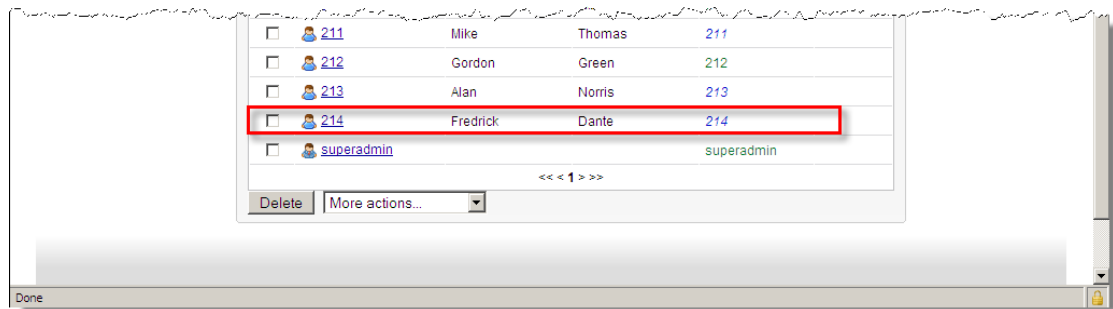
Aliases are additional names for the user. Like the user ID, an alias can be either a numeric extension or a name. When entering multiple aliases, separate them with spaces.

☐ Create another user after this one?

Software Communication System (4.2.1-018680 2010-04-22T19:36:18)

Done

6. The configured User will be displayed.



Step 3- Firewall & Router Configuration

In this example, the SCS is located behind a router configured with a firewall and NAT. Therefore the router that fronts the SCS system requires firewall rules / port forwarding configuration, to allow access to the SCS by the Remote Worker. This will provide the Remote Worker with the capability to make calls to other SCS users and to the public network.

The following configuration steps are required:

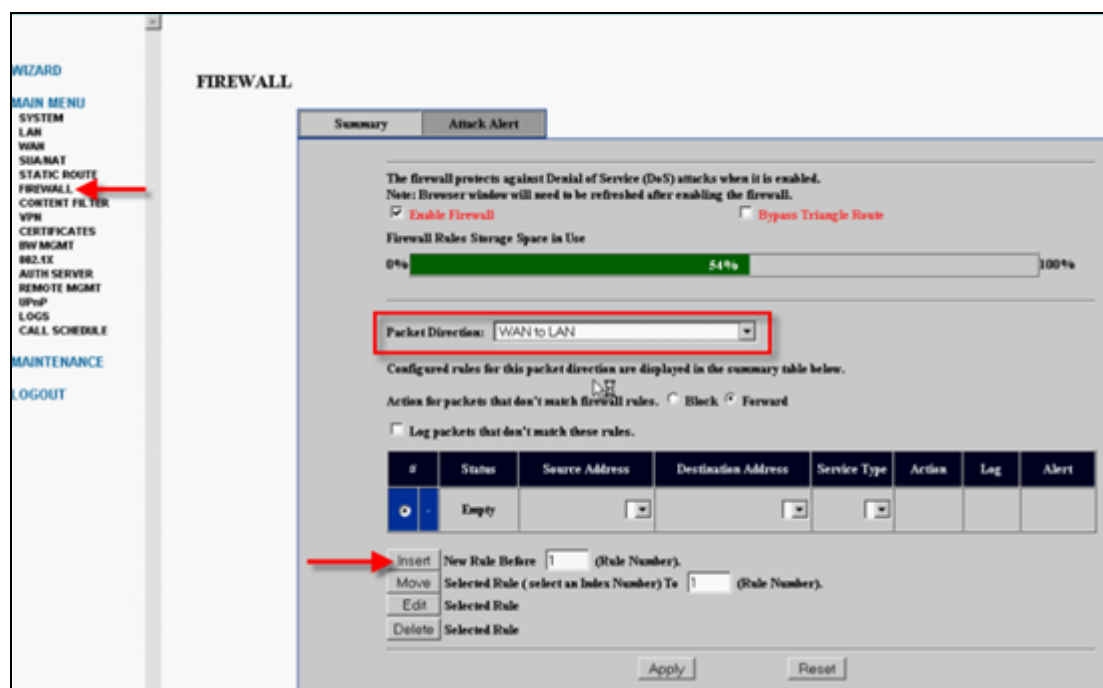
- Ports **5060 and 5061** for **TCP and UDP** service types to be open and forwarded to the **private IP address** of the SCS on the LAN.
- Ports **30000 to 31000** for the **UDP** service type to be open and forwarded to the **private IP address** of the SCS on the LAN.

Note: To enhance network security, the Source IP Address can be configured as the static Public IP address of the router at the Remote Worker's location. There are many ways to add rules to enhance the router's security, but this will depend on the individual network environment, the type of router used, and whether the Remote Worker has static or Dynamic Public IP address.

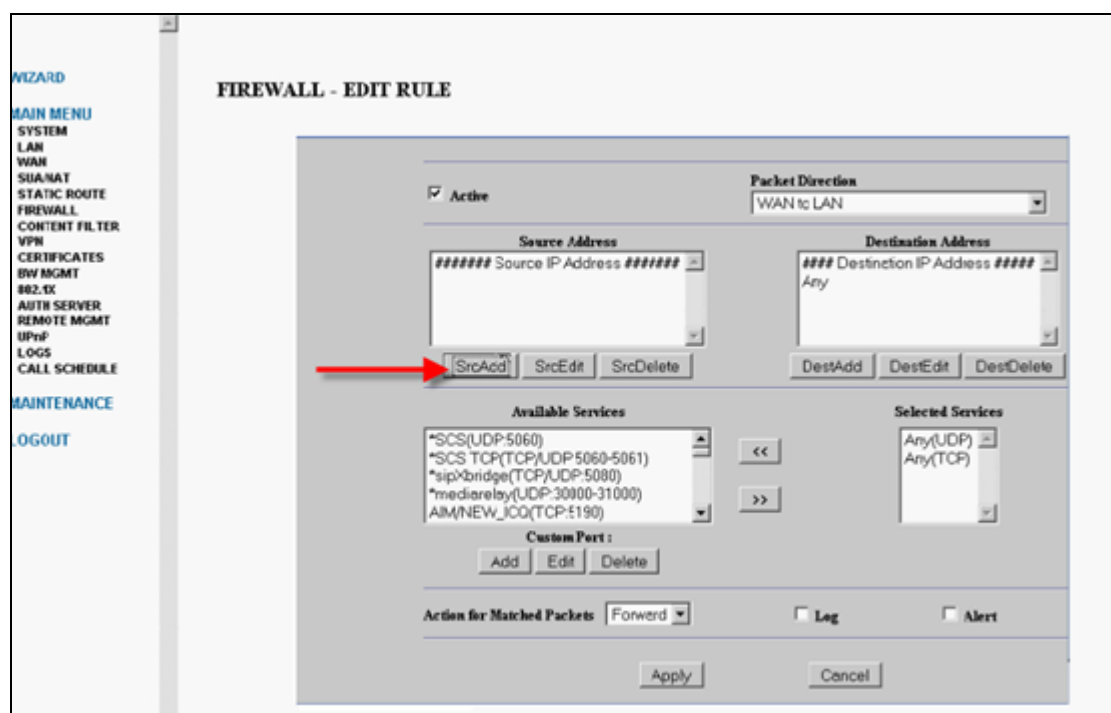
Note: When using the SCS-resident NAT traversal facility you must disable any STUN/TURN/ICE facility on remote phones and disable SIP ALGs (Application-level gateway) in the remote router's NAT / Firewall configuration.

The following steps outline the configuration of a router with the parameters required for a successful SCS remote worker installation. It should be noted that there are numerous routers publicly available that can be utilized for this process. Therefore the configuration steps and screen captures illustrated here are the general parameters defined on a typical router, which may differ to your own network router interface.

1. The router's firewall should be configured with a rule that will direct incoming packets from the **WAN to LAN** upon which the SCS resides.



2. The **Source IP Address** and the **Services** affected by this rule should be defined. In this example the **Destination Address** has been left as **Any**, therefore the incoming packets can be directed to any IP address on the network where the SCS resides. If preferred, the IP address of the SCS can be defined as the **Destination Address**.



3. In most cases '**Any**' source address would be defined as an **Address Type**, particularly if you have several remote workers, as you would require a rule for each worker.

WIZARD

MAIN MENU

SYSTEM

LAN

WAN

SUAMAT

STATIC ROUTE

FIREWALL

CONTENT FILTER

VPN

CERTIFICATES

BW MGMT

802.1X

AUTH SERVER

REMOTE MGMT

UPnP

LOGS

CALL SCHEDULE

MAINTENANCE

LOGOUT

FIREWALL - EDIT RULE - EDIT IP

Address Type: Any

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Apply Cancel

4. However, if required configuration for a single remote worker can be defined. In this example, a single Source IP address is defined as 122.166.26.182. This is the **Public IP address** of the router fronting the remote worker's private network.

WIZARD

MAIN MENU

SYSTEM

LAN

WAN

SUAMAT

STATIC ROUTE

FIREWALL

CONTENT FILTER

VPN

CERTIFICATES

BW MGMT

802.1X

AUTH SERVER

REMOTE MGMT

UPnP

LOGS

CALL SCHEDULE

MAINTENANCE

LOGOUT

FIREWALL - EDIT RULE - EDIT IP

Address Type: Single Address

Start IP Address: 122.166.26.182

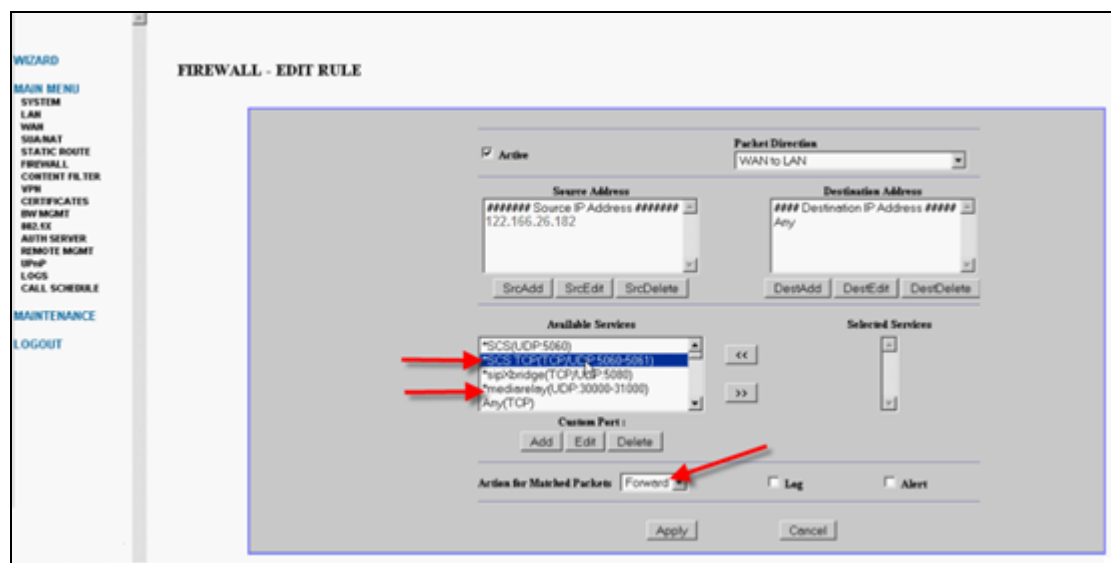
End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

