SCS 4.0

Troubleshooting

Task Based Guide

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

Table of Contents

Troubleshooting

Introduction

There may be occasions when users and administrators encounter operational issues with the SCS. Often such issues are caused by minor configuration errors or incorrect usage of a particular function. Normally such issues can be solved by following set procedures to identify the source of the problem and then taking steps to rectify it in the quickest time possible – usually these procedures start with the simplest and most innocuous causes and then work towards more complex issues. This guide aims to provide you with some of the more common issues you may come across when using the SCS and their solutions.

Note: For outage and system recovery related issues please see the SCS 'Disaster Recovery Planning Guide'.

As well as the steps suggested in this guide, you might also consult some of the following diagnostic tools when trying to resolve a problem:

- **Registrations** – The Registrations facility provides information on the status of users registered to the SCS.

- **DNS Advisor** – Determines and validates DNS records required for the SCS

- **Call Detail Records** – Call Detail Records show historic call data and can be filtered to provide information based on particular names or dates.

- **Statistics** – The Statistics diagnostic can be used to find information on performance-related issues, for example: HDD usage, memory availability, and CPU load.

- **Alarms** - The alarm server collects alarms in the system and sends out notification to system administrators. The advanced section displays all alarm types defined by the system. You can enable/disable e-mail notification on each alarm type.

- **Syslog** - The location of a Syslog Server can be defined that is used to obtain Syslog messages from devices connected to the SCS, such as Phones or Gateways that have Syslog enabled. Logs from these devices will be sent to the Syslog server. The logs can then be collected with the SCS snapshot facility.

- **ACD Reports** – Use ACD Reports to generate reports on the ACD queue, including: agent availability, queue activity, and abandoned calls.

- **Job Status** – The job status page shows the status of various processes on the SCS, for example phone profile creation, file replication across a high availability configuration.

- **Configuration Tests** – These are a collection of tests that can be run to test the availability of certain services that support the SCS infrastructure. Available tests include: DHCP server verification, TFTP service verification, local host configuration. You may be asked to run some of these tests in a support call scenario.

- **Services** – The Services utility enables you to stop or restart services, as well as refresh service status. It is recommended that you only access this area if instructed to by a support engineer or documentation.

- **Snapshot** – The Snapshot tool is a very useful facility that allows you to create an instant archive of SCS and Apache web server logs and other diagnostic information. Output can be filtered to particular time ranges or user names. Again, you may be requested to create snapshot logs by a support representative.

Note: When a Snapshot is taken in a HA environment, 2 Snapshots are produced one for Master and other for the distributed system

- **Login History** – Use the Login History tool to create a report showing successful and unsuccessful login attempts.

Scenarios

Problem: Unable to access the SCS GUI

Solutions:

There could potentially be any number of reasons why you are unable to access the SCS GUI, chief among which would be:

- **Connectivity between your workstation and the LAN** Start simple. Ensure that your workstation or laptop is connected to the LAN. Is the Ethernet cable securely connected to the network card on your workstation – if using Wi-Fi, make sure that you have a connection to your usual wireless access point.

  Once you have ensured that your physical or wireless connection to the LAN is intact try **pinging** the IP address of another device on the network – for example the default gateway or a neighbour's workstation. If the ping is successful then you know your workstation is connected to the LAN, if you still cannot access the SCS GUI, explore the other issues in this guide.

- **IP Address** Ensure that you have the correct IP address and domain name for the SCS – your SCS administrator should be able to inform you of the correct details.

- **Connectivity between the SCS and the LAN** Once you know that your workstation is connected to the network and that it can see other devices, and you are certain of the IP address and SCS domain name, it's time to check whether or not you can contact the SCS. Use Ping again and ping the SCS IP address. **If the ping packets are not returned then there is the possibility that the SCS is not connected to the network, in which case you may wish to escalate this issue to the network administrator.**

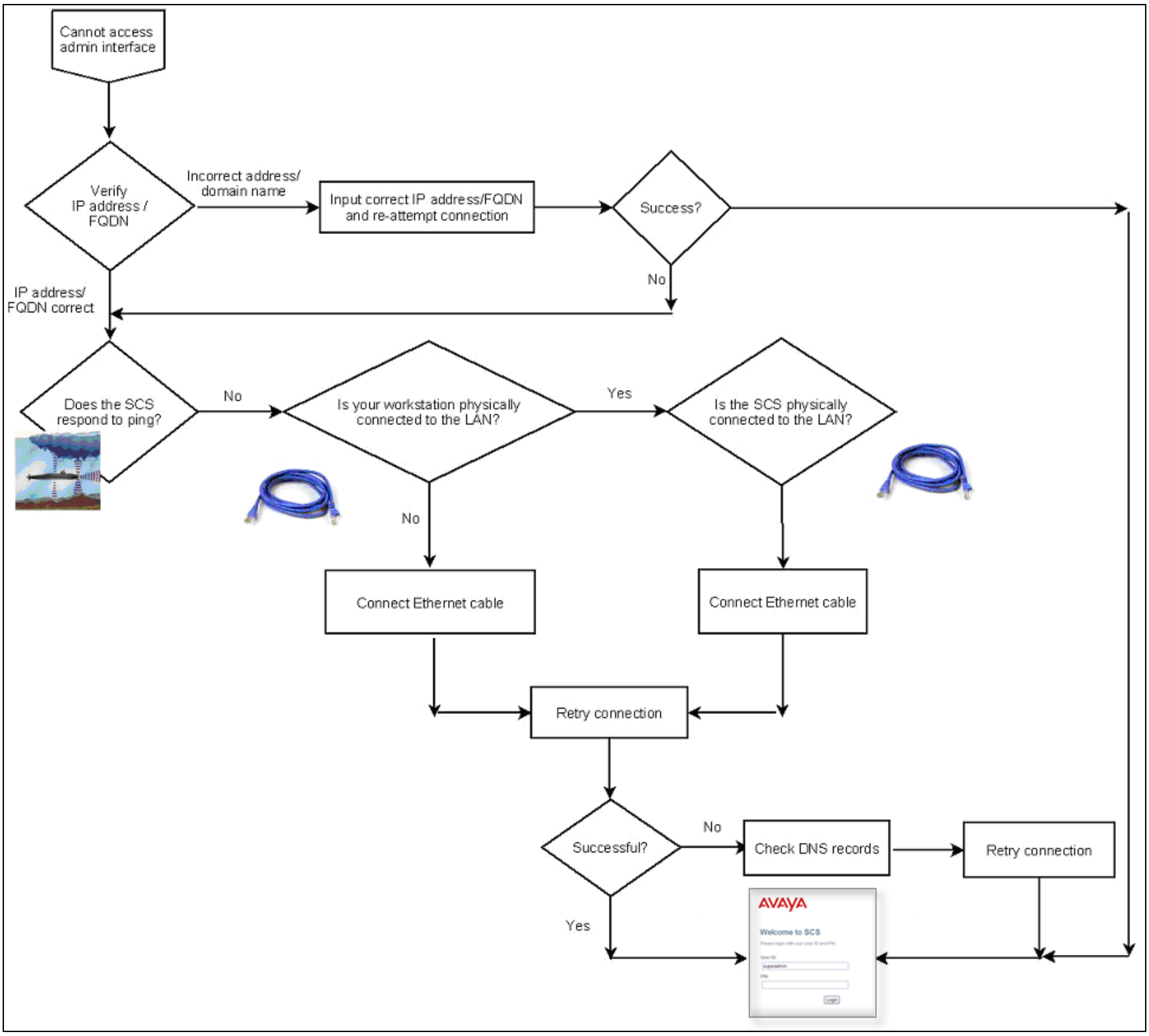
  If the ping packets are returned then you know that the SCS is connected to the LAN. Attempt to browse to the SCS GUI using the IP address instead of the Fully Qualified Domain Name (FQDN) in your web browser of choice. If you are able to browse to the SCS using the IP address but not the FQDN then there is a chance that there is a **DNS issue**.

- **DNS issues** In simple terms DNS is used to resolve address names such as *scs.scsdomain.com* to IP addresses, which is why if there is a DNS issue you will probably be able to browse to the SCS GUI using an IP address and not the fully qualified domain name. Not being able to browse to the GUI using the FQDN is a symptom of a larger problem because DNS plays an important roll in the SCS environment. If you suspect a DNS issue escalate the problem to your local network administrator.

- **Internet browser restriction** Some internet browsers can be configured to connect to the Internet through a proxy. This can cause some issues when attempting to connect to the SCS GUI. Proxy settings can be disabled within IE and Firefox in the following way (check with your network administrator that it is OK to disable proxy settings first):

    - **Mozilla Firefox 3.5:** Open the **Tools** menu and select **Options**. Click on the **Advanced** tab and select the **Network** sub-tab. Under the **Connection** header, click on **Settings**. Select **No Proxy**. Click **OK** to confirm changes and exit the options screen.

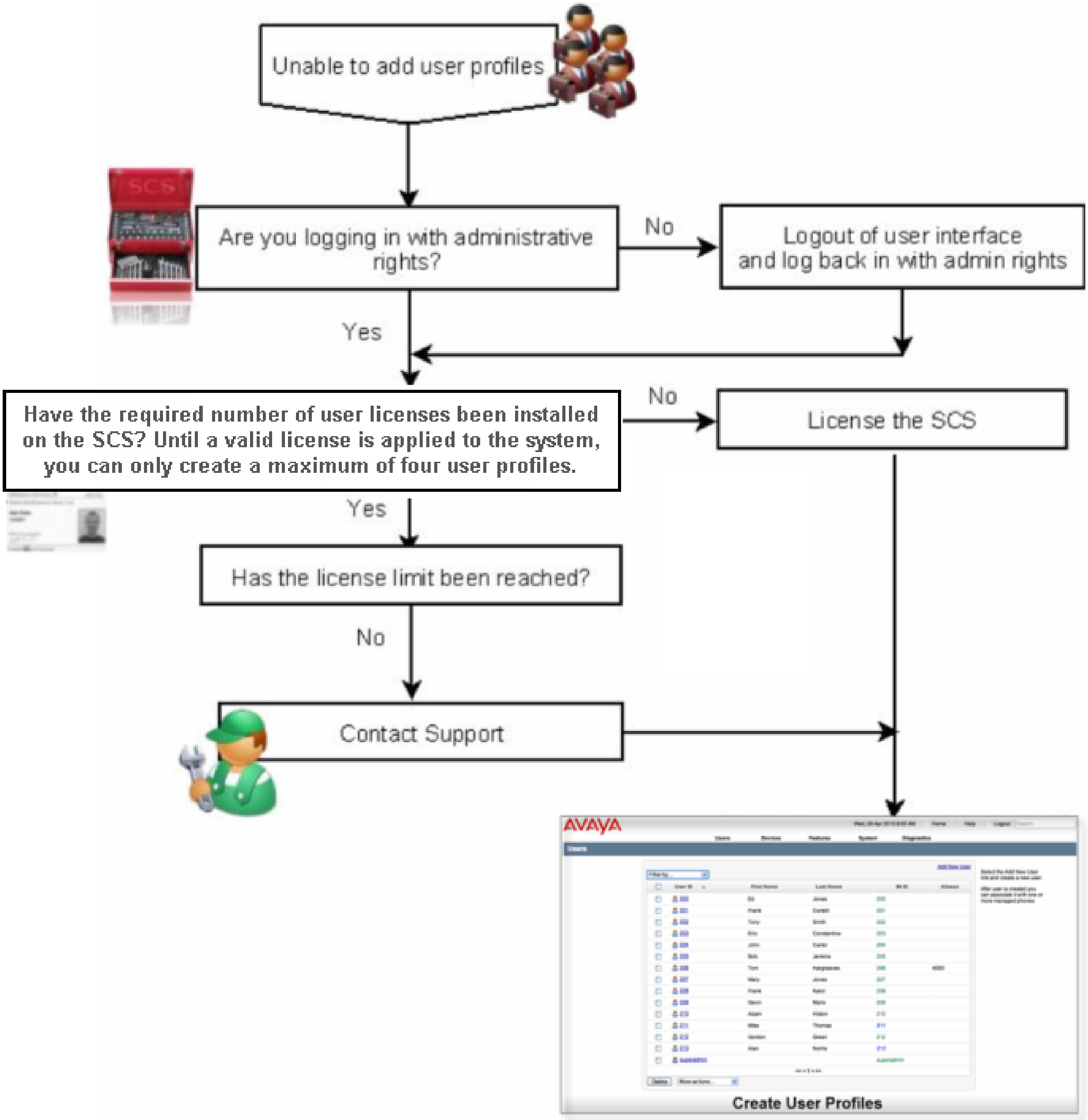
    - **Microsoft Internet Explorer 7:** Open the **Tools** menu and select **Internet Options**. Click on the **Connections** tab and then the **LAN settings** button. Under the **Proxy server** heading, untick the **Use a proxy server for your LAN** check-box. Click the **OK** button to confirm changes and exit the options screen.