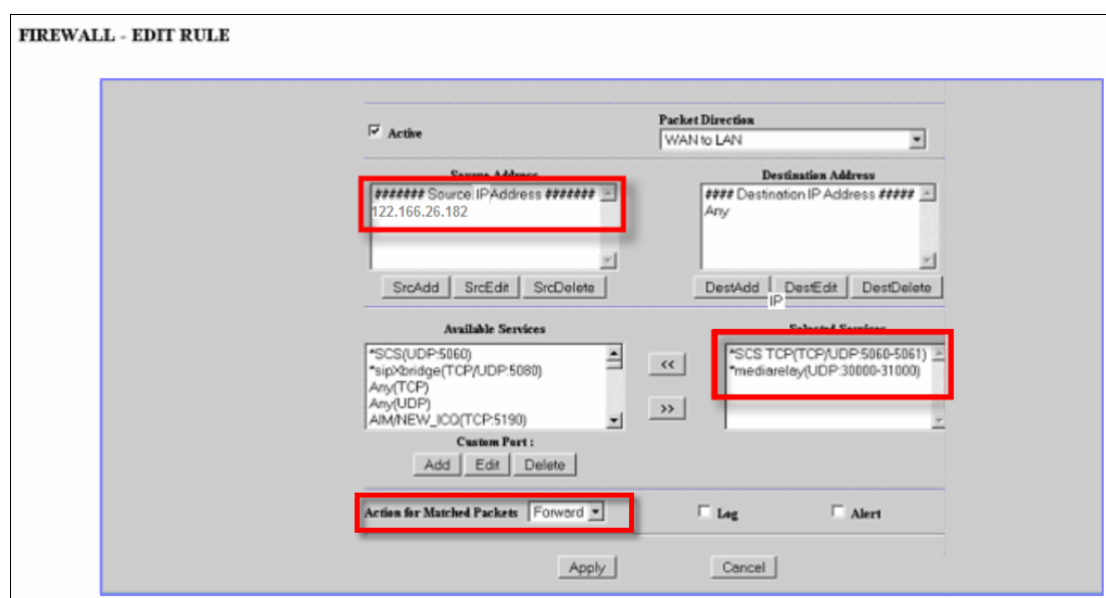
Apply Cancel

Note: This is an optional step that cannot be used if the Remote Worker's public IP address is subject to change without warning. Also, the **Single Address** example described in point 4 may not be practical if you have several remote workers, as you would need a rule for each worker.

5. The services affected by this rule can now be defined. These are **Ports 5060 and 5061 for TCP and UDP** service types and **Ports 30000 to 31000** for the UDP service type. The action for the marked packets should be set to **Forward**.



6. In this example, the source address has been defined as the Public IP address of the remote worker's router. Packets from the WAN to the LAN where the SCS is located destined for Ports 5060 and 5061 for TCP and UDP and Ports 30000 to 31000 for the UDP, will be forwarded to the network upon which the SCS resides.



7. The configured WAN to LAN firewall rule will be displayed.

Packet Direction:

Configured rules for this packet direction are displayed in the summary table below.

Action for packets that don't match firewall rules. ☐ Block ☐ Forward

☒ Log packets that don't match these rules.

#	Status	Source Address	Destination Address	Service Type	Action	Log	Alert
1	Active	122.166.26.182	Any	*SCS TCP(TCP:5060-5061)	Forward	Disabled	No
2	Active	122.166.26.182	Any	*mediarelay(UDP:30000-31000)	Forward	Disabled	No
3	Active	Any	Any		Forward	Disabled	No
4	Active	Any	Any		Forward	Disabled	No
5	Active	Any	Any		Forward	Disabled	No
6	Active	Any	Any		Forward	Disabled	No
7	Active	Any	Any		Forward	Disabled	No
8	Inactive	Any	Any		Forward	Enabled	No
9	Inactive	Any	Any		Forward	Enabled	No
10	Inactive	Any	Any		Forward	Enabled	No

Go To Page

Insert New Rule Before (Rule Number).

Move Selected Rule (select an Index Number) To (Rule Number).

Edit Selected Rule

Delete Selected Rule

8. The firewall has now been configured to allow signalling and media traffic into the SCS network from the Remote Worker's network. The final router configuration steps require NAT Port forwarding rules to direct traffic through defined ports to the SCS server.

In this example Port Forwarding rules have been created for ports 5060 and ports within a range 30000 to 31000 to direct traffic through these ports to the SCS IP address of 10.1.1.195

#	Active	Name	Start Port	End Port	Server IP Address
1	☒	scs	5060	5060	10.1.1.195
2	☒	media	30000	31000	10.1.1.195
3	☐		0	0	0.0.0.0
4	☐		0	0	0.0.0.0
5	☐		0	0	0.0.0.0

This completes the configuration of the SCS and the router fronting the network upon which the SCS resides. The IP phones to be used by the remote worker can now be configured.

NOTE: Service for users deployed as Remote Workers over the public internet is unavailable if the server they are registered to fails. This is true both for a single server deployment and if the SCS is deployed with a High Availability server option. This limitation is a result of the way NAT traversal operates. Under some conditions this NAT limitation may be partially overcome to provide one-way calling depending on the customer router capabilities and/or the DNS configuration. The networking dependencies and programming for this are beyond the scope of this guide.

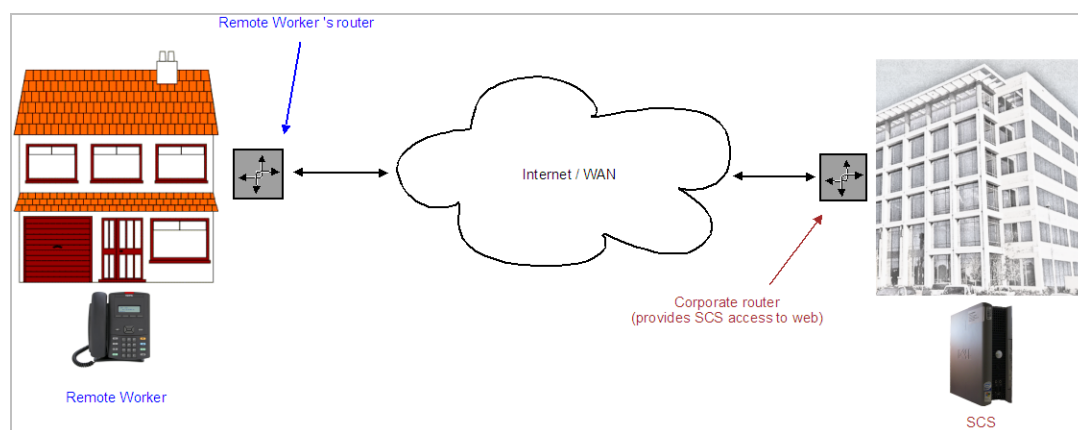
Remote Workers – Configuring IP Phones

The SCS provides users with the option of configuring an IP phone at a remote location – e.g., a home office – thereby providing the user with full access to office-based telephony, including contact lists, presence information, conferencing, and of course, PSTN calls through a gateway.

The following IP sets are supported for remote working:

- Avaya 1200 series phones
- Avaya IP Softphone 3456
- Polycom SoundPoint series phones

Each phone type requires a varying amount of configuration but the network topology remains the same. In essence, the remote worker's phone needs to be able to 'see' the router responsible for transporting data to and from the SCS at the corporate end, and vice-versa, the SCS needs to be able to send data to and receive it from the user's router.



Therefore, in order to successfully configure a remote worker account, 4 steps must be undertaken:

1. The SCS must be configured for NAT Traversal and remote user access.
2. A user account must be configured on the SCS for the remote user.
3. Firewall, NAT, and Port Forwarding rules must be set on the router fronting the SCS system (the right-hand router in the diagram above).
4. Configure remote IP and VoIP settings on the phone set that the user will use.

The purpose of this section of the guide is to guide users through step 4 in the process. Steps 1,2 and 3 should already have been completed by the SCS administrator before users come to configure their sets for remote working.

Note: Polycom SoundPoint phones can **only** be configured using the SCS; remote users will not be able to configure all necessary settings on Polycom sets manually. See the section on Polycom SoundPoint later in this guide.

Avaya 12xx Series IP Phones



Note: Ensure that a user account has been created before attempting remote registration.

Avaya 12xx series IP phones can be configured either through the phone interface or through a graphic user interface (GUI) accessed via a web browser. It is recommended that you configure the necessary settings for remote working through the GUI rather than the phone interface, since the GUI makes it easier to enter some of the more complex values such as domain names and Registrar Addresses.

It is also recommended that the phone is DHCP-enabled to make it easier for it to acquire an IP address at the remote location – it is assumed that DHCP is used to provide devices at the remote end with IP addresses. If this is not the case you will need to configure static IP settings on the 12xx, please see SCS guide ‘Configuring Network Settings on Avaya 1200 IP phones’.

When you receive your phone it should be set to configure LAN settings using DHCP by default.

You will need to know certain IP and VoIP settings in order to register remotely to the SCS. The following table outlines the credentials you will need to configure, use the space provided to note each value.

Registrar Address	sip:
SCS user ID	
SCS SIP password	
Outbound Proxy	
Voicemail Access Number	
Music-on-hold URI	
MWI R URI	
RLS Subscription URI	

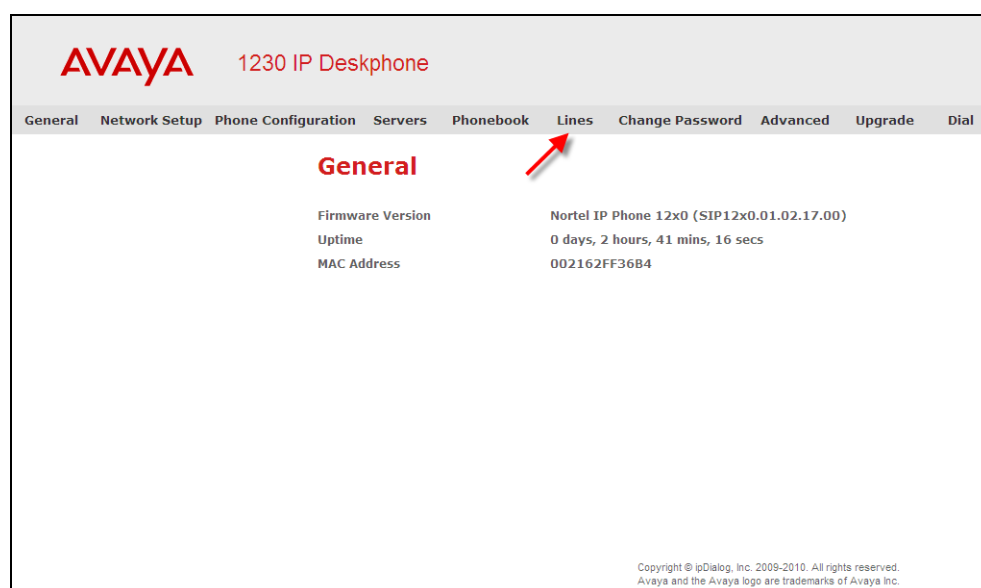
- **Registrar Address** – The address of the fully qualified domain name of your provisioning SCS. If you are unsure what your SIP domain is please contact your SCS administrator. This URI should be prefixed **sip:**
- **SCS username** – This is the user ID defined in your SCS user account. Often defined as an extension number, this value can also be set as a name. If you are unsure of your user ID contact your SCS administrator.
- **SCS SIP password** – The SIP password is an alpha-numeric value usually automatically created by the SCS when an account is configured, your SCS administrator will have to advise you of this. **This is not your SCS PIN.**
- **Outbound Proxy** – This is the public IP address of the router fronting the SCS system that is used to access the Internet or a WAN. Your network administrator should be able to advise you of this.
- **Voicemail Access Number** – This is made up of the voicemail extension you dial when picking up messages and the SCS SIP domain. Your network administrator will know what the voicemail URI is.
- **Music on Hold URI** – The address of the music on hold service on the SCS. Check with the SCS administrator if you are unsure of this parameter.
- **MWI R-URI** – Message waiting indicator URI, this is the address that the phone will check for voicemail messages.
- **RLS Subscription URI** – If speed dials are configured on the user account then there is a chance that Presence information has been requested, this information is displayed on the phone using busy icons. In order for this feature to work on a remote phone you will need to supply the address of the service that handles BLF – Busy Lamp Field, used to determine another user's status, i.e., whether they are available to take a call. Check with your SCS administrator if you are unsure what to enter.

To configure the phone:

1. Plug the phone into the router.
2. When the phone has finished booting press the **Services** button to view the phone's IP address.
3. Open a web browser and navigate to the phone's IP address.



- The default username is 'admin' and the password is '1234'. Click on the **Lines** menu.

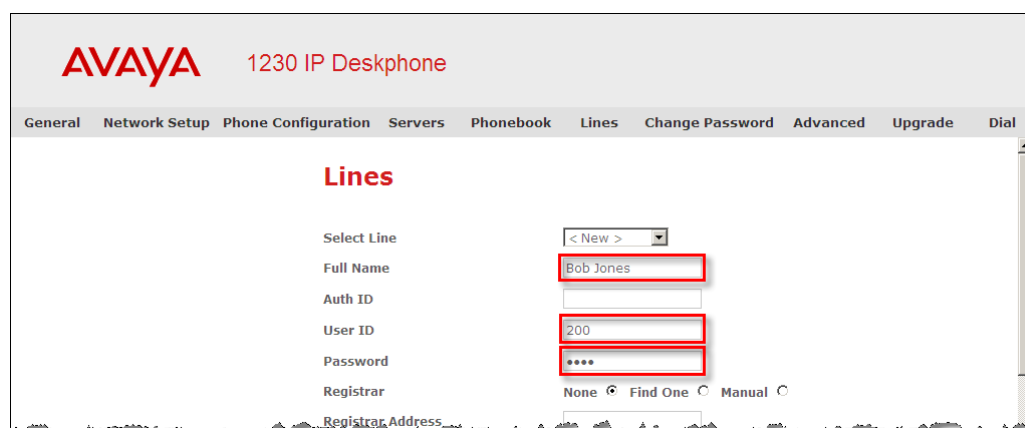


- Enter your name in the **Full Name** field.

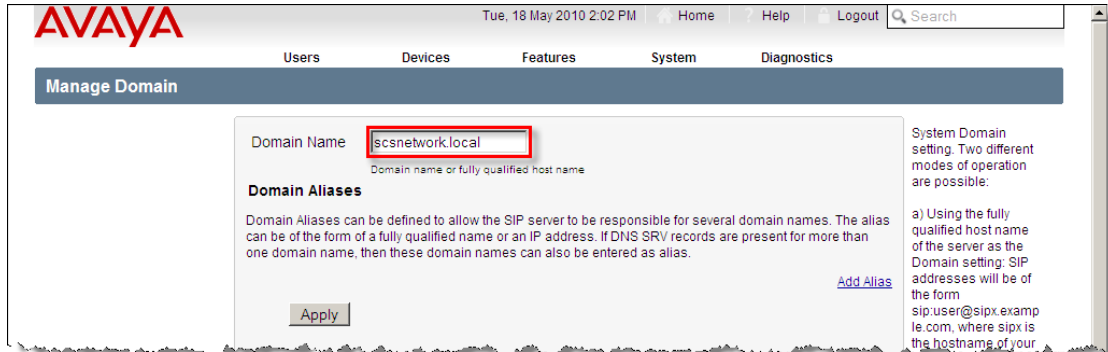
Note: If your phone already has an account configured on it, click on the **Advanced** menu, scroll to the bottom of the screen and select **Restore Factory Defaults**. Enter the administrative user name ('admin' by default) and password ('1234' by default) and press **Enter**. This will clear the phone and reboot it making it ready for your account details. When reboot is complete start at step 2 again.

- Enter your SCS Username in the **User ID** field.
- Enter your SIP password in the **SIP Password** field – if you are unsure of your SIP password please contact your SCS administrator.

Note: The SIP Password is an alpha-numeric value assigned to the account by the SCS, it is not the User PIN.



Set the **Registrar Address**, this is the domain name of the SCS, prefixed with **sip:**. Your SCS administrator will know what the SIP domain is; they can find it by opening the SCS administrative interface and selecting the **Domain** option from the **System** menu.



You can see from the illustration above that in this instance the SIP URI would be: **scsnetwork.local**

8. Tick the **MWI Subscribe** check-box.
9. Enter the **MWI R-URI**, this should take the form of your SIP address prefixed by **sip:**, for example:

sip:username@scshost.business.com

Your SIP address is constructed from your username and the SIP domain.

10. Enter the **Voicemail Access Number** as a complete URI – that is, the extension number of the voicemail server followed by the SIP domain. For example:

101@scshost.business.com

If you are unsure what to enter here, contact your SCS administrator.

AVAYA 1230 IP Deskphone

General Network Setup Phone Configuration Servers Phonebook Lines Change Password Advanced Upgrade Dial

Lines

Select Line: Alex Samson

Full Name: Alex Samson

Auth ID: 200/002162ff36b4

User ID: 200

Password: *****

Registrar: None ☐ Find One ☒ Manual ☒

Registrar Address: sip:scsnetwork.local

☐ Use domain name from network configuration

Transport: Auto

Expires (sec): 3600

Number of Line Keys: 1

Shared: ☒

SIP Outbound Proxy: scsnetwork.local

SIP Outbound Proxy Port:

MWI Subscribe? ☒

MWI R-URI: 200@scsnetwork.loc

Voicemail Access Number: 101@scsnetwork.loc

MoH Server: ~mh~@scsnetwork

Call Forwarding Mode: None ☒ CFU ☐ CFB ☐ CFNA ☐ TIMER 20

Call Forwarding URI:

Commit changes

Copyright © ipDialog, Inc. 2009-2010. All rights reserved.
Avaya and the Avaya logo are trademarks of Avaya Inc.

Done

11. Enter the MOH (Music on Hold) server address in the following format **sip:~mh~@scsnetwk.local** – your SCS administrator will be able to advise you of what to enter in this field.

MoH Server: ~mh~@scsnetwork

Call Forwarding Mode: None ☒ CFU ☐ CFB ☐ CFNA ☐ TIMER 20

Call Forwarding URI:

Commit changes

Copyright © ipDialog, Inc. 2009-2010. All rights reserved.
Avaya and the Avaya logo are trademarks of Avaya Inc.

Done

12. Click **Commit Changes**.
13. Click on the **Servers** menu.

14. Enter the **Outbound Proxy**, this is the public IP address of the router fronting the SCS system that is used to access the Internet or a WAN. Ask your SCS administrator if you are unsure what to enter here.

The screenshot shows the AVAYA 1210 IP Deskphone configuration interface. The 'Servers' tab is selected in the top navigation bar. The page title is 'AVAYA 1210 IP Deskphone'. The 'Servers' section contains the following fields:

- Outbound Proxy 1: [Text input field]
- Outbound Proxy 1 Port: [Text input field]
- Outbound Proxy 1 Transport: [Auto] (dropdown menu)
- ☐ SIP PING for Server Redundancy
- Outbound Proxy 2: [Text input field]
- Outbound Proxy 2 Port: [Text input field]
- Outbound Proxy 2 Transport: [Auto] (dropdown menu)
- Conference Server: [Text input field]
- [Commit changes] (button)

15. Click **Commit Changes**.

16. Finally, If speed dials have been configured on your user account you can use BLF (Busy Lamp Field) to see whether users are busy on a call or not. In order for this facility to work, you will need to click on the **Phone Configuration** menu and enter an **RLS Subscription URI** value. For a 1200 phone the URI takes the following form: **sip:~r1~C~xxxx@sip domain**, where **xxxx** is your username. Your SCS administrator will be able to advise you of the BLF URI if you are unsure what to enter.

The screenshot shows the AVAYA 1210 IP Deskphone configuration interface. The 'Phone Configuration' tab is selected in the top navigation bar. The page title is 'AVAYA 1210 IP Deskphone'. The 'Phone Configuration' section contains the following fields:

- Enable Do Not Disturb: ☐
- Disable Call Waiting: ☐
- Enable IM Beep Alert: ☒
- Blink Light On Incoming Calls: ☒
- Enable Flashing for MWI Indicator: ☒
- Block My Caller ID: ☐
- RLS Subscription URI: [sip:~r1~C~xxxx@sip] (highlighted with a red box)
- Note: RLS subscription is sent from first available line.
- Dial Plan: [Text input field]
- Language: [English] (dropdown menu)

Note: Depending on firewall settings and other security considerations you may or may not be able to access the SCS user interface in order to add or amend speed dials. Contact your network administrator to find out whether or not you will be able to access the user interface from your remote location.

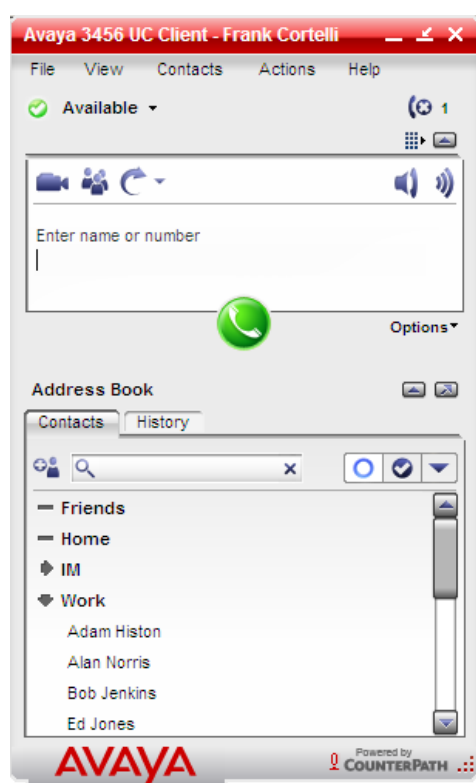
Note: BLF will only function with the primary user line.

17. Click **Commit Changes** to complete configuration. Your phone should flash off and then back on as it updates its settings.

18. Reboot the phone to register it to the SCS – press the **Services** button on the phone, followed by the **Setup** soft key, then **Reset** and **Phone**.

When the phone has rebooted, the screen should display your username and a black phone icon next to the bottom-right line key, indicating that you are registered. Check your registration by dialing the voicemail attendant (101 by default) or the auto-attendant (100 by default). If you are unable to dial either of these numbers check your settings and reboot the phone. If you are still having difficulty registering after reboot, contact your SCS administrator.

Avaya IP Softphone 3456



Note: Ensure that a user account has been created for the user before commencing with remote worker configuration.

The 3456 softphone can be configured to connect to the SCS from a remote location such as a home office.

You will need to know certain IP and VoIP settings in order to configure a remote worker account on the phone. The following table outlines the credentials you will need to configure, use the space provided to note each value.

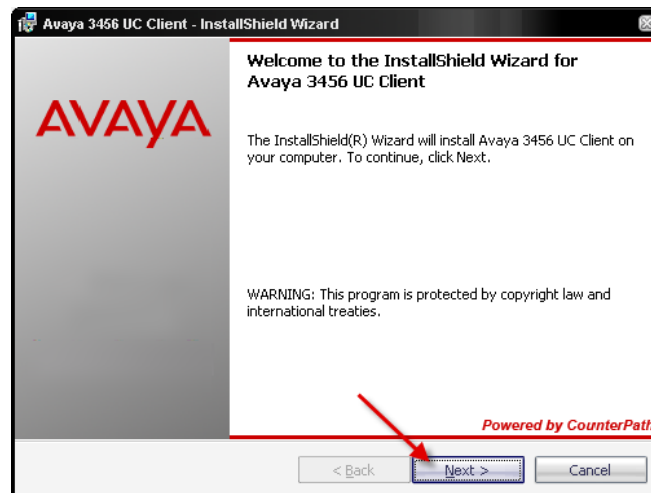
SCS SIP Domain	
SCS username	
SCS SIP password	
Domain Proxy	
Voicemail extension	
BLF URI	

- **SCS Domain** – The SCS SIP domain. If you are unsure what your SIP domain is please contact your SCS administrator.
- **SCS Username** – This is the user ID defined in your SCS user account. Often defined as an extension number, this value can also be set as a name. If you are unsure of your user ID contact your SCS administrator.
- **SCS SIP password** – The SIP password is an alpha-numeric value usually automatically created by the SCS when an account is configured, your SCS administrator will have to advise you of this. **This is not your SCS PIN.**
- **Domain Proxy** – This is the public IP address of the router fronting the SCS system that is used to access the Internet or a WAN. Your network administrator should be able to advise you of this.
- **SCS voicemail extension** – This is the extension number you dial when retrieving voicemail messages.
- **BLF URI** – (Busy Lamp Field) If speed dials are configured on the user account then there is a chance that Presence (a user's current call status) information has been requested. In order for this feature to work on a remote phone you will need to supply the address of the service that handles BLF. Check with your SCS administrator if you are unsure what to enter.