Cannot access admin interface
Verify IP address / FQDN
Incorrect address/ domain name
Input correct IP address/FQDN and re-attempt connection
Success?
No
IP address/ FQDN correct
Does the SCS respond to ping?
No
Is your workstation physically connected to the LAN?
Yes
Is the SCS physically connected to the LAN?
No
Connect Ethernet cable
Connect Ethernet cable
Retry connection
Successful?
No
Check DNS records
Retry connection
Yes
AVAYA
Welcome to SCS

Problem: Cannot create user accounts

Solution:

In order to create user accounts on the SCS, the system must be licensed to support the required number of users. If you are unable to create new accounts then there is a strong chance that either the system has not been licensed or the maximum number of allowed user accounts has been reached. See your SCS administrator or contact Avaya for further licensing options. Also, please see the 'System Configuration' guide for more on licensing the system.



Problem: Incoming calls do not route to SCS user DIDs

Solutions:

Calls can be routed to individual **DIDs** (Direct Inward Dial) in one of two ways, you can either:

1. Configure a dial plan for every user which defines where calls to a certain number route. For example, all calls to 670238 are routed to User ID 238. This is a perfectly valid way of routing calls to individual worker DIDs but a **Custom Dial Plan** will need to be created for **every** worker.

   If you find that this solution is not working, ensure that:

   - All plans have the correct **Dialled Number Prefix** (that is the number that callers will dial to reach the user) entered – you can check these with your service provider.

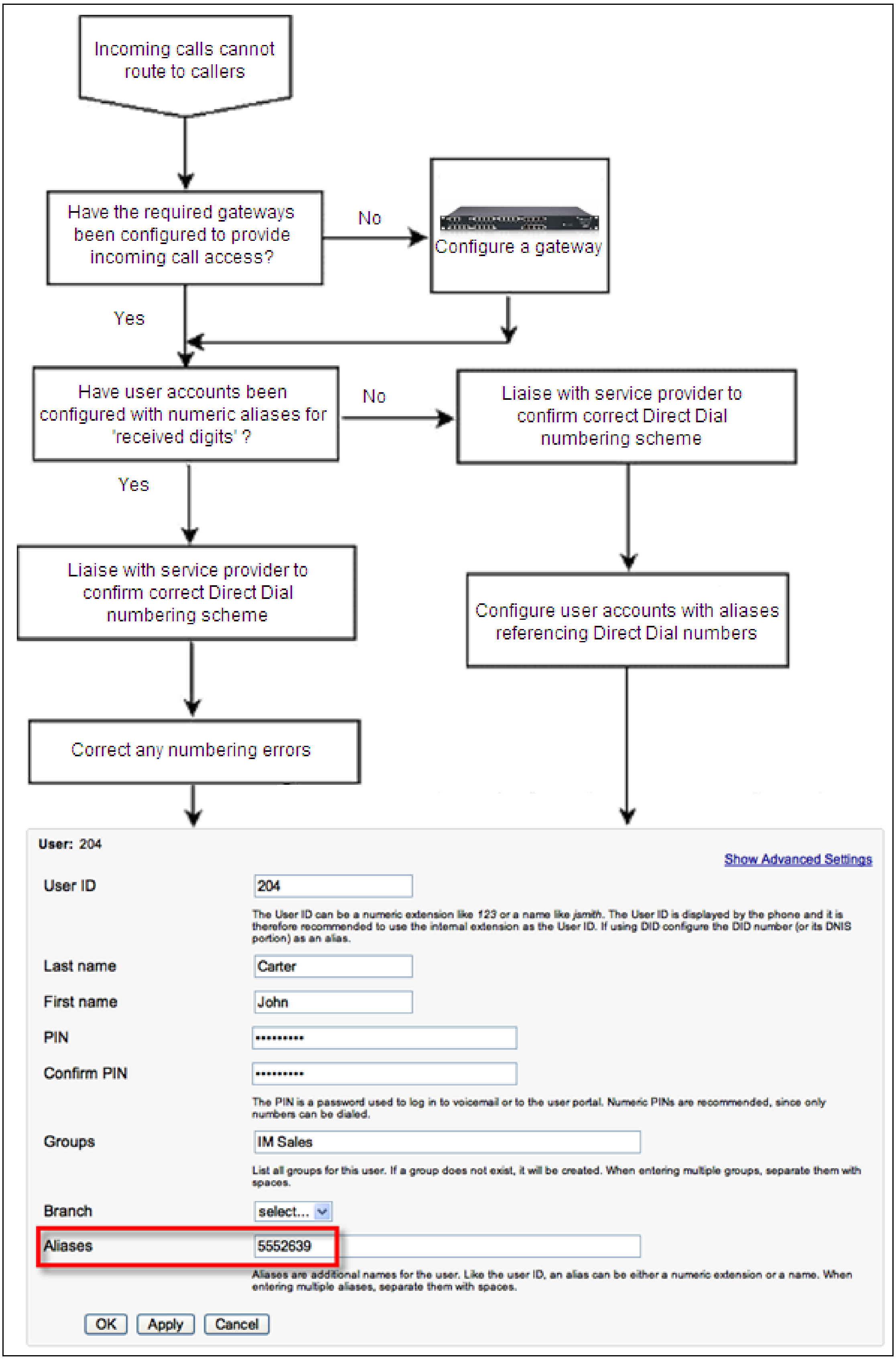
   - The **Resulting Call** field is populated with the correct user ID/extension.

   - All plans have been **enabled**.

   For more on Dial Plans see the SCS 'System Configuration' guide.

2. Define an **Alias** for every user that is made up of their DID. This approach eliminates the need to create a separate dial plan for every worker in the system.

   All user accounts must have a User ID. This is a unique identifier that marks the user out from everybody else on the system, it can be a number (a three digit extension for example) or a name (johns). As well as the User ID, you can define **Aliases**, which are effectively another name by which the user is known on the system. Aliases can be anything you like but must be unique. To facilitate direct inward dialling you could assign every user their DID as an alias; that way, when a call comes in to those numbers the SCS will know exactly where to send the call. For more on Aliases, please see the 'Configuring User Profiles' guide.


Incoming calls cannot route to callers
Have the required gateways been configured to provide incoming call access?
No
Configure a gateway
Yes
Have user accounts been configured with numeric aliases for 'received digits' ?
No
Liaise with service provider to confirm correct Direct Dial numbering scheme
Yes
Liaise with service provider to confirm correct Direct Dial numbering scheme
Configure user accounts with aliases referencing Direct Dial numbers
Correct any numbering errors
User: 204
Show Advanced Settings
User ID
204
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
Carter
First name
John
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.
Groups
IM Sales
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
select...
Aliases
5552639
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.
OK
Apply
Cancel

Problem: Managed IP phones (phones automatically provisioned and managed by the SCS) do not register

Solutions:

If you are unable to register a managed phone to the SCS then the problem lies either with the SCS or the phone itself.

1. On the SCS check the following:

- Has a **Phone Profile** for the phone in question been created?
- Has a user account been added as a Line to the phone profile?
- Has the profile been **sent**?

Before a managed phone can register to the SCS a profile must first be created on the SCS. This profile contains information about the phone and the user who will be using the phone (described in the profile as a 'line'. The profile must be 'sent' to the SCS TFTP server so that it can be collected by the phone device when it boots on the network.

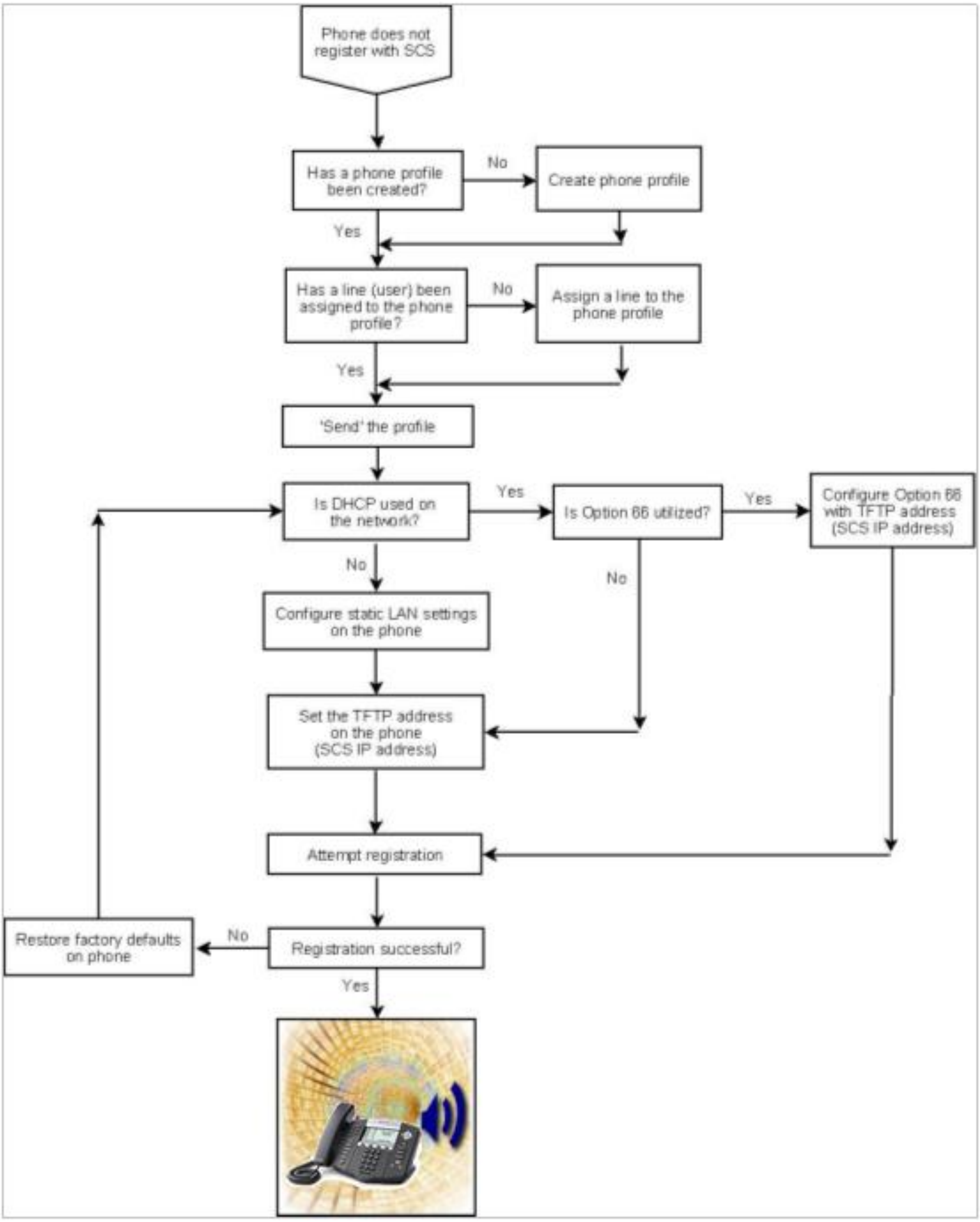
For more on creating phone profiles, please see the 'Configuring User Profiles' task based guide.

2. In order for the phone to successfully gather its profile information, certain phone and/or network settings must be configured:

   - **DHCP Option 66** can be configured to 'point' phones at the SCS for profile collection. This is not mandatory but can make configuring a phone quick and easy. If Option 66 is not utilized you will have to configure the IP address of the SCS as the TFTP value on the phone manually when you configure other LAN settings.

   - **Phone LAN Settings**. Either enable DHCP to allow automatic configuration LAN settings, or configure LAN settings manually. Once LAN settings have been configured, set the TFTP address if Option 66 is not in use, this is the IP address of the SCS.

For more on configuring settings on a managed phone see the Configuration Task Based Guide appropriate to your phone model.