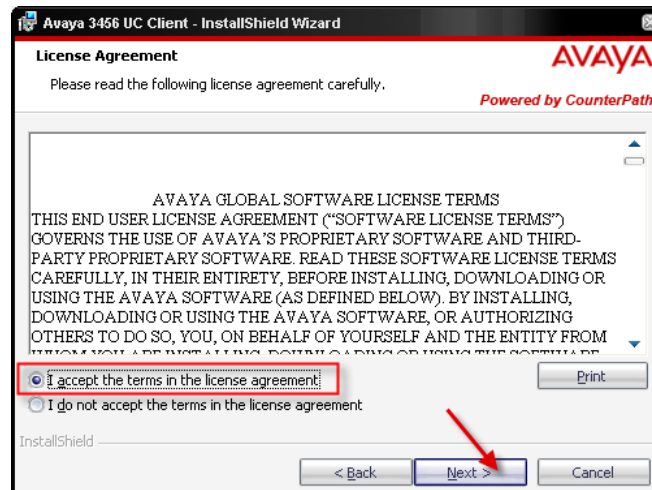
Installation

The 3456 installs on your PC or laptop like any other piece of software.

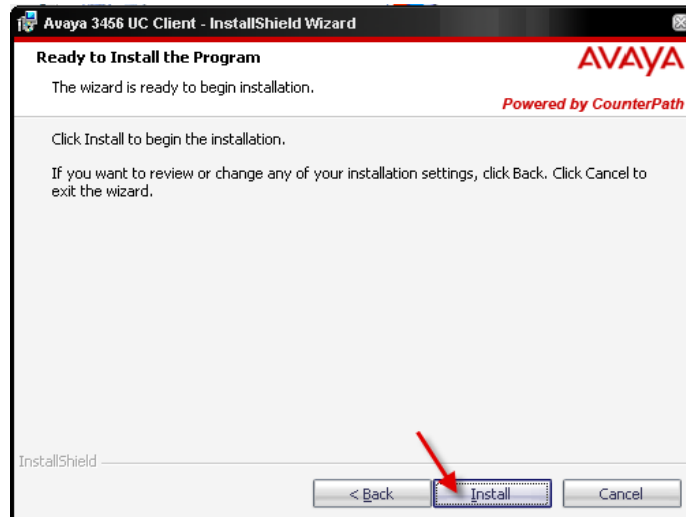
1. Launch the client installer by double-clicking on the installer icon.
2. Click **Next** to clear the introductory dialogue.



3. When you have read and understood the license agreement, click the 'I accept the agreement' radio button and then click the **Next** button.



4. Click **Next** to accept the default folder location – or click on the **Browse** button to select a different location.
5. Click the **Install** button to begin the installation.

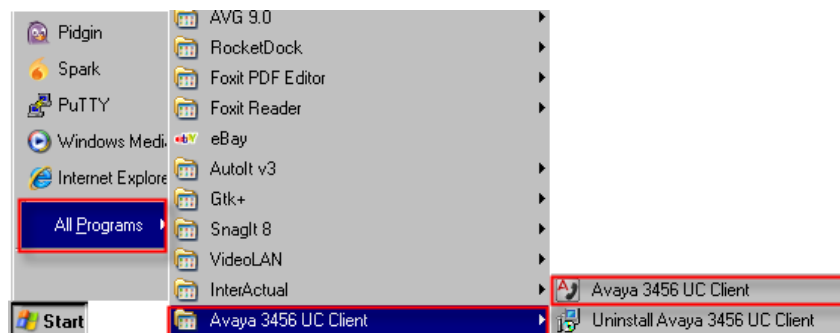


6. When the files have been copied, tick the options that you would like to take effect upon exiting the installer. Then click **Finish**.

Note: If you ticked **Launch 3456** in the final window, ignore the following section, 'Starting the 3456'.

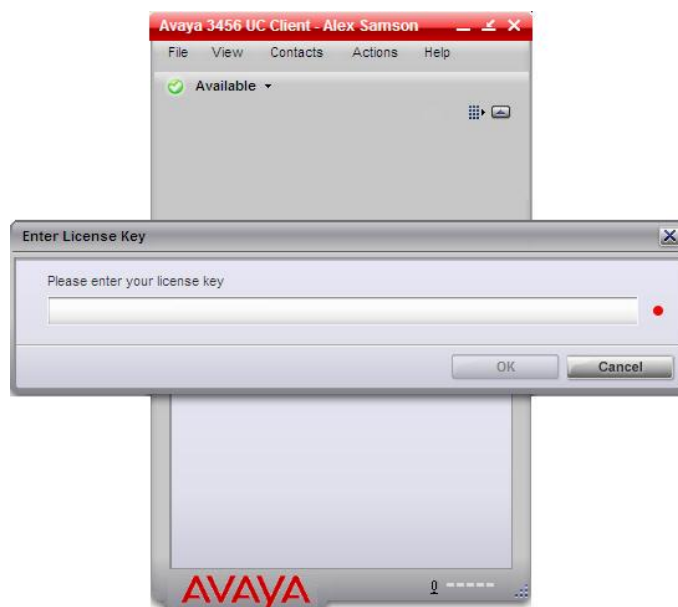
Starting the 3456

Like any other application, the SMC is launched either from a desktop icon or by opening the **Start** menu and navigating to **Programs > Avaya 3456 UC Client > Avaya 3456 UC Client**.



Licensing

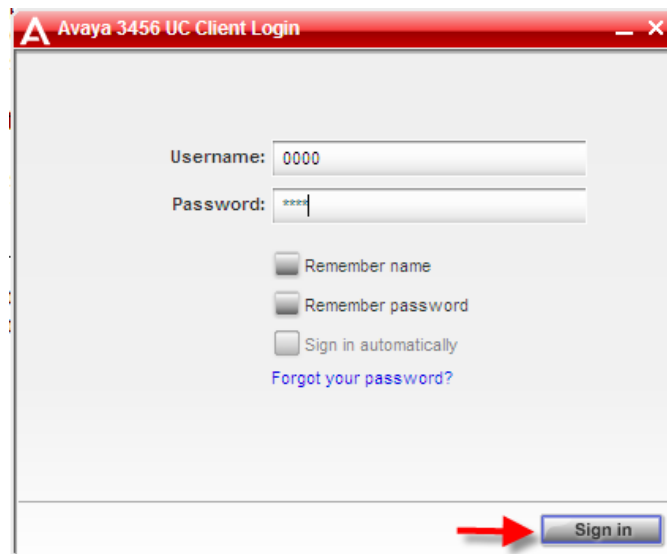
Before the soft client can be configured or used in anyway it needs to be licensed with a keycode. The licensing screen will appear the first time the client is started. Simply enter the keycode in the field provided and then click the **OK** button.



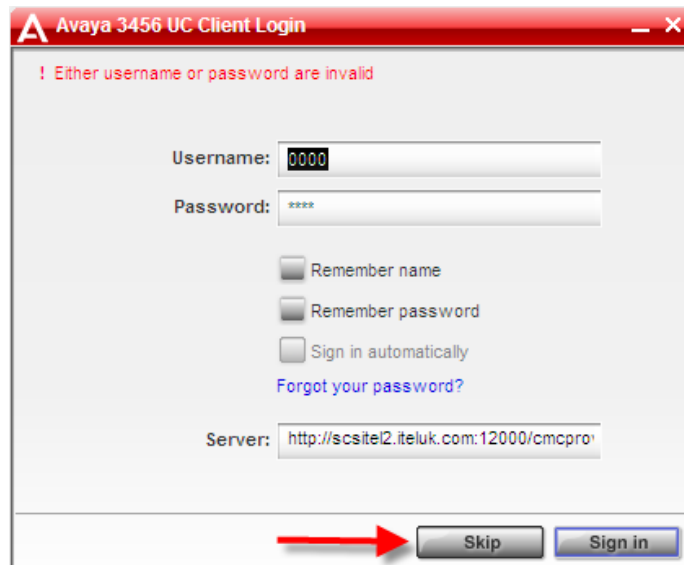
Disabling the Provisioning Server

The 3456 can be configured to gather account and configuration data from a central provisioning server when used on a local network. This feature has been designed to facilitate large-scale rollouts of the phone across the enterprise infrastructure. When started for the first time, the application will request a user name, password, and SCS server location for quick and easy registration. In a Remote Worker scenario it is not possible to take advantage of the provisioning server option; account settings must be entered manually. You must therefore first disable the server login screen before continuing. This section will show you how to disable this particular function.

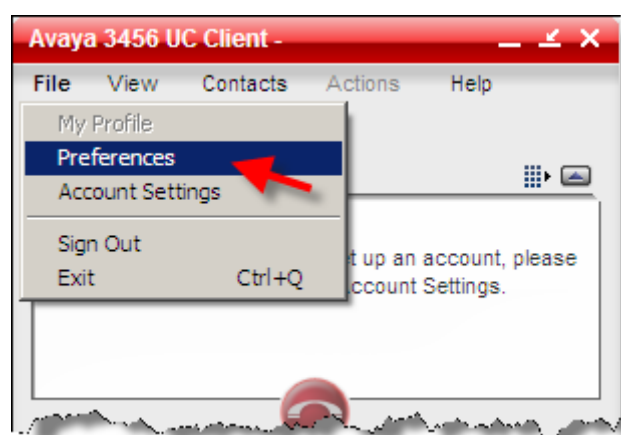
1. To access the phone for configuration purposes, a login attempt must be made. In the Client Login screen, enter 0000 as the user name and password, and then click **Sign in**.



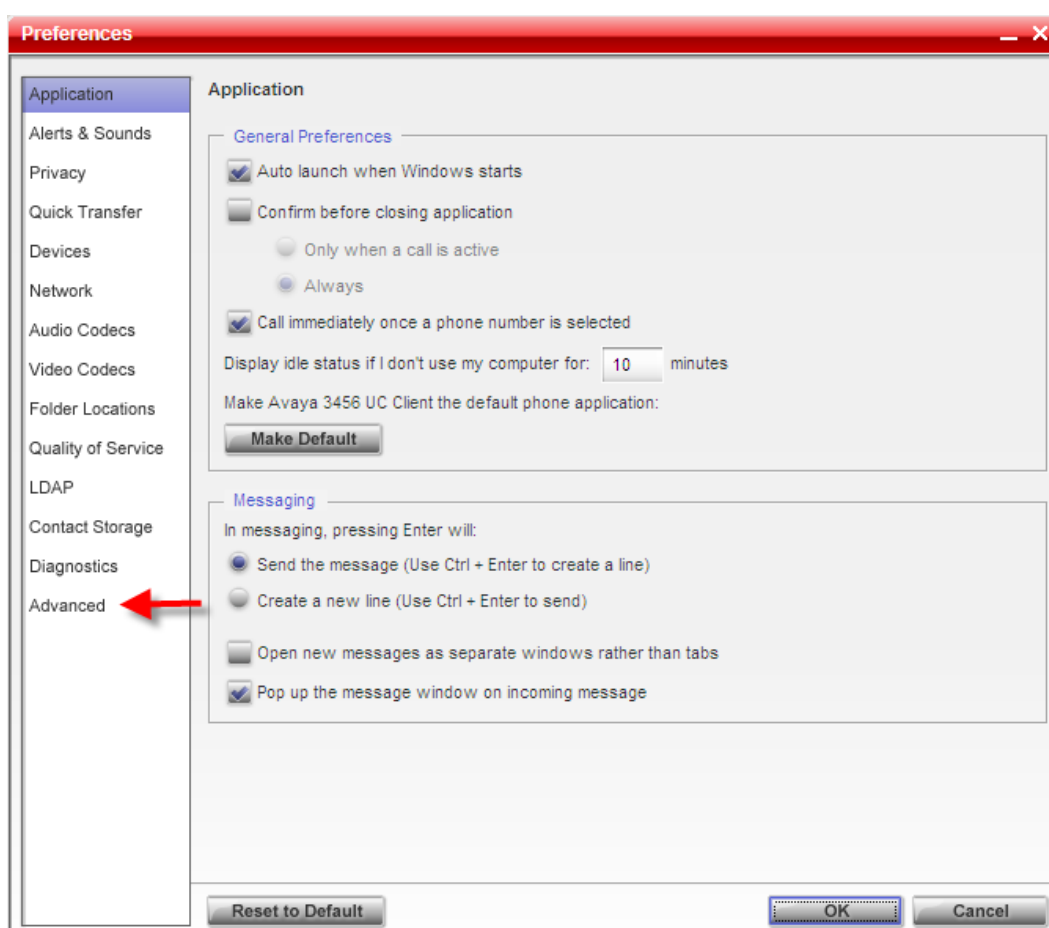
2. This will attempt to access the SCS to validate the credentials, as this may not be on the local domain (for a remote worker) it will return an invalid login attempt.



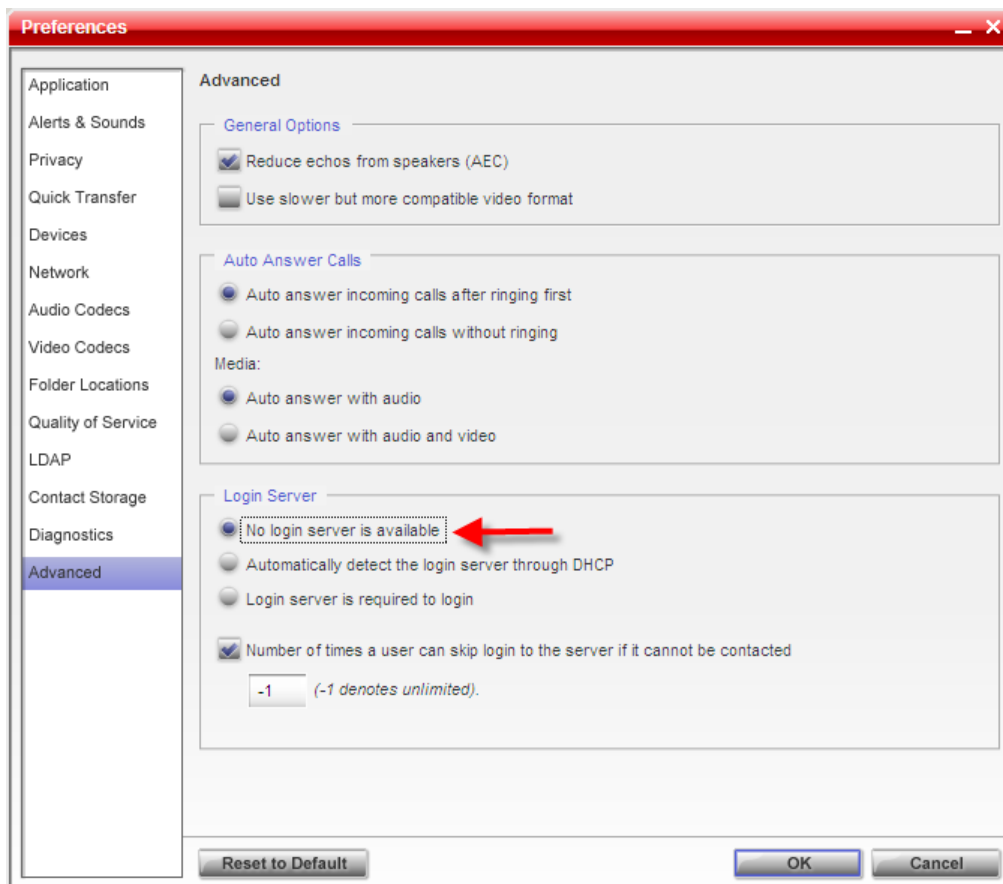
3. Click on the **Skip** button.



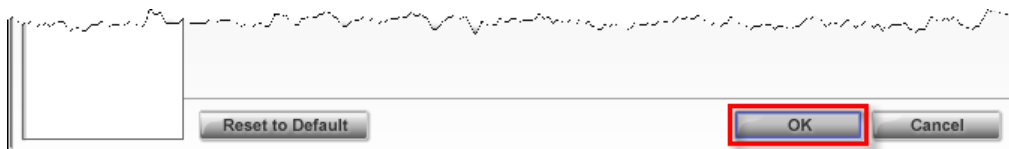
4. Open the **File** menu and select **Preferences**.



5. Click on the **Advanced** button, located at the bottom of the window.



6. The lower third of the Advanced window deals with Login Server settings. Select the **No login server is available** radio button.

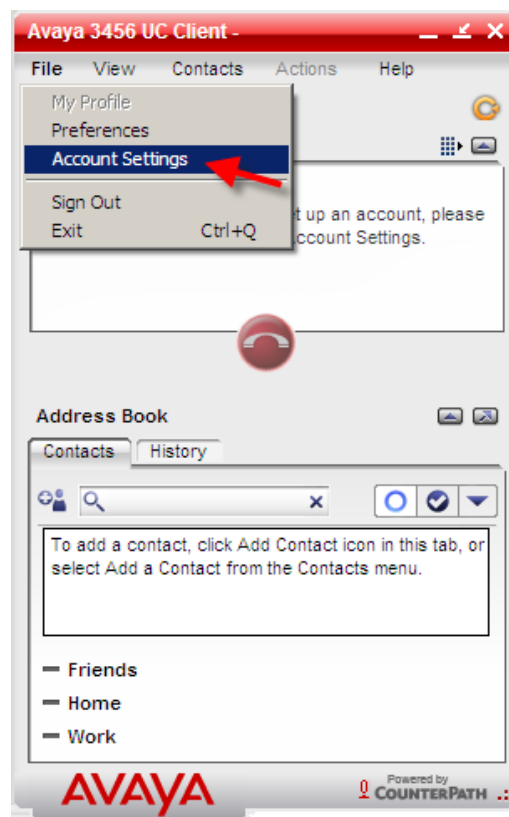


7. Click the **OK** button.

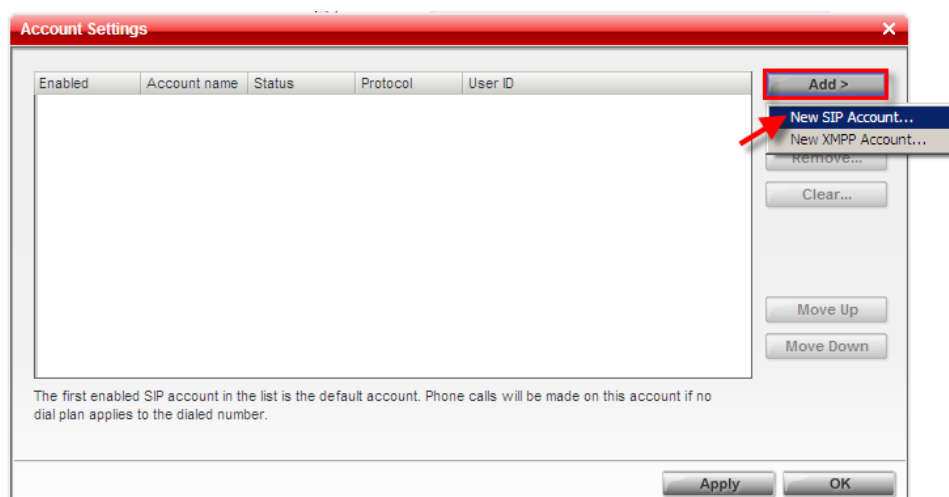
Server login at start-up is now disabled. You can now configure your softphone to register remotely with the SCS.

Configuring Remote Settings

1. Open the **File** menu and select **Account Settings**.



2. Click the **Add** button and select **New SIP Account**.



3. Enter your SIP URI in the **User ID** field. Your SIP URI is made up of your SCS username and the SCS SIP domain in the form of an email address – for example **203@scshost.business.com**

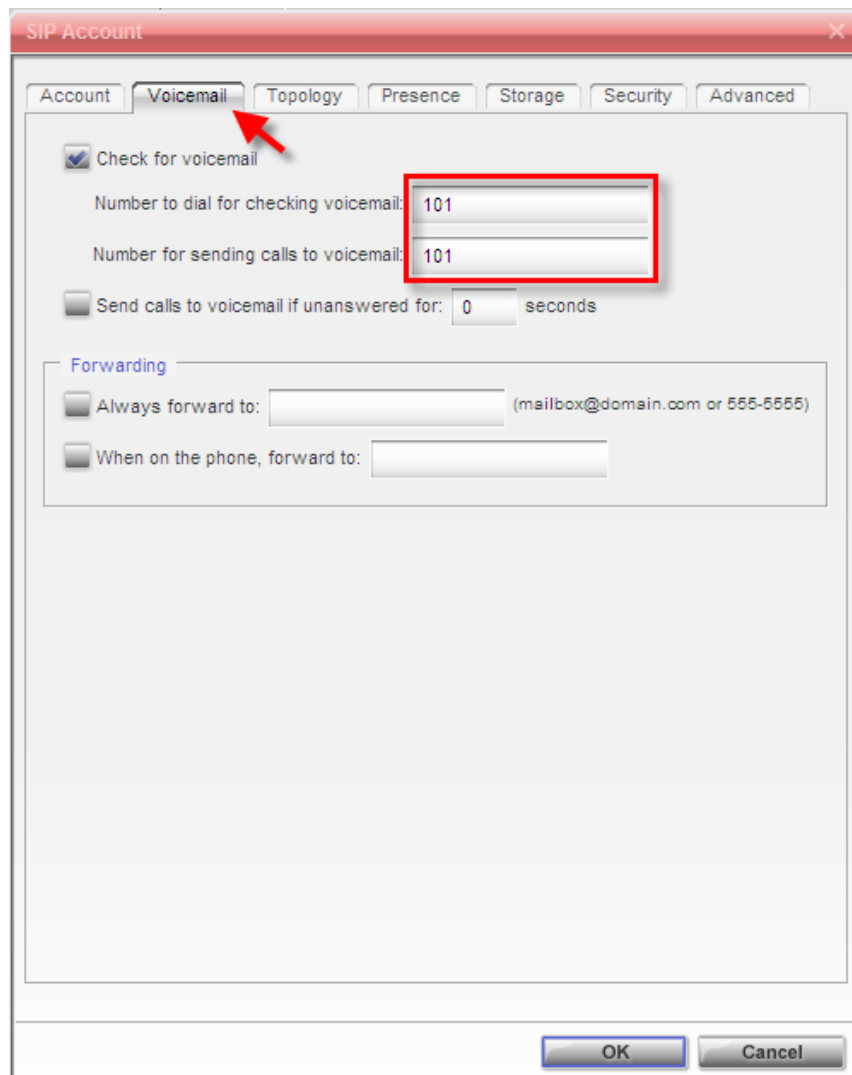
Your SCS administrator will be able to find your SIP domain in the administrative interface under **System>Domain**.

4. Enter your SIP password in the **Password** field. A SIP password is an alpha-numeric password created by the SCS when your account is initially configured, it is **not** your login PIN. Check with the SCS administrator if you are unsure of your SIP Password.
5. Enter a **Display Name**, this can be anything you choose.
6. In the **send outbound via** section select the **Proxy** option and then enter the public IP address of the router fronting the SCS system that is used to access the Internet or a WAN. If you are unsure of this IP address, please contact the SCS administrator.