Problem: Users cannot access voicemail

Solutions:

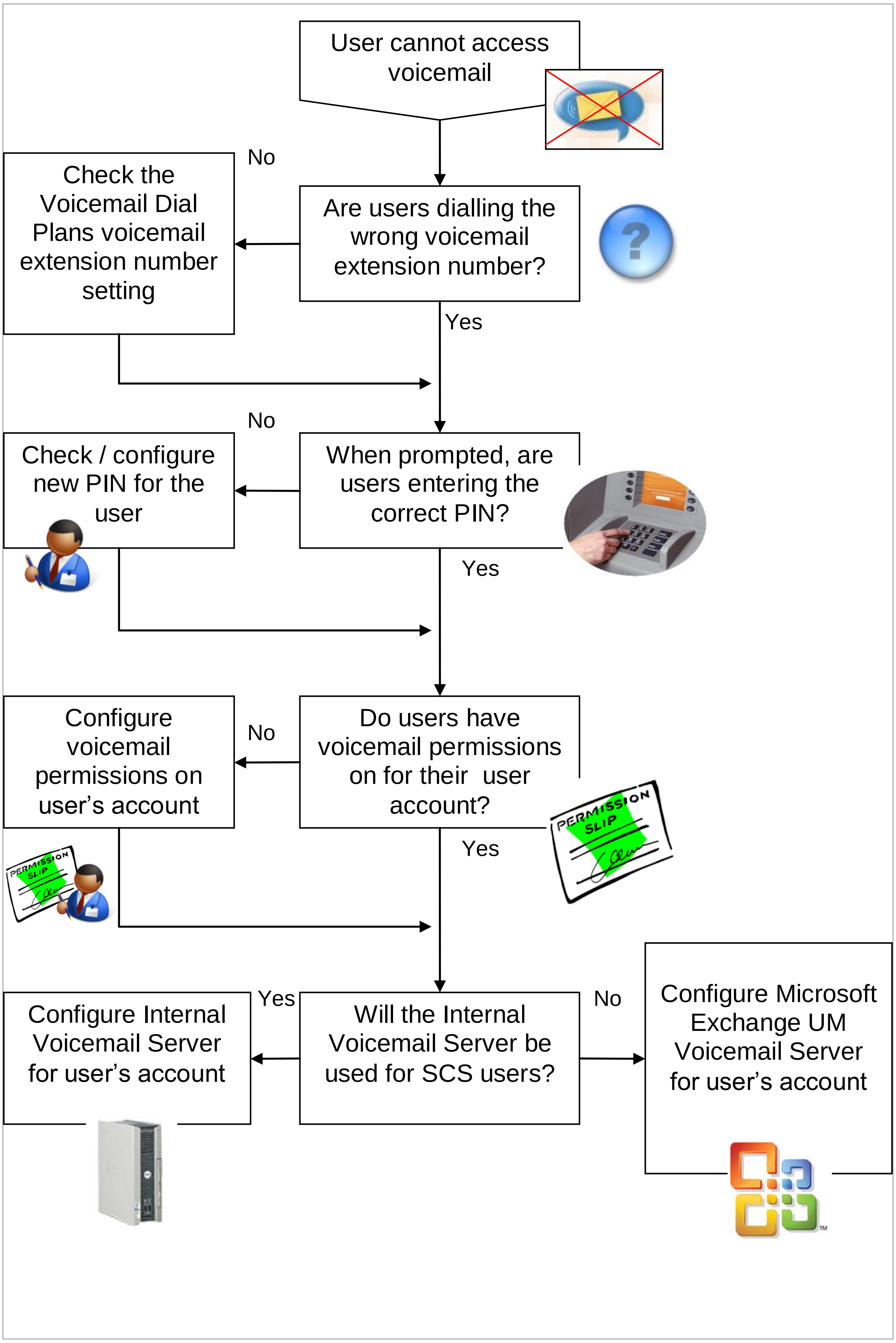
There are four possible reasons why a user would not be able to access their voicemail inbox:

- They are dialling the wrong voicemail extension number. Check the number that has been configured in the **Voicemail Dial Plan**. See the 'Voicemail Setup and Operation' guide for more on this.

- They are using the wrong PIN. Check the PIN.

- They do not have permission to access voicemail. Ensure that the **Voicemail** permission is checked on their user profile permissions page – see the 'Configuring User Profiles' guide for more.

- The user account has been configured with the wrong voicemail service, e.g., Internal voicemail service instead of Microsoft Exchange UM Voicemail service. See the 'Voicemail Setup and Operation' guide for help on selecting a voicemail service.


User cannot access voicemail
Are users dialling the wrong voicemail extension number?
No
Check the Voicemail Dial Plans voicemail extension number setting
Yes
When prompted, are users entering the correct PIN?
No
Check / configure new PIN for the user
Yes
Do users have voicemail permissions on for their user account?
No
Configure voicemail permissions on user's account
PERMISSION SLIP
Yes
Will the Internal Voicemail Server be used for SCS users?
Yes
Configure Internal Voicemail Server for user's account
No
Configure Microsoft Exchange UM Voicemail Server for user's account

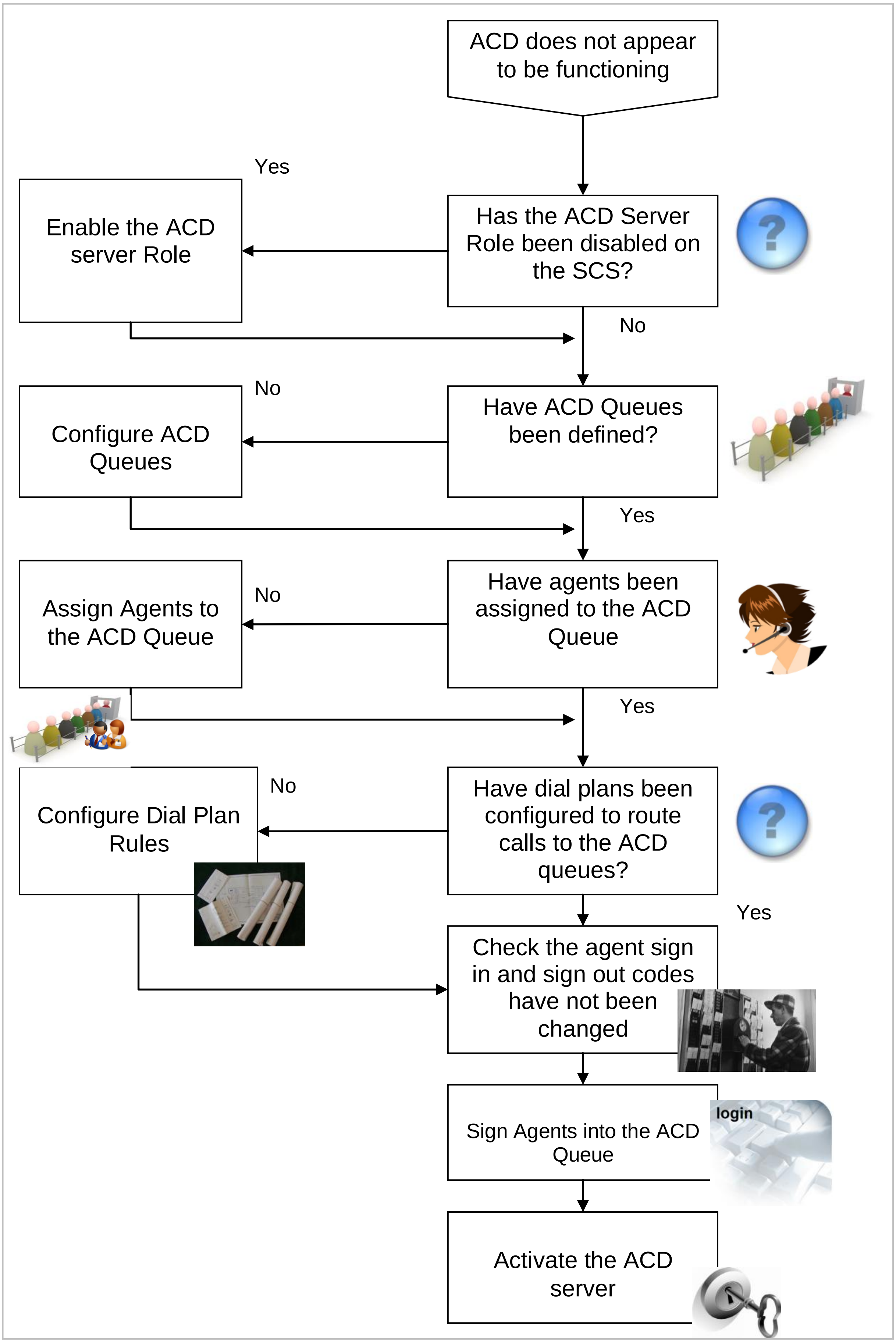
Problem: ACD does not function

Solutions:

There are several configuration details that you should check:

- Check that the ACD server role has not been disabled on the SCS.
- Define ACD queues. The ACD queue determines how incoming calls are handled and potentially queued.
- Assign agents to queues to ensure that agents can log in and receive calls. If there is no queue then agents cannot field calls.
- Check that agents are signed in to the ACD queue.
- Ensure that a dial plans exist to ‘point’ to the correct ‘ACD Line’. An ACD line is a virtual line that defines how calls reach the ACD queue. ACD lines, like user extensions, have an identifier (for example, 500) or a DID number (for example, 200786). You therefore assign an ACD line to a queue in the same way that you would assign an extension to a user in order to direct calls to them.
- Check that the sign in and out codes used by agents is correct. The default sign in code is ***88**, the default sign out code is ***86**.
- Ensure that the ACD is ‘active’. Just because the ACD server is present it does not necessarily follow that it has been activated. If the server is not active the ACD will not function.

For more help on the ACD please see the ‘ACD Setup and Operation’ guide.

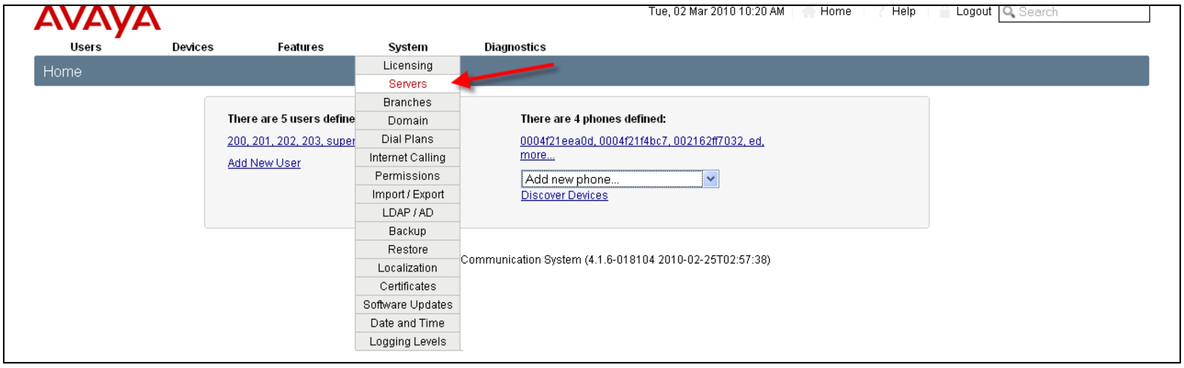

ACD does not appear to be functioning
Has the ACD Server Role been disabled on the SCS?
Yes
Enable the ACD server Role
No
Have ACD Queues been defined?
No
Configure ACD Queues
Yes
Have agents been assigned to the ACD Queue
No
Assign Agents to the ACD Queue
Yes
Have dial plans been configured to route calls to the ACD queues?
No
Configure Dial Plan Rules
Yes
Check the agent sign in and sign out codes have not been changed
Sign Agents into the ACD Queue
login
Activate the ACD server

Checking the ACD Server Role is Enabled

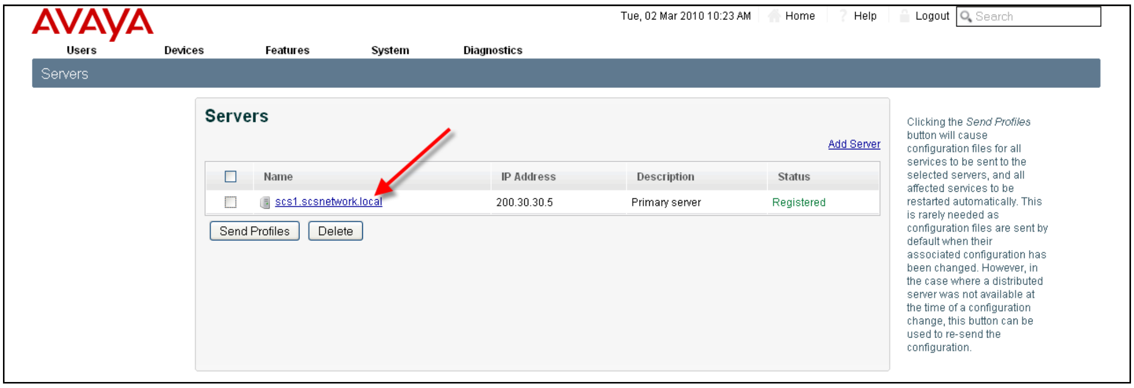
The ACD server role required for the ACD to function, is enabled by default on the SCS server. However, before commencing with ACD configuration, it is good practice to check the status of the server role to ensure the role has not been disabled.