The screenshot shows the 'SIP Account' configuration window. The 'Account' tab is selected. The 'User Details' section contains the following fields: 'Account name' (Account 1), 'Protocol' (SIP), 'User ID' (203@scshost.business.com), 'Password' (masked with ****), 'Display name' (Alex), and 'Authorization name'. The 'Domain Proxy' section has a checked box for 'Register with domain and receive calls'. Under 'Send outbound via', the 'Proxy' radio button is selected, and the 'Address' field contains 89.123.65.218. The 'Dial plan' field contains #1\$a.T;match=1;prestrip=2;. The 'OK' and 'Cancel' buttons are at the bottom right.

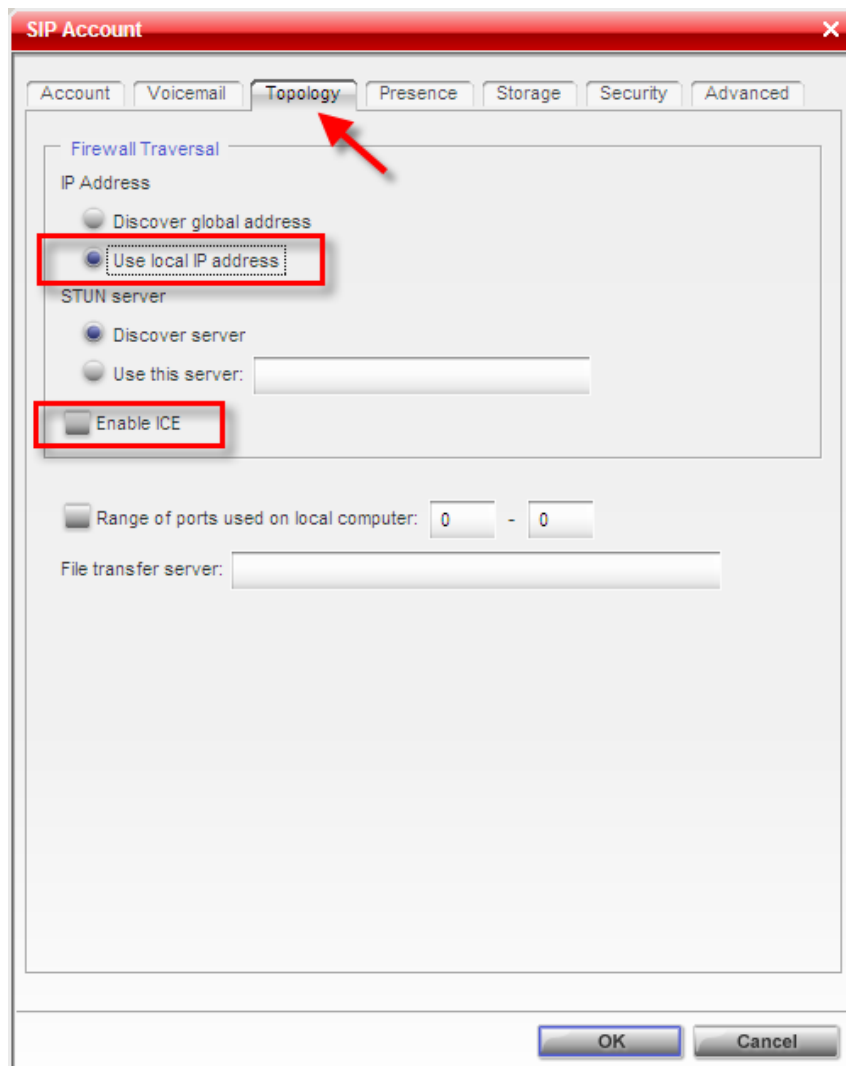
7. A softphone dial plan can be configured to enable your phone to process numbers dialed using Click to Dial Outlook contacts so that the SCS can route them correctly using its own dial plans. For more on writing a dial plan see 'Softphone Dial Plans' after this section.
8. Click on the **Voicemail** tab.

9. Enter the voicemail extension (101 by default) in both **Number to dial for checking voicemail** and **Number for sending calls to voicemail**.



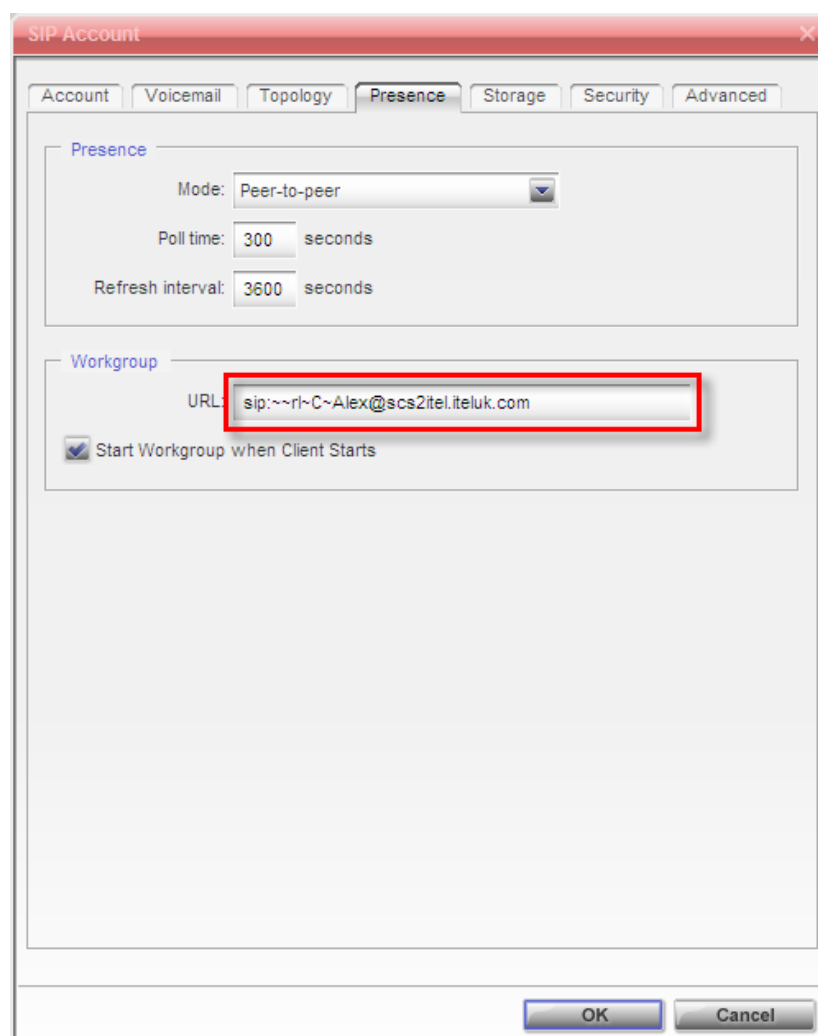
10. Click on the **Topology** tab.
11. Under **Firewall Traversal**, set **IP Address** to **Use local IP address**.

12. Deselect the **Enable ICE** check-box.



13. Finally, If speed dials have been configured on your user account you can use BLF (Busy Lamp Field) to see whether users are busy on a call or not. In order for this facility to work, you will need to click on the **Presence** tab and enter the URL of the **Workgroup**. For a 3456 softphone the URI takes the following form: **sip:~r1~C~xxxx@scshost.business.com**, where **xxxx** is your user ID and **scshost.business.com** is your SCS SIP domain – Your SCS administrator will be able to advise you of the BLF URI if you are unsure what to enter.

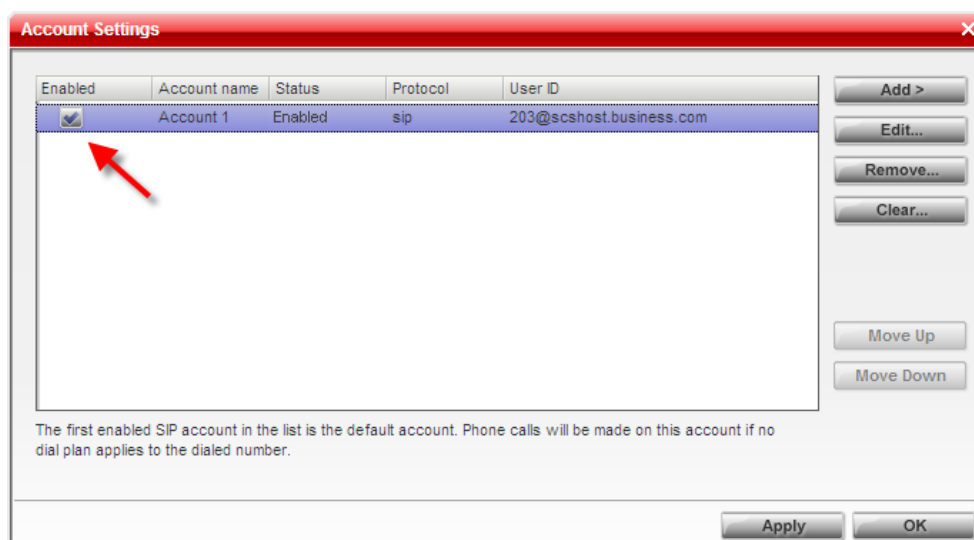
Note: Depending on firewall settings and other security considerations you may or may not be able to access the SCS user interface in order to add or remove speed dials. Contact your network administrator to find out whether or not you will be able to access the user interface from your remote location.



14. Click **OK**.

15. Tick the **Enabled** check-box to activate the account you just created.

16. Click **Apply** followed by **OK**.



Your 3456 is now configured and connected to the SCS. To check your registration, dial the voicemail attendant (101 by default) or the auto-attendant (100 by default).

Polycom SoundPoint (Administrators Only)



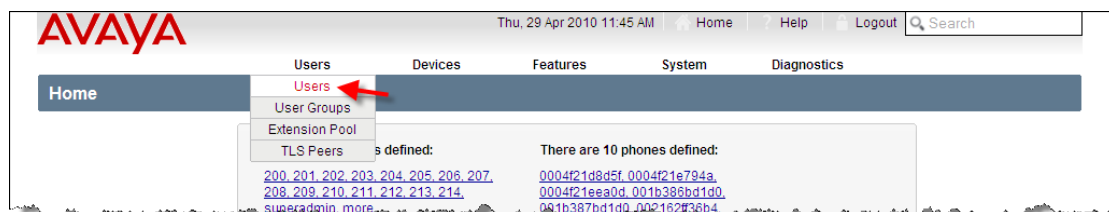
Due to the way Polycom SoundPoint IP phones are designed they can only be configured for remote worker usage using the SCS's TFTP provisioning service. This means that they can only be configured locally at the SCS site by the administrator rather than manually by the user at the remote site. Once settings have been loaded onto the phone it can be shipped to the remote site for immediate use by the remote worker.

In order to configure the phone you will need to:

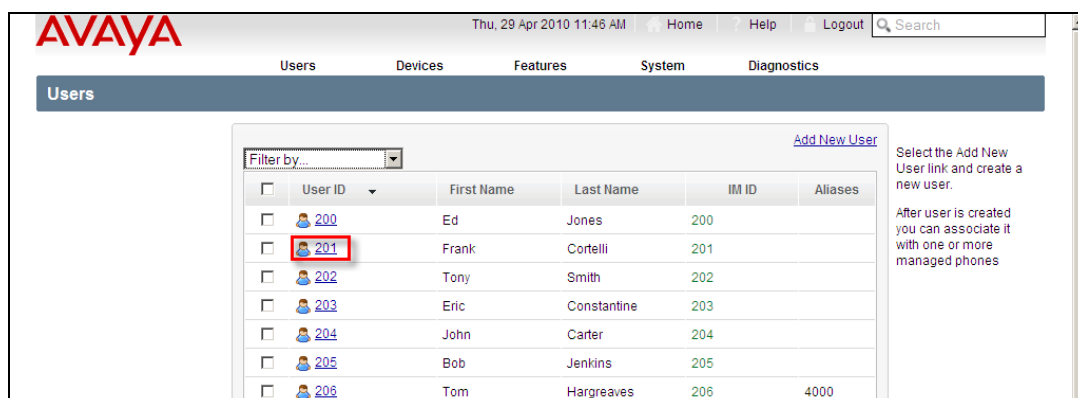
1. Create/select a user account to assign as a line to the phone.
2. Create a phone profile and assign the chosen line.
3. Configure the outbound proxy address (the public IP address of the router used by the SCS to access the Internet or a WAN).
4. Send the profile
5. Configure the phone with DHCP and an FTP address and then boot the phone.

User Accounts and Phone Profiles

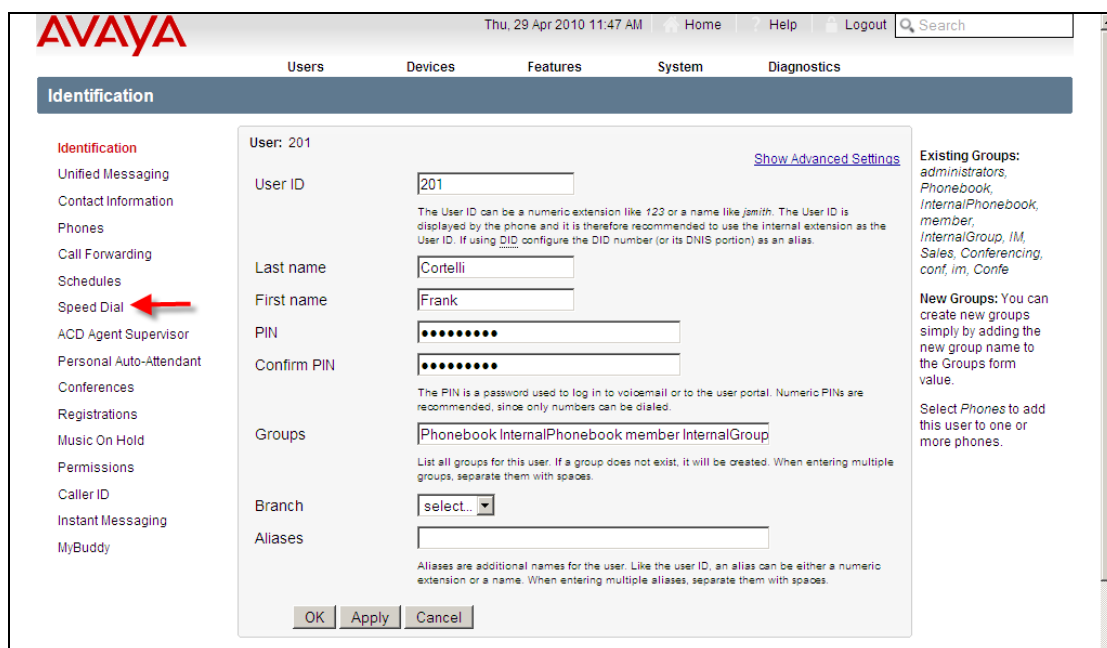
1. In the SCS administrative interface, open the **Users** menu and select **Users**.



2. Select the user that will be using the Polycom SoundPoint phone – if the required user does not yet exist you will need to configure a new user profile, see the 'Configuring User Profiles' guide.



3. If required, set up speed dials for the user by clicking on **Speed Dial**. (If you do not need to configure speed dials, continue to step 7.)



Note: for the purpose of this scenario we will assume that the user will not be using the Group Speed Dials option.

4. Disable the Use Group Speed Dials option. This will display the Add Number option. Click **Add Number**.

AVAYA Thu, 29 Apr 2010 11:49 AM Home Help Logout Search

Users Devices Features System Diagnostics

Speed Dial

User: 201

Identification
Unified Messaging
Contact Information
Phones
Call Forwarding
Schedules
Speed Dial
ACD Agent Supervisor
Personal Auto-Attendant

Name Number Subscribe to presence

Use Group Speed Dials ☐

Warning: Enabling this option will delete all your existing Speed Dials and replace them with the Group Speed Dials

OK Apply Cancel Save and Update Phone(s)

[Add Number](#)

Speed dial numbers are defined on a per user basis. They are assigned to phones capable of speed dialing, for which the user is registered as the first line on the phone. Note that speed dial is not yet implemented for all the phones.

Make sure you choose names that

5. Enter the name and the extension number of the speed dial contact. Tick the **Subscribe to Presence** check-box to enable BLF (Busy Lamp Field) notification.

AVAYA Thu, 29 Apr 2010 11:53 AM Home Help Logout Search

Users Devices Features System Diagnostics

Speed Dial

User: 201

Identification
Unified Messaging
Contact Information
Phones
Call Forwarding
Schedules
Speed Dial
ACD Agent Supervisor
Personal Auto-Attendant
Conferences

Name Number Subscribe to presence

Julie 208 ☒

Use Group Speed Dials ☐

Warning: Enabling this option will delete all your existing Speed Dials and replace them with the Group Speed Dials

OK Apply Cancel Save and Update Phone(s)

[Add Number](#)

Speed dial numbers are defined on a per user basis. They are assigned to phones capable of speed dialing, for which the user is registered as the first line on the phone. Note that speed dial is not yet implemented for all the phones.

Make sure you choose names that can be displayed by the phones.

6. Repeat as necessary then click **Apply**, followed by **Save and Update Phone(s)** to update the profile.

Note: When **Subscribe to Presence** is selected you will be prompted to restart the Presence server, simply click on the **here** link, tick the **Presence** server check-box and then click **Restart Services**.

To return to configuring the phone, open the **Users** screen and select the user profile and continue to step 7.

7. Click on the **Phones** menu option on the left-hand side of the screen.

AVAYA Thu, 29 Apr 2010 11:56 AM Home Help Logout Search

Users Devices Features System Diagnostics

Identification

Identification
Unified Messaging
Contact Information
Phones
Call Forwarding
Schedules
Speed Dial
ACD Agent Supervisor
Personal Auto-Attendant

User: 201

User ID: 201

The User ID can be a numeric extension like 123 or a name like jsmith. The User ID is displayed by the phone and it is therefore recommended to use the internal extension as the User ID. If using DID configure the DID number (or its DNIS portion) as an alias.

Last name: Cortelli

First name: Frank

PIN:

Confirm PIN:

Show Advanced Settings

Existing Groups: administrators, Phonebook, InternalPhonebook, member, InternalGroup, IM, Sales, Conferencing, conf, im, Confe

New Groups: You can create new groups simply by adding the new group name to the Groups form

8. Add the Polycom phone to the user account by opening the drop-down menu and selecting the phone model.

AVAYA Thu, 29 Apr 2010 11:57 AM Home Help Logout Search

Users Devices Features System Diagnostics

User's Phones

Identification
Unified Messaging
Contact Information
Phones
Call Forwarding
Schedules
Speed Dial
ACD Agent Supervisor
Personal Auto-Attendant
Conferences
Registrations
Music On Hold
Permissions
Caller ID
Instant Messaging
MyBuddy

User: 201

Shared ☐

If checked this user has lines on several phones and calls will be shared between these phones. This is known as B.L.A.

Apply

Phone Lines

Send Profiles Restart Delete

Polycom SoundPoint IP 550/560

Avaya 3456 UC Client

LG Nortel IP Phone 6804

LG Nortel IP Phone 6812

LG Nortel IP Phone 6830

Nortel IP Phone 1535

Polycom SoundPoint IP 300/301

Polycom SoundPoint IP 320/330

Polycom SoundPoint IP 321

Polycom SoundPoint IP 331

Polycom SoundPoint IP 335

Polycom SoundPoint IP 430

Polycom SoundPoint IP 450

Polycom SoundPoint IP 500/501

Polycom SoundPoint IP 550/560

Polycom SoundPoint IP 600/601

Polycom SoundPoint IP 650/670

Polycom SoundStation IP 4000

Polycom SoundStation IP 6000

Polycom SoundStation IP 7000

Polycom VVX IP 1500

Add existing phones

Quick Links

Job Status

Phonelines table displays all the devices associated with the current user. The system assigns default parameters to the phone's configuration, so that normally phones do not need to be further configured.

Most devices allow for multiple user lines; the phone is displayed here if any of those lines can be associated with the current user. Click on the phone's serial number to configure phone settings; click on the line name to configure line settings.

9. Enter the phone's MAC address in the **Serial Number** field. If necessary, enter a brief description of the phone for reference purposes. Click **OK** to continue.

AVAYA Thu, 29 Apr 2010 12:01 PM Home Help Logout Search

Users Devices Features System Diagnostics

New Phone

Phone: Polycom SoundPoint IP 550/560

Serial number: **0004f21d9d5f**

The serial number is a unique identifier for this device. In most cases the serial number is the phone's MAC address. For softphones you can enter user name instead.

Description: Remote Worker Phone

Groups:

☐ Create another phone after this one?

OK Cancel

Existing Groups:
Intercom,
Analog_Phone_Group

New Groups: You can create new groups simply by adding the new group name to the Groups form value.

To configure a new phone or FXS gateway fill in the parameters on this page, then assign users to lines. No other settings need to be considered as all phone parameters are auto-configured for a typical

10. Now click on the line listed with the phone – this is the user profile that you associated with the phone.

AVAYA Thu, 29 Apr 2010 12:02 PM Home Help Logout Search

Users Devices Features System Diagnostics

User's Phones

Identification
Unified Messaging
Contact Information
Phones
Call Forwarding
Schedules
Speed Dial
ACD Agent Supervisor
Personal Auto-Attendant
Conferences

User: 201
Shared ☐
If checked this user has lines on several phones and calls will be shared between these phones. This is known as **BLA**.

Apply

Add new phone... Add existing phones

Phone	Lines	Model	Description
☐ 0004f21d9d5f	201	Polycom SoundPoint IP 550/560 v2.0	Remote Worker Phone

<< 1 >>

Send Profiles Restart Delete

Quick Links
[Job Status](#)

Phones table displays all the devices associated with the current user. The system assigns default parameters to the phone's configuration, so that normally phones do not need to be further configured.

11. Click on **Registration**.

AVAYA Thu, 29 Apr 2010 12:02 PM Home Help Logout Search

Users Devices Features System Diagnostics

Line

Line
Registration
Call Handling
Dial Plan
Messaging

Line
Phone: 0004f21d9d5f / Polycom SoundPoint IP 550/560
Line: Frank Cortelli<scip:201@scsitel2.iteluk.com>

Normally you should not have to alter any settings to make or receive calls. The defaults should be setup to match your system configuration appropriately. If, however, there are changes you'd like to make then just select the appropriate links from the list to the left.

Cancel

12. Clear the contents of the **Outbound Proxy** field and replace them with the public IP address or fully qualified domain name of the router fronting the SCS system utilized to gain access to the Internet or WAN. Click **OK** to continue.

The number of calls or conferences which may be active or on hold per line key for a specific registration on the phone. If not specified, value is 1

callsPerLineKey

The number of calls or conferences which may be active or on hold per line key for a specific registration on the phone.