To view the status of the ACD Server Role, navigate to the SCS server:

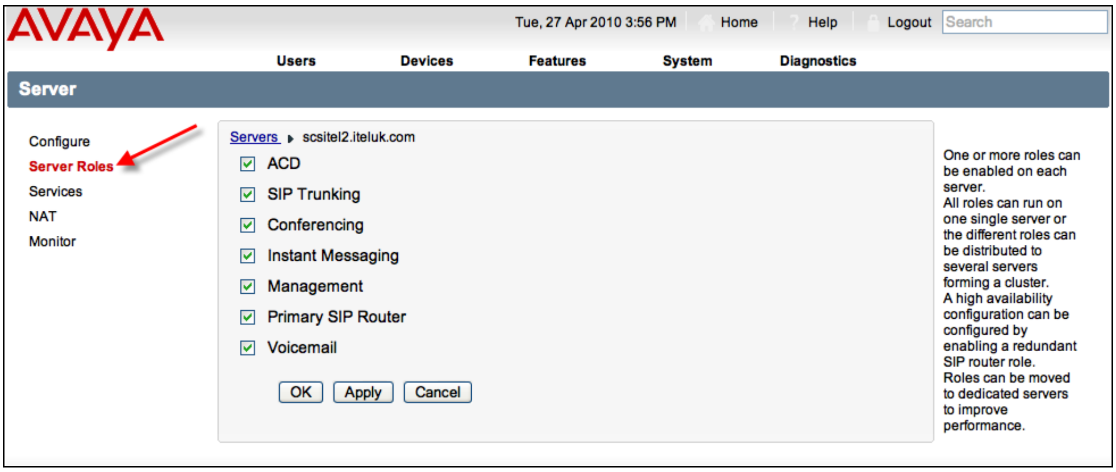
1. Click the **System** heading, followed by **Servers**.



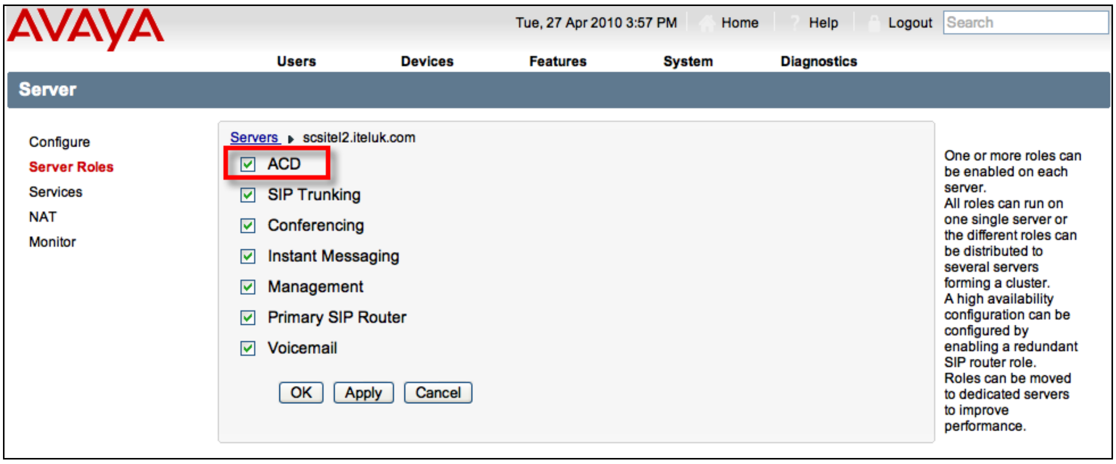
2. You will be presented with the **Servers** screen. Click the server's link.



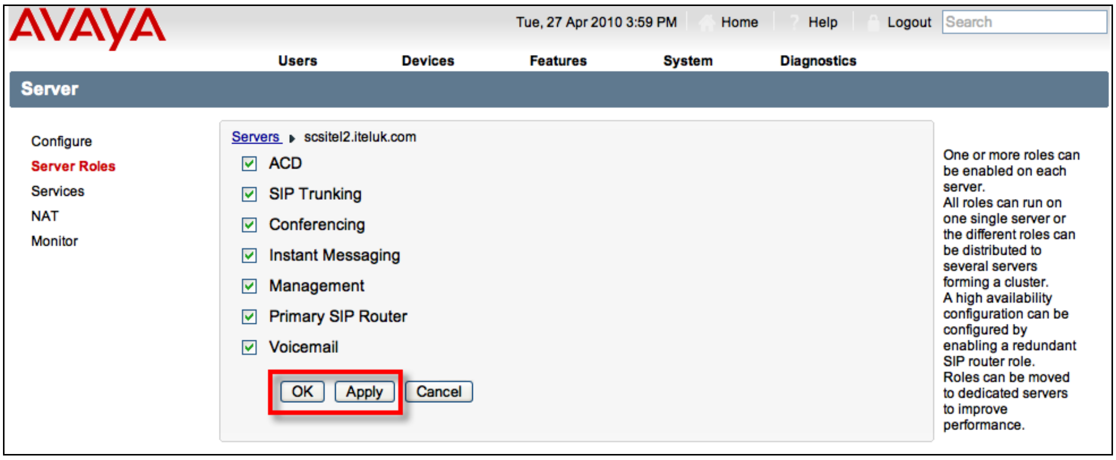
3. The **Server** screen will be displayed. Click the **Server Roles** link.



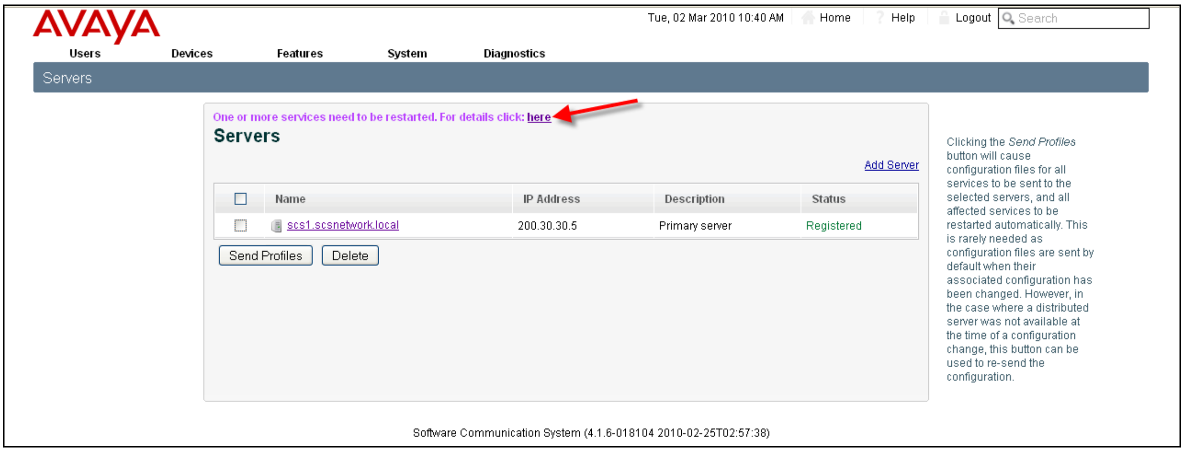
4. Within the grey panel, there are a number of checkboxes defining the server roles. The **ACD** check box should be selected by default.



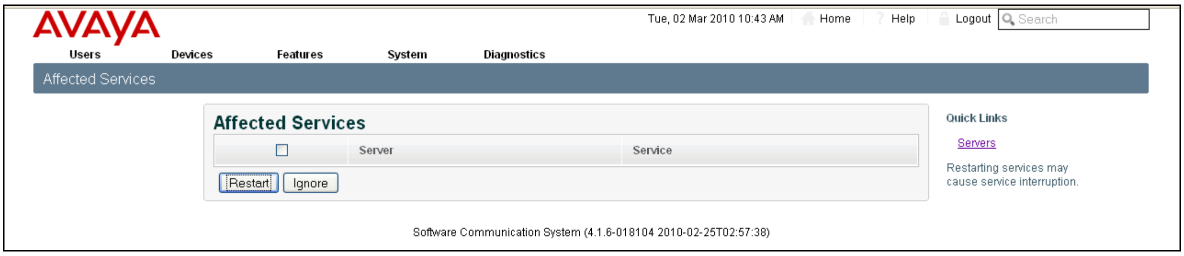
5. If it is not selected, click the **ACD** check box followed by the **Apply** button and the **OK** button.



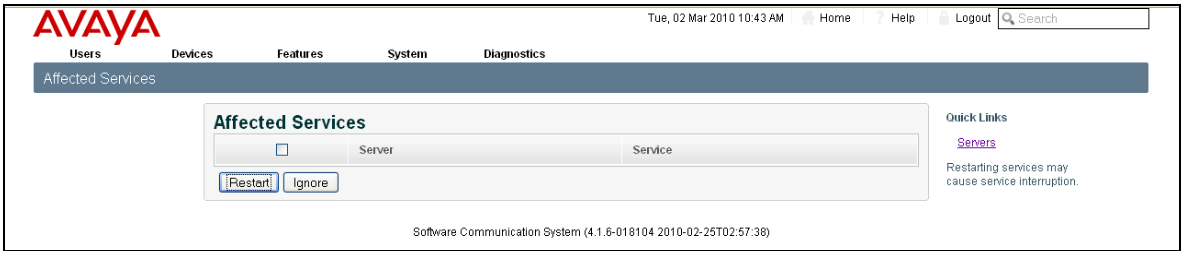
6. If changes have been made, you will be prompted to restart services. Click the **here** link.



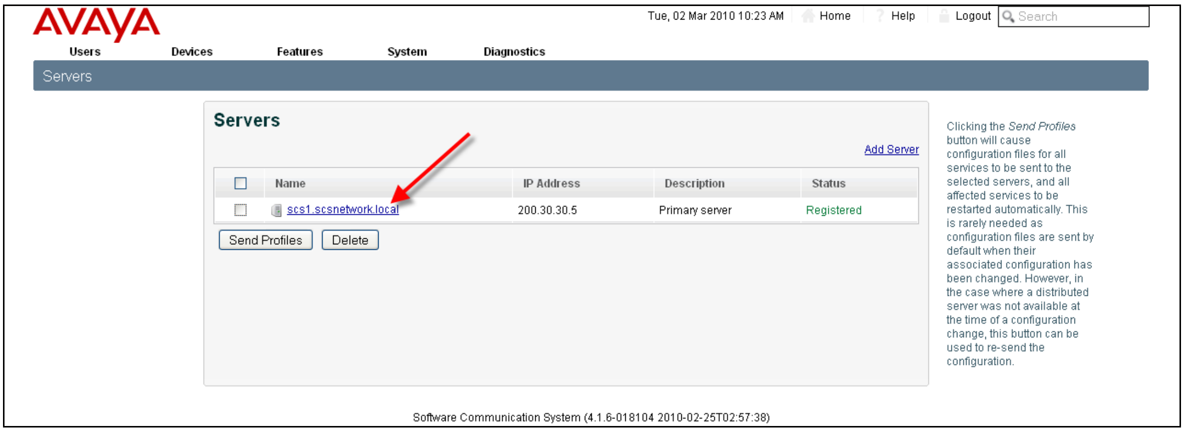
7. You will be presented with the **Affected Services** screen. Select the services and click **Restart**.



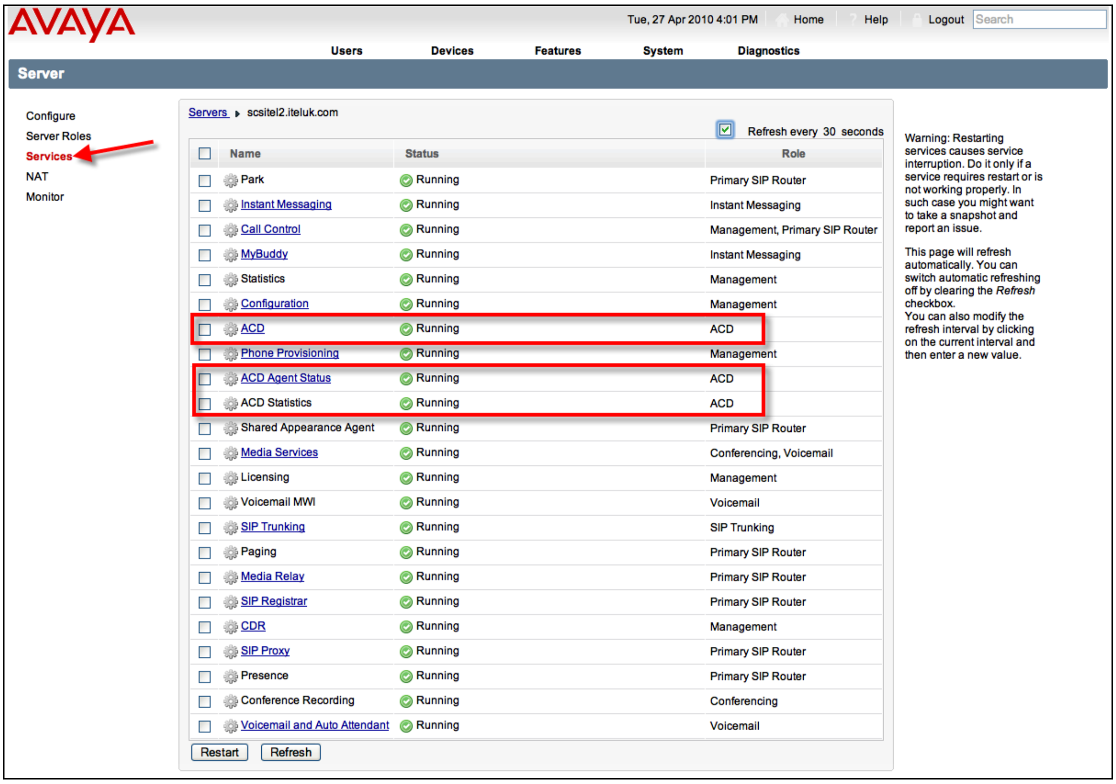
8. The affected services will be restarted.



9. To check that the ACD services are running, navigate to the **Servers** page and click the link for the SCS server.



10. Select the **Services** link. The ACD services will be displayed.



Problem: Auto-attendant is not functioning

Solutions:

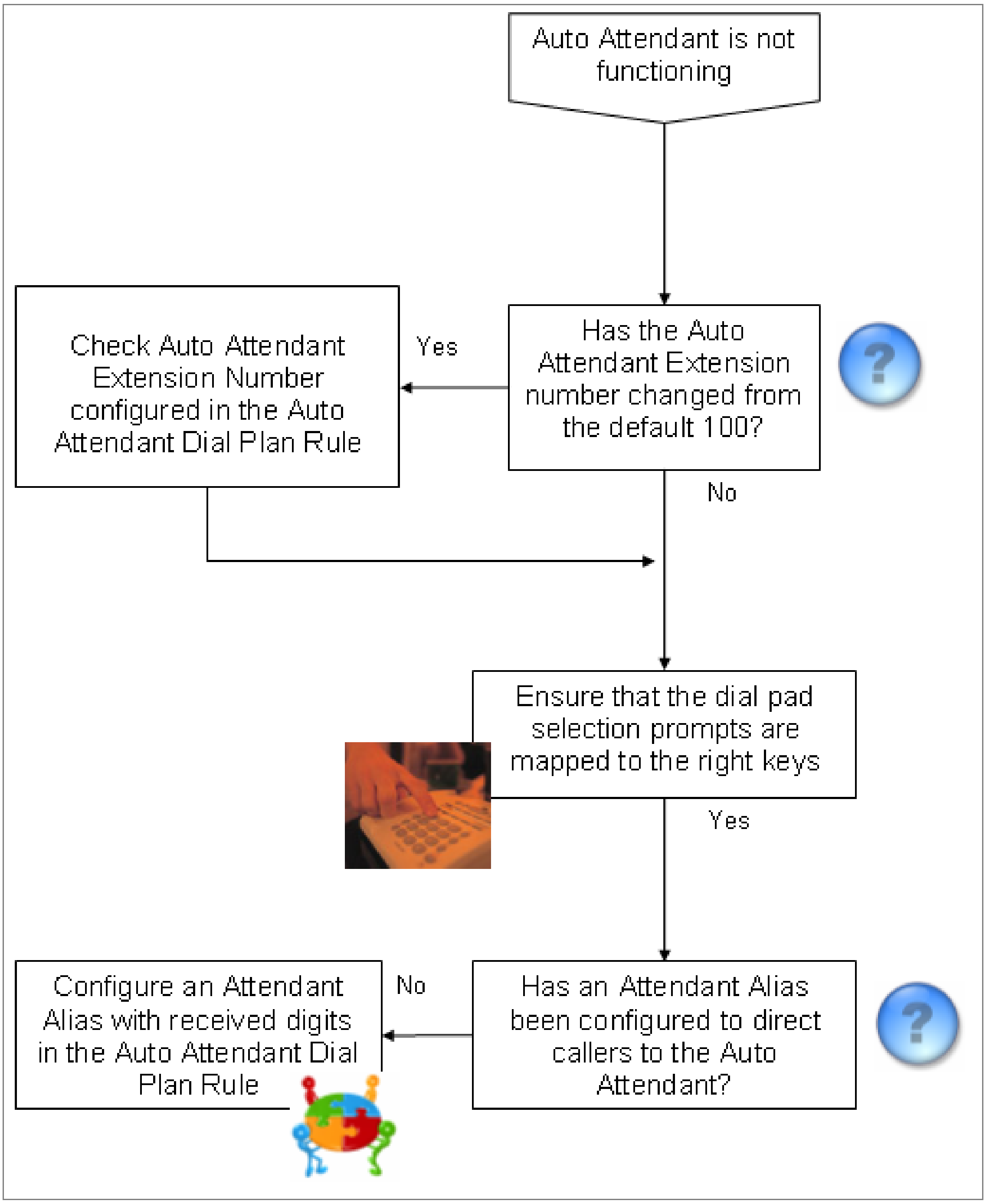
Auto-attendant issues can range from callers not being directed to the attendant (Operator) to users not being able to dial the attendant internally. If you experience any issues with the auto-attendant, check the following:

- Check that the right **extension number** is referenced in the auto-attendant dial plan (the auto-attendant dial plan is called Operator). By default the extension number is **100**. If users are dialling an extension number other than the one referenced in the dial plan they will not be able to access it.

- Ensure that the dial pad selection prompts are mapped to the right keys so that callers and users can access the right service from the right button.

- Callers will only be able to access the auto-attendant if the correct received digits are referenced in the dial plan under **Attendant aliases**.

For full instructions on configuring these options see the 'Auto-Attendant Setup and Configuration' guide.



Auto Attendant is not functioning
Has the Auto Attendant Extension number changed from the default 100?
Yes
Check Auto Attendant Extension Number configured in the Auto Attendant Dial Plan Rule
No
Ensure that the dial pad selection prompts are mapped to the right keys
Yes
Has an Attendant Alias been configured to direct callers to the Auto Attendant?
No
Configure an Attendant Alias with received digits in the Auto Attendant Dial Plan Rule

Problem: Contact names are not recognised by Dial-by-Name

Solution:

In order for contacts to be searchable using Dial-by-Name they must be added to the **Directory**. To be part of the directory a user must have the Directory **Permission** enabled in their user profile. Browse to a user's profile, select Permissions and ensure that the **Directory** option is ticked. SCS Users contained within the Directory must also record their name Refer to SCS 4.0 Voicemail Setup & Operation Task Based Guide.

Problem: Cannot 'Park' calls

Solution:

Check that call park **extensions** have been allocated and that the Call Park Service has been restarted.

Problem: Unable to retrieve parked calls

Solution:

Ensure that a **call park retrieval code** (*4 by default) been configured and also check that users are entering the right park extension number after the park retrieval code. This can be made more simple by configuring a speed dial of *4xxx on a user's phone – where xxx is the park extension - , the user could then retrieve calls simply by pressing the speed dial button.

For more on Call Park see the 'System Configuration' guide.

Problem: Unable to Page

Solutions:

Check the following:

- Are users dialling the correct **Paging Prefix**?
- Have **Page Groups** been defined and have users been added to page groups?
- Has the page group been **Activated**? An 'enabled' page group is not an 'activated' page group. In the page groups list, tick the check-box of the page group in question and then click the **Activate** button, then follow the pink link at the top of the screen to restart the paging service.

See the 'System Configuration' guide for more on paging.

Problem: **Directed Call Pickup not functioning**

Solution:

Check call **pickup code** on the **SIP Registrar** screen, accessed from the **Servers** page. In order to pick up a call, users must dial this code followed immediately by the extension number of the phone that is ringing.

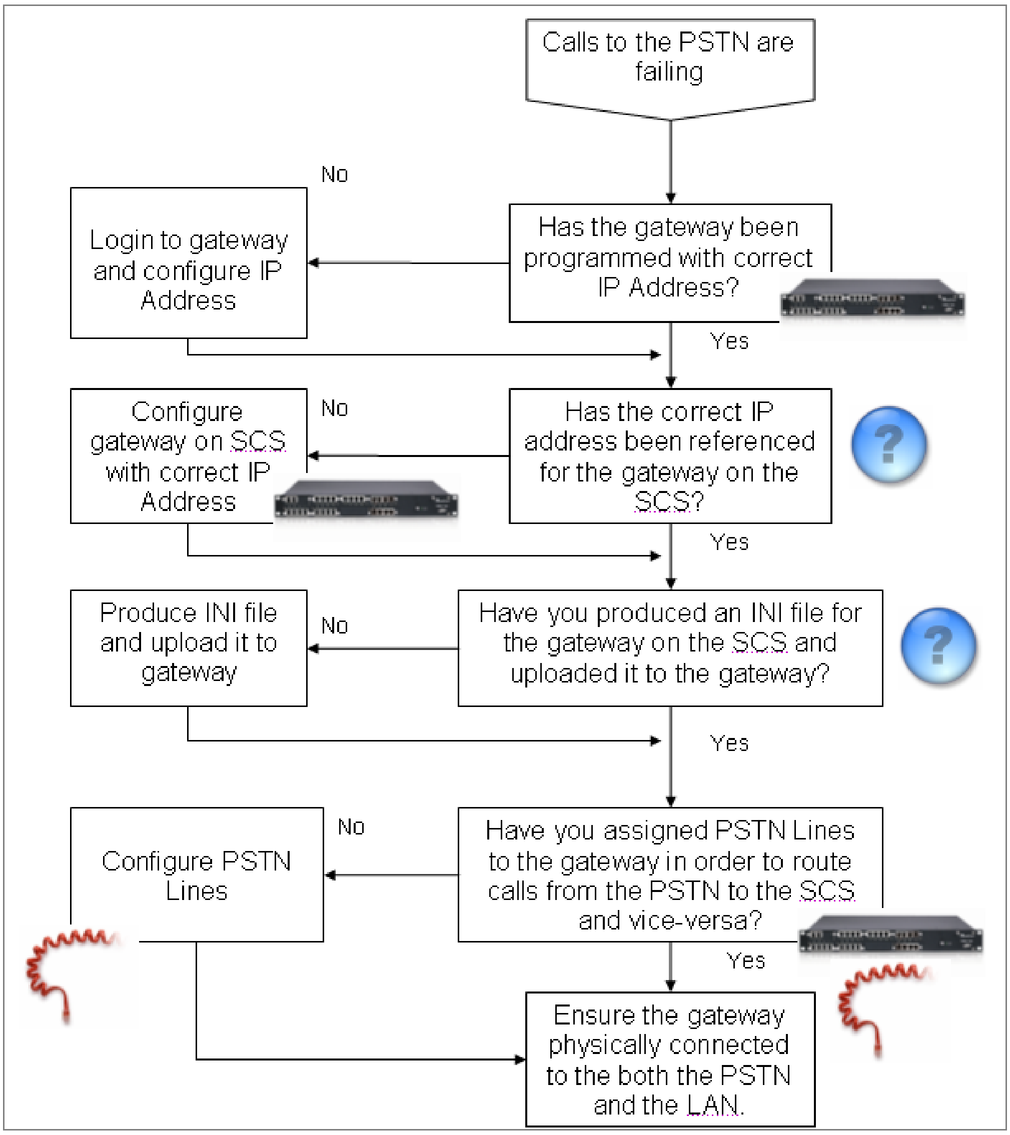
See the 'System Configuration' guide for more on call pickup.