Outbound Proxy **80.124.54.159** (Default: scsitel2.iteluk.com)

Only required if both the following conditions are true. First, you want to direct all outgoing SIP traffic to a server other than the address you specified for the registration server. Second, you want the outbound proxy only for this line. All other lines will continue to send traffic to the registrar. NOTE: If you want to set the outbound proxy for all lines, goto to the phone settings for "Sip Server"

Outbound Proxy Port

Outbound Proxy Transport **UDPOnly** (Default: UDPOnly)

serverFeatureControl.cf ☐ Enable/disable server-based call forwarding

serverFeatureControl.dnd ☐ Enable/disable server-based do not disturb

musicOnHold.uri **~mh~@scsitel2.iteluk.** (Default: ~mh~@scsitel2.iteluk.com)

Registration server

13. Open the **Devices** menu and select **Phones** to return to the phone list.

AVAYA Thu, 29 Apr 2010 12:04 PM Home Help Logout Search

Users Devices Features System Diagnostics

Registration

Line

Registration

Call Handling

Dial Plan

Messaging

Phone: 0004f21d9d

Line: "Frank Cortelli"

Registration

label

Text label to appear on the display adjacent to the associated line key. If omitted, the label will be derived from the user part of "Registration Server"

lcs

Microsoft 2005 LCS server

SCA barge in ☐ (Default: unchecked)

Phones

Phone Groups

Gateways

SBC Routes

Device Files

Network Parameters

Discover Devices

Device Time Zone

oint IP 550/560

sluk.com>

Show Advanced Settings

14. Tick the phone's check-box and then click on **Send Profile** to upload the phone data to the FTP server.

☐	001b386bd1d0	202	Polycom VVX IP 1500 v2.0	
☐	001b387bd1d0	202	AudioCodes MP114 FXS v6.0	
☐	002162ff7032		Avaya 1220 IP Deskphone	Auto-provisioned ID: 47T Version: SIP12x0.01.02.13.00
☐	paulsoftclient	203	Avaya 3456 UC Client	
☐	xxxxxxxxxx	200	Avaya 3456 UC Client	
☐	0004f21e794a	208	Polycom SoundPoint IP 650/670 v2.0	Auto-provisioned ID: WJJ Version: 3.2.3.1734
☐	002162ff36b4	206	Avaya 1230 IP Deskphone	Auto-provisioned ID: 6QS Version: SIP12x0.01.02.11.00
☐	0004f21d8d5f	203	Polycom SoundPoint IP 550/560 v2.0	Auto-provisioned ID: QQ2 Version: 3.2.3.1734
☐	0004f21eea0d	207	Polycom SoundPoint IP 320/330 v2.0	Auto-provisioned ID: V3F Version: 3.2.2.0477
☒	0004f21d9d5f	201	Polycom SoundPoint IP 550/560 v2.0	Remote Worker Phone

<< < 1 > >>

Send Profiles Send All Profiles Restart Delete More actions...

Software Communication System (4.2.1-018680 2010-04-22T19:36:18)

Warning: If the first line configured on the restarted phone is also registered on other phones, then restarting this phone via the *Send Profiles* function will also restart those other phones. This includes phones used as attendant consoles.

15. Once complete, click **OK** to confirm profile sending.

The phone profile is now ready for collection by the phone. The easiest way to do this is to connect the phone to the network using DHCP and set the FTP address to the IP address of the SCS.

Configure DHCP and FTP on the Phone

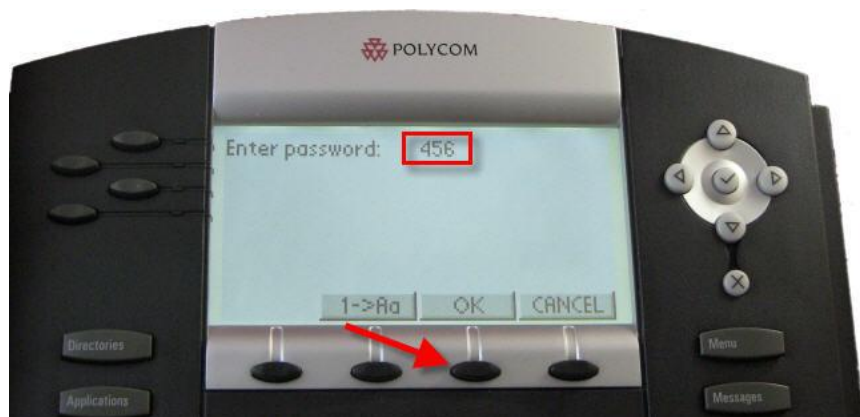
Note: You will only need to configure an FTP address if Option 66 is **not** utilized on your DHCP server. Option 66 can be used to automatically issue devices with the location of TFTP/FTP services when they acquire their IP address from the DHCP server.

By default, a new phone should be set to automatically request an IP address via DHCP as soon as it is connected to the network. In the event that the phone has previously been configured with static IP information, DHCP will need to be enabled.

1. Connect the phone to the network and power it up. When the 'Welcome' screen appears, press the **Setup** soft key.



2. Enter the administration password to access the configuration screen – by default this is set to **456** – and press the **OK** soft key.

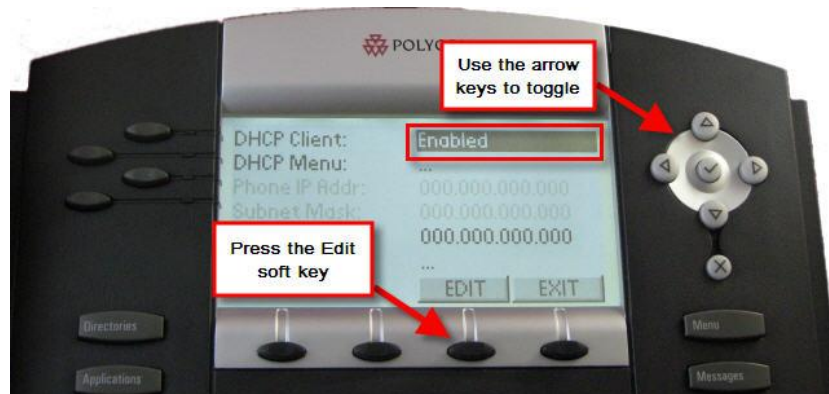


Note: To access the Setup utility if the phone is already powered up:

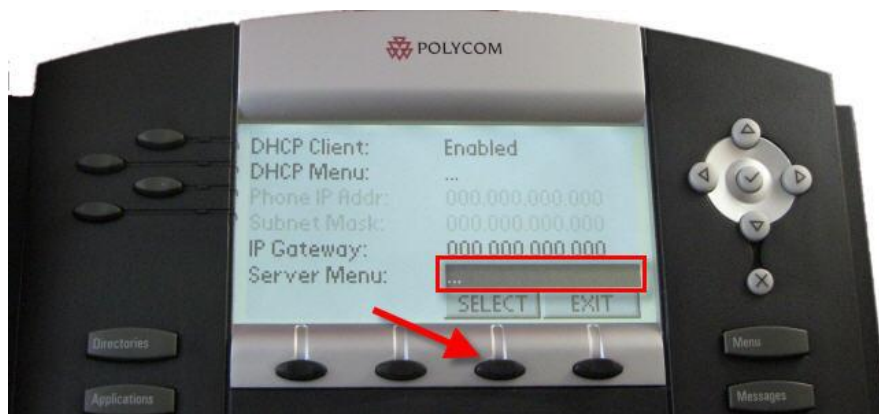
1. Press the **Menu** button.
2. Select option 3, **Settings**.
3. Select option 2, **Advanced**.
4. Enter the administrator password – 456 by default – and press the **Enter** soft key.

5. Select option 1, **Admin Settings**.
6. Finally, select option 1 **Network Settings**.

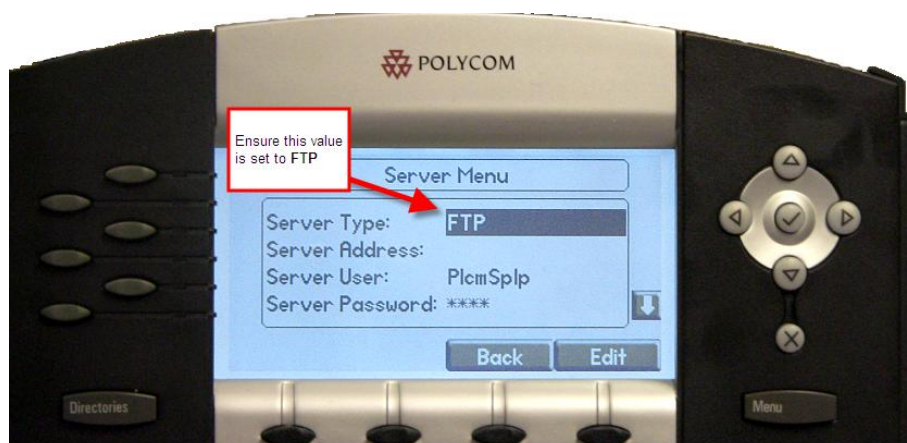
3. The first option in the configuration menu is the DHCP option. This can either be enabled or disabled. By default, DHCP should be enabled. If it is not, press the **Edit** soft key, or the tick in the center of the navigation cross key, and then press **Up**, **Down**, **Left**, or **Right** on the navigation cross to toggle between 'disabled' and 'enabled'. Press the **OK** soft key or the tick button to set the option and continue.



4. Use the arrow keys to scroll down to the **Server Menu** option and press the **Select** soft key.

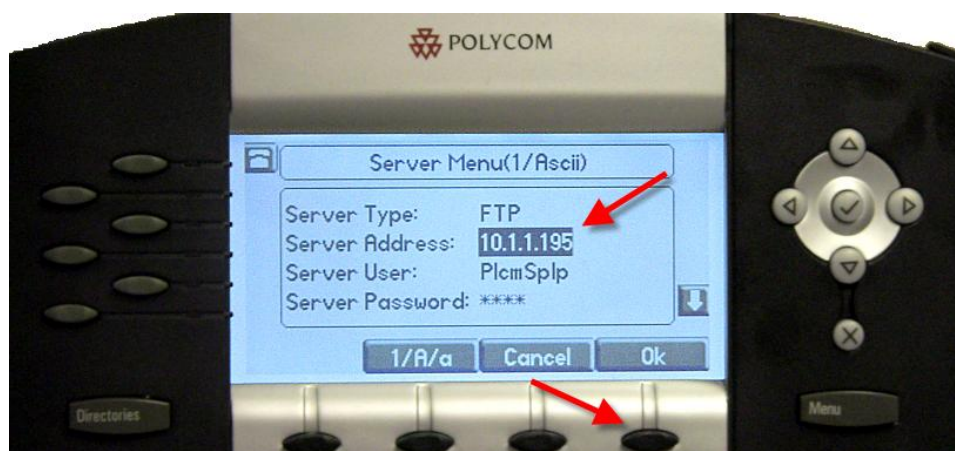


5. Ensure that the 'Server Type' is set to the default setting: **FTP**. If it is not, Press the **Edit** soft key to access the setting and then use the arrow keys on the navigation cross to set the option to **FTP**.



6. Press the **OK** soft key to confirm this setting and highlight the next option: **Server Address**.
7. Press the **Edit** soft key and then enter the IP address of the SCS server (press the star key * to enter dots and the **a->1A** soft key to toggle between numeric and alpha input). Press the **OK** soft key to continue.

To delete a character use the 'x' button or, if your phone does not have this button, press the **Left** arrow on the navigation cross.



8. Press the **Exit** soft key to return to the main configuration screen.
9. Configuration is complete, press the **Exit** soft key again to completely exit the configuration utility.

10. Using the arrow keys, navigate to and highlight the **Save and Reboot** option and then press the **Select** soft key.



The phone will now reboot and attempt to pick up any profile information stored on the SCS server.

Note: Before rebooting the phone, ensure that all necessary user and phone profile configuration steps have been carried out on the SCS server – see the 'Configuring User Profiles' guide.

When the phone finishes rebooting setup will be complete, If successful the user's user ID (name or extension number usually) will be displayed on the screen. The phone can now be boxed and shipped to the remote user.

Note: If the phone requires any future changes to its configuration – e.g., if the SCS domain name changes – it will have to be shipped back to the SCS and updated via SCS provisioning.

Avaya Documentation Links

- [SCS 4.0 Configuring User Profiles Task Based Guide](#)
- [SCS 4.0 System Configuration Task Based Guide](#)
- [SCS 4.0 Device Configuration - Getaways Task Based Guide](#)
- [SCS 4.0 Troubleshooting Task Based Guide](#)