Problem: Calls to and from the PSTN are failing

Solutions:

PSTN Gateways are devices that enable calls from the Public Switched Telephone Network (PSTN) to interface with telephone devices on the SCS. If you are unable to make or receive calls from or to the PSTN check the following:

- Has the gateway been programmed with the correct IP address?
- Has the correct IP address been referenced for the gateway on the SCS?
- Have you produced an INI file for the gateway on the SCS and uploaded it to the gateway?
- Have you assigned **PSTN Lines** to the gateway in order to route calls from the PSTN to the SCS and vice-versa.
- Ensure the gateway is physically connected to both the PSTN and the LAN.

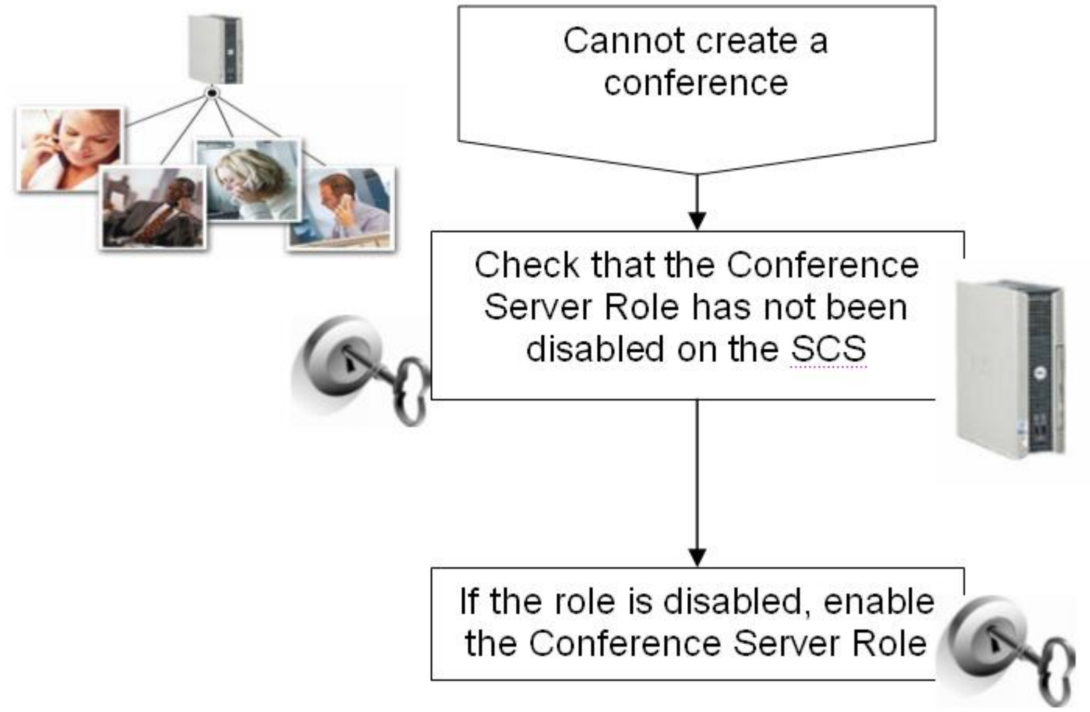


See the ‘Device Configuration – Gateways’ guide for detailed instructions on how to configure a PSTN gateway for use with the SCS.

Problem: Cannot create a conference

Solution:

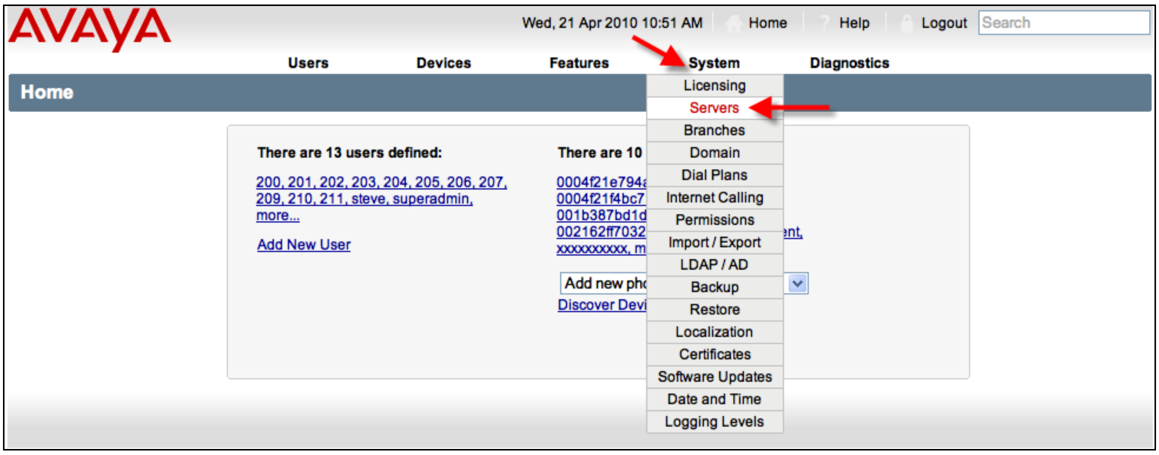
Check that the **Conference Server Role** has not been disabled on the SCS (Open the **System** menu, select **Servers**, and then click on the server to view enabled roles).



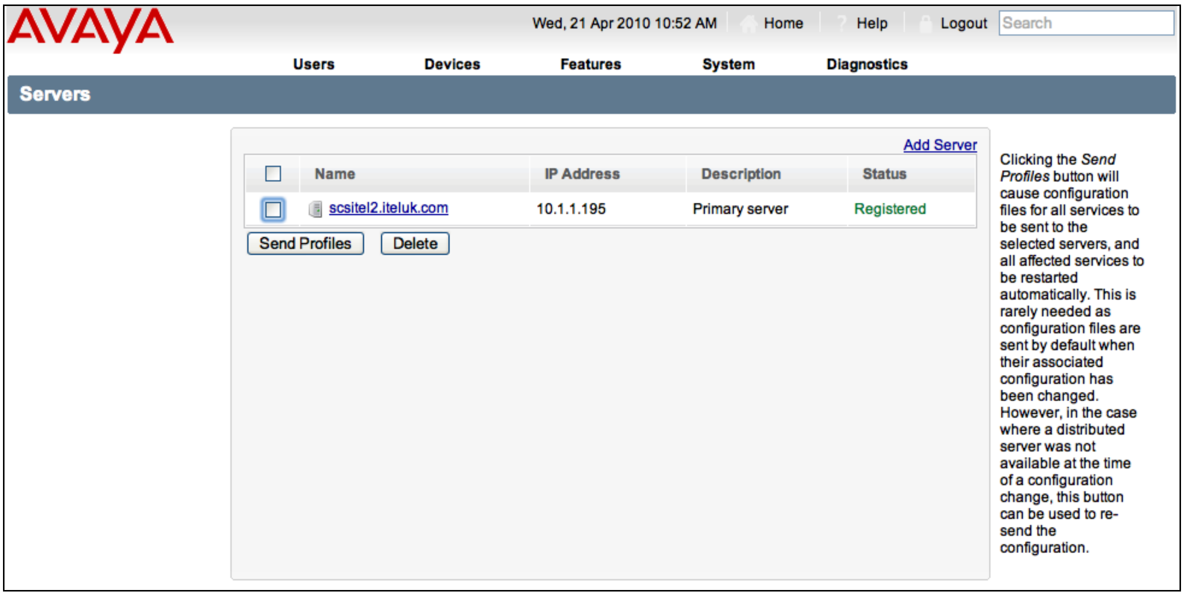
Checking the Conference Server Role

The Conference Server role is enabled by default on the SCS server. To check the enabled status of the server role:

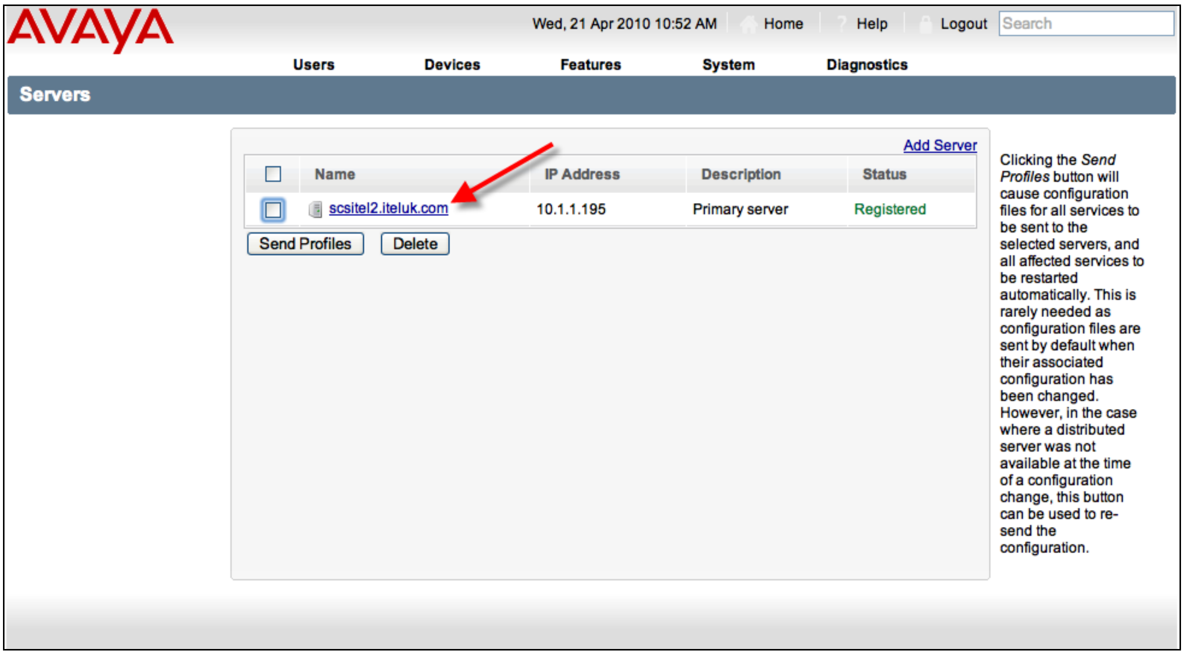
1. From the SCS Home Page, select the **System** link followed by **Servers**.



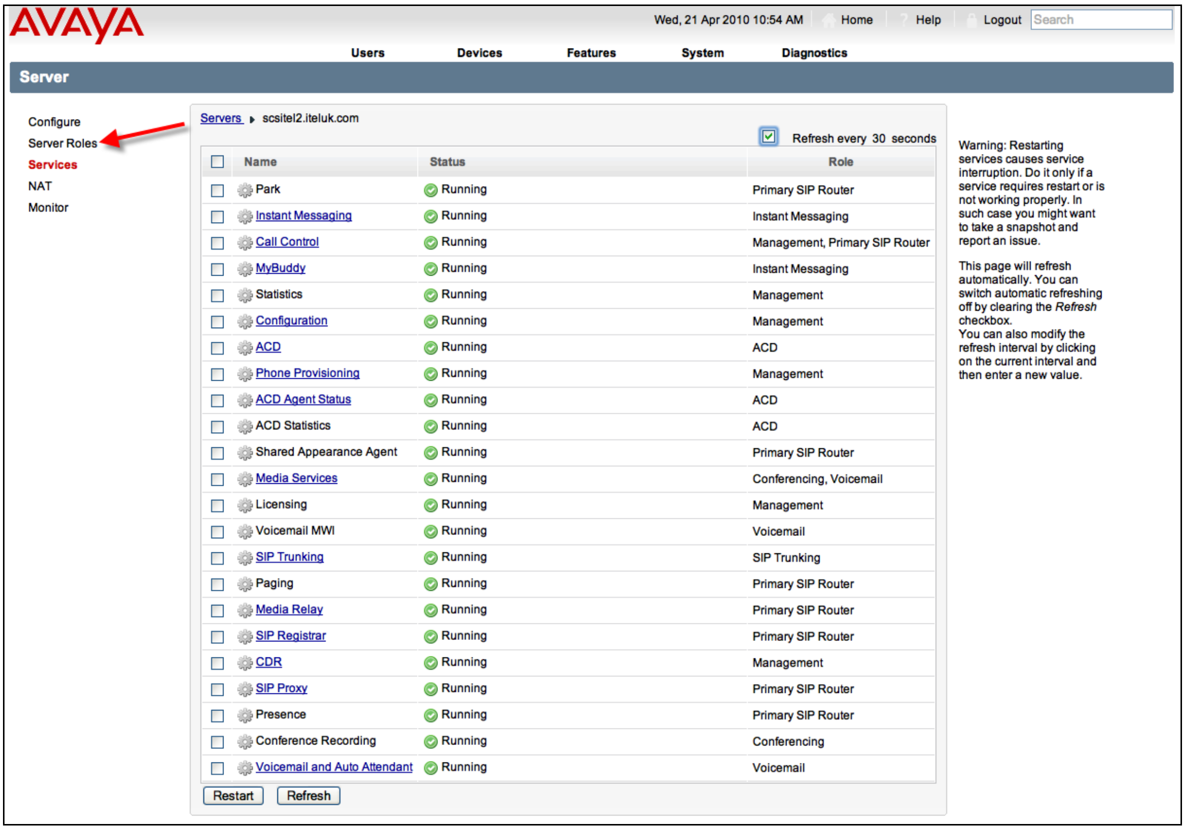
2. The Primary SCS Server will be displayed



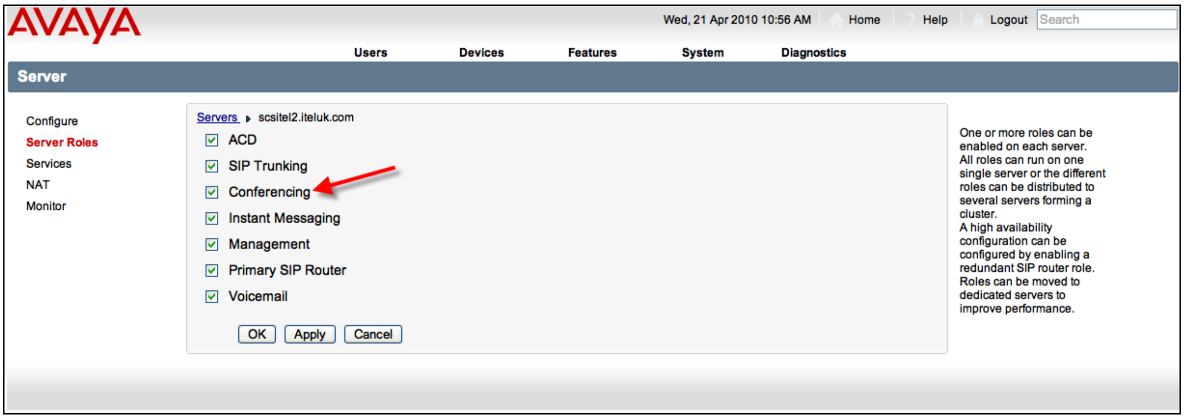
3. To view the **Server Roles**, click on the **Name** link of the Primary Server.



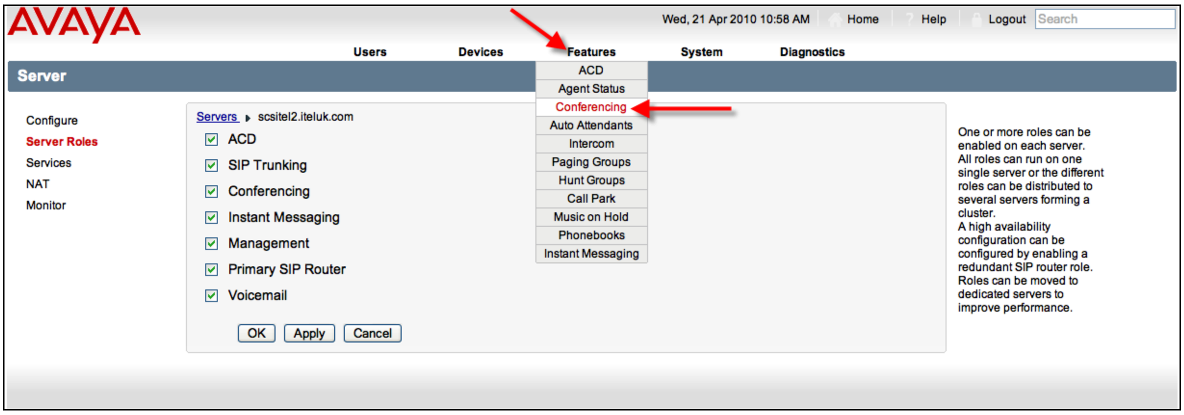
4. The server screen will be displayed. Click the **Server Roles** link.



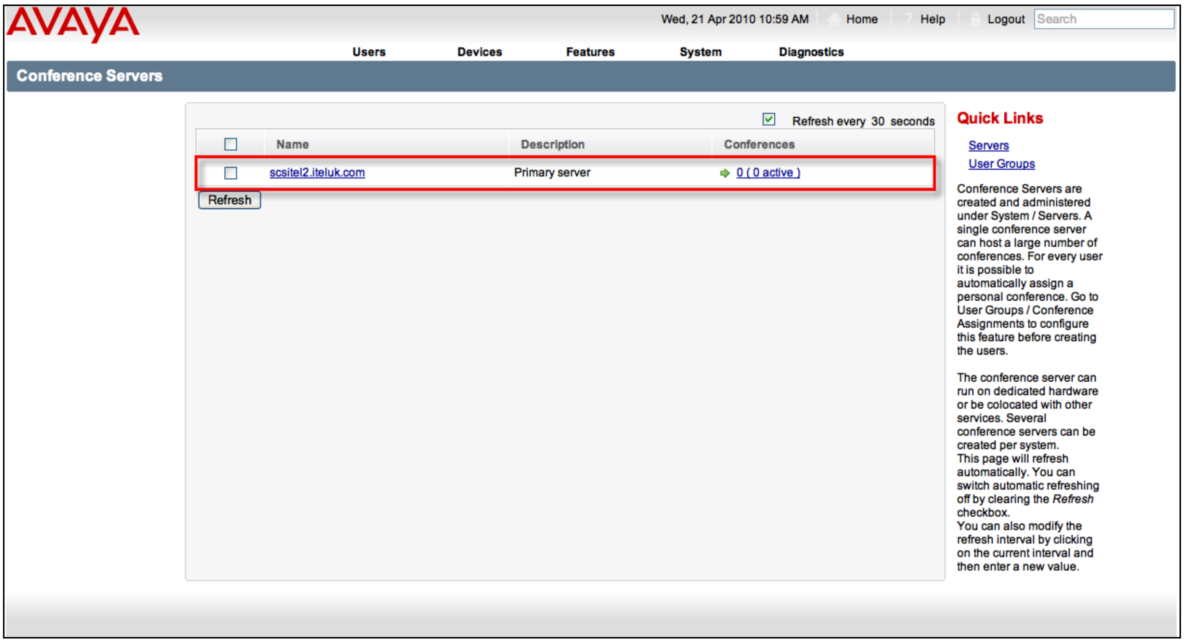
5. The Conferencing Server will be displayed in an enabled state. If it is not, select the roles check box and click the **Apply** button followed by the **OK** button.



6. Click the **Features** link, followed by **Conferencing**.



7. The **Conference Servers** screen will be displayed.



Problem: Cannot change conference settings

Solution:

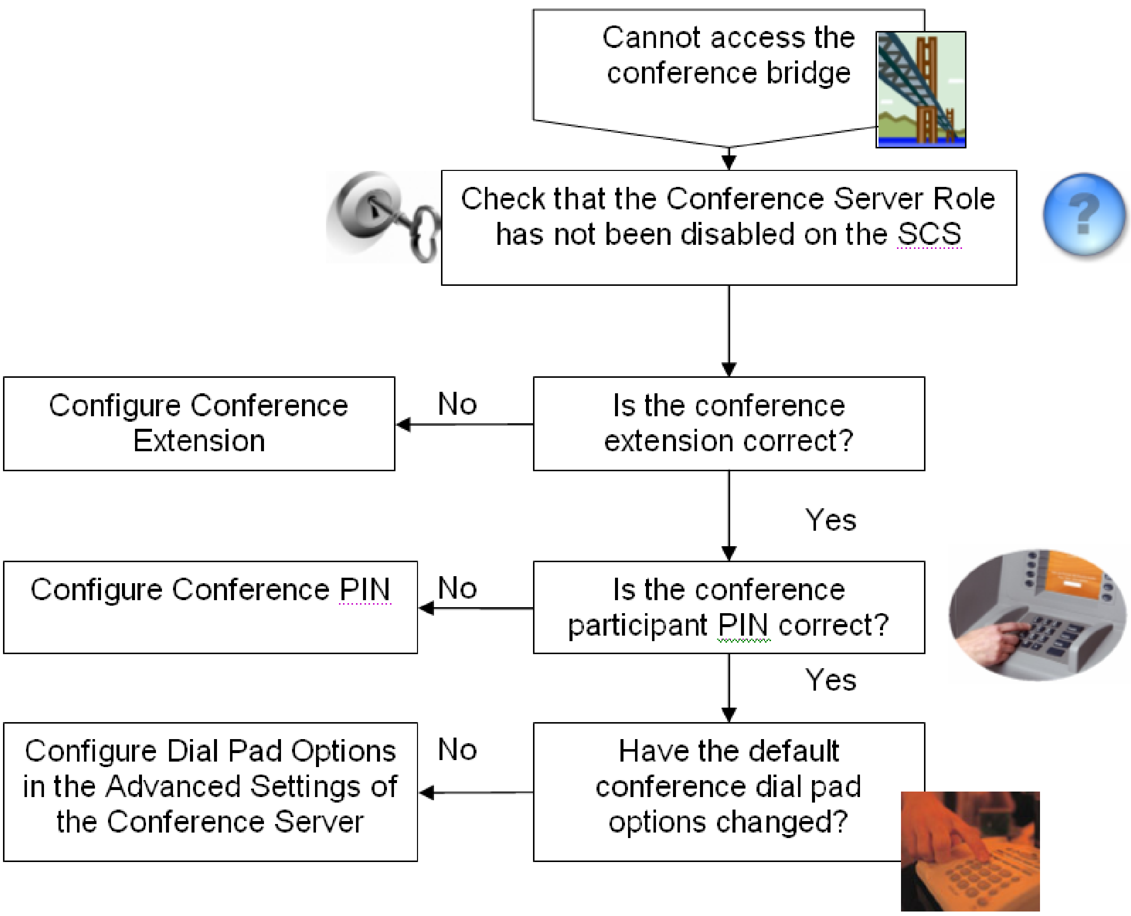
Check that the conference has been assigned an owner.

Problem: Cannot access the conference bridge

Solutions:

Check the following:

- Has the conference server role been disabled?
- Is the conference extension correct?
- Is the conference **participant PIN** correct?
- Have the default conference dial pad options changed?



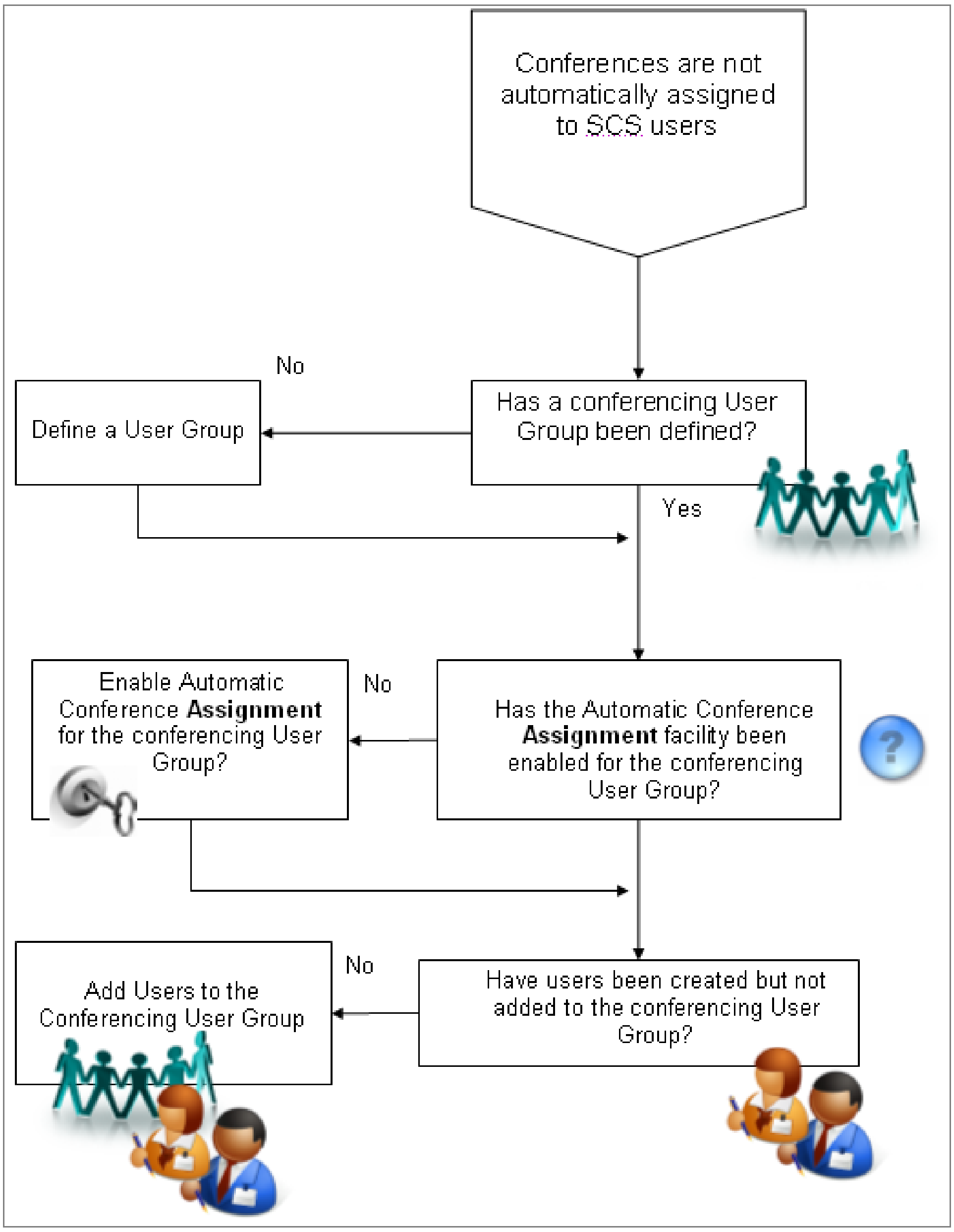
Problem: Conferences are not automatically assigned to SCS users

Solutions:

Check the following:

- Has a conferencing **User Group** been defined?
- Has the **Automatic Conference Assignment** facility been enabled for the conferencing User Group?
- Have users been created but not added to the conferencing User Group?

See the 'Conferencing' guide for in-depth guidance on configuring and using the conference server.



Problem: Users can’t dial Outlook contacts direct from soft phones

Solution:

Due to the length and make-up of contact numbers within the Outlook contact list, some issues may arise when you attempt to dial a number using the softphones’ ‘Click-to-Dial’ facility. You therefore need to find a way to format numbers before they leave the softphone and are passed to the SCS. For example:

- A customer has dial plans for local and long distance calls configured on the SCS.
- The local dial plan is configured to deal with numbers of seven digits with a prefix of 9. For example: 9 123-4567.
- The long distance plan is configured to deal with ten digit numbers with a prefix of 91. For example: 91-123-4567-899.
- The customer wishes to use Click to Dial to dial contacts directly from the Outlook contact list.
- Problem: contacts within the Outlook contact list have been stored as ten digit numbers, whether they are local or long distance.

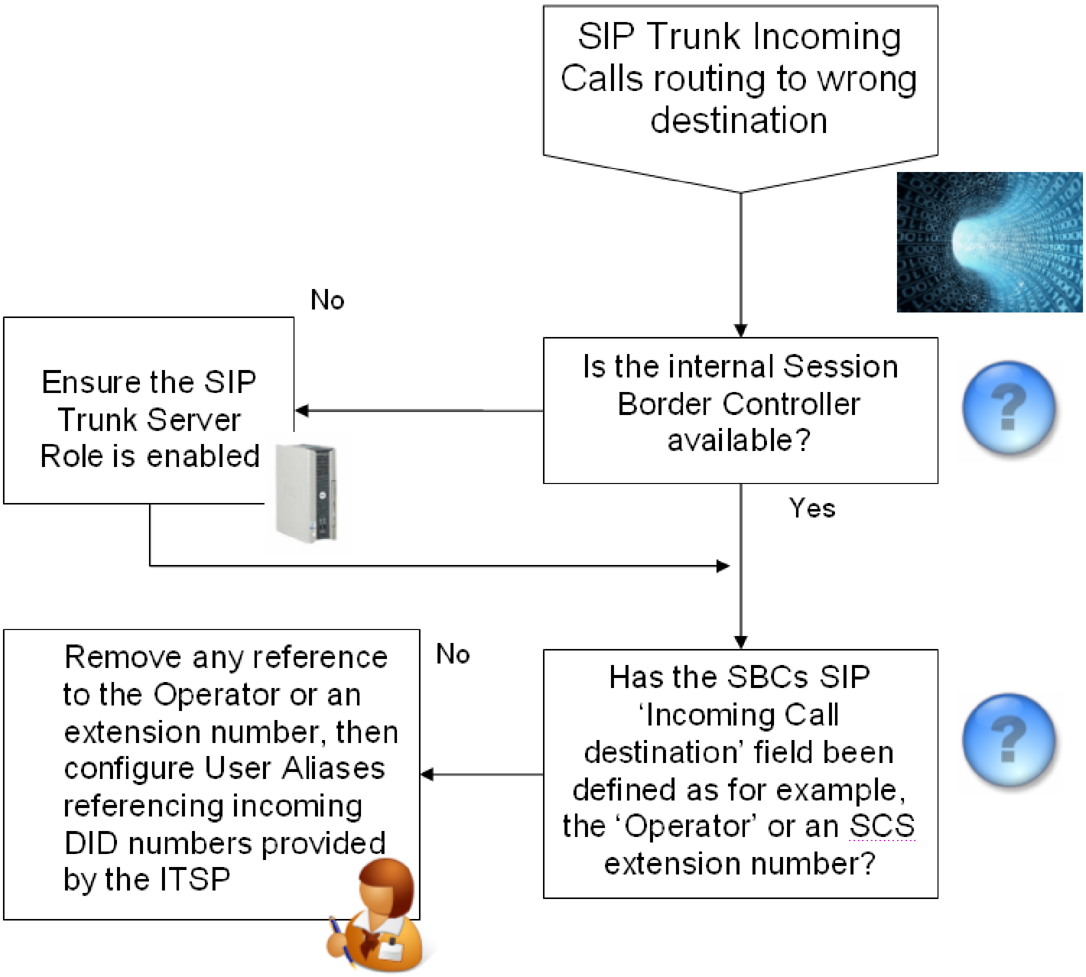
The solution to this problem is to configure a dial plan directly within the softphone to enable it to format all numbers dialled either directly from the contact list or via the dial pad so that the SCS can interpret them and then utilize its local and long distance dial plans accordingly. See the SCS 4.0 Configuring the Avaya 3456 UC Client Task Based Guide for instructions on how to configure such a plan.

Problem: SIP Trunk incoming calls routing to wrong destination

Solutions:

Check the following:

- Is the internal Session Border Controller available?
- Has the SIP Trunk server Role been added?
- Has the SBCs SIP Incoming Call destination been left as the default 'Operator'? If the operator is not required as the incoming SIP call destination, clear the field and add aliases referencing incoming SIP trunk numbers.
- Have user aliases been defined referencing incoming DID numbers provided by the ITSP?
- For conferences, have Dial Plan rules been created to direct calls to the conference extension. Alternatively, do conference extensions represent incoming DID numbers?



Problem: SIP Trunks General Call Failure

Solutions:

Check the following:

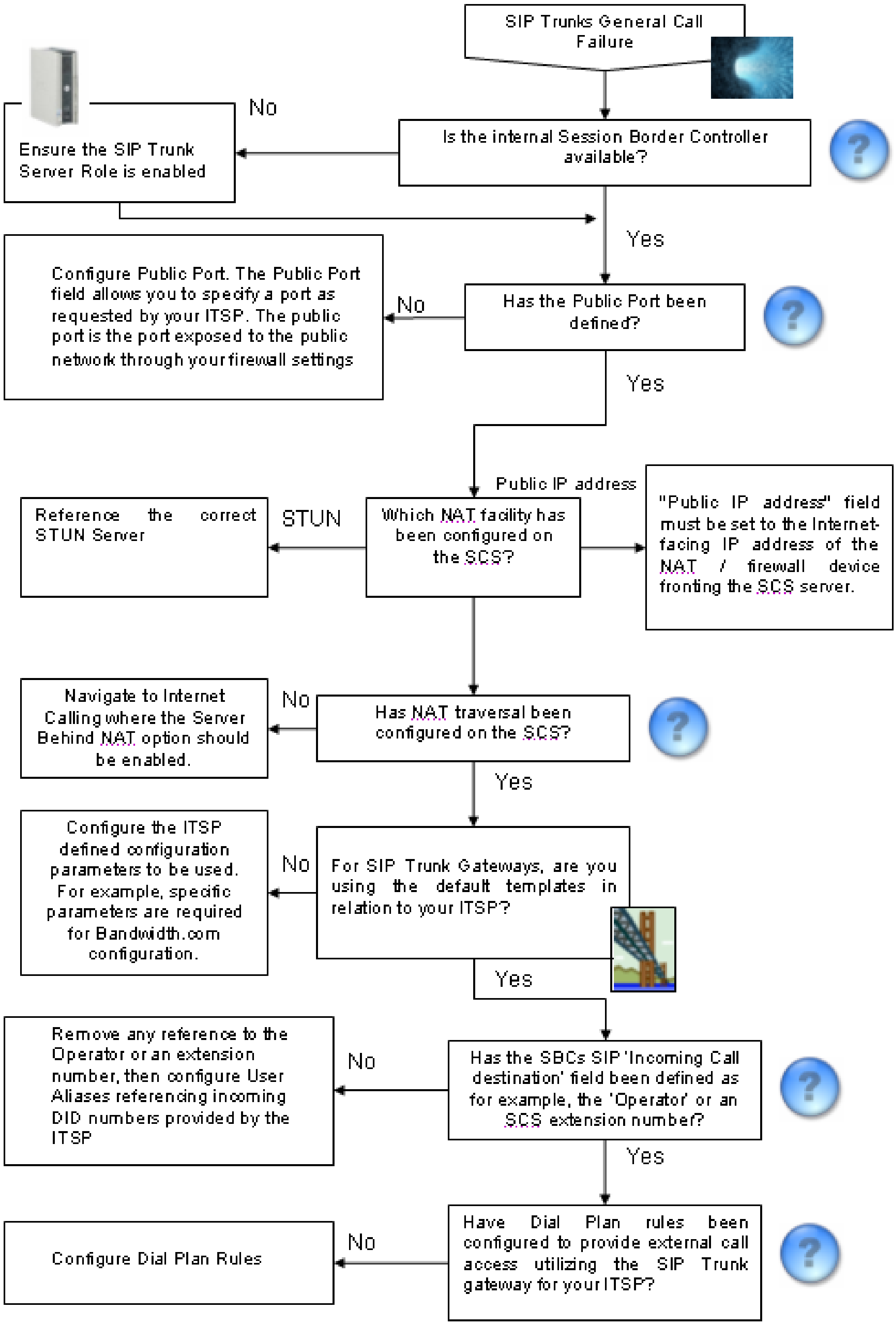
- Is the internal Session Border Controller available?
- Has the SIP Trunk server Role been disabled?
- Has the Public Port been defined?
- The Public Port field allows you to specify a port as requested by your ITSP. The public port is the port exposed to the public network through your firewall settings. If your firewall restricts inbound traffic, you must open this port on the firewall to allow inbound signaling from the ITSP. The SCS ‘external port’ is the port that ‘faces’ the firewall and is associated with the firewall’s public port. Therefore, the firewall must be configured to send packets from the firewalls public port to the SCS external port. If you leave the public port field blank, the external port is assumed to be the same as the public port and the mapping assumed to be symmetric. Please confer with your ITSP for details regarding NAT and any specific firewall rules the ITSP may require.
- Has NAT been configured on the SCS?
    - Is STUN utilised and if so, is the correct STUN Server referenced?
    - Will a Public IP address be referenced for NAT. When the server is deployed behind a NAT, the "Public IP address" field must be set to the Internet-facing IP address of the NAT / firewall device fronting the SCS server.
- Has NAT traversal been configured on the SCS, this is found under Internet Calling where the Server Behind NAT option should be enabled.
- With regards to SIP Trunk Gateways, are you using the default templates in relation to your ITSP?
- Has the ITSP defined specific configuration parameters for you to use? For example, specific parameters are required for AT&T ITSP configuration.
- Has the SBCs SIP Incoming Call destination been left as the default ‘Operator’

- Have user aliases been defined referencing incoming DID numbers provided by the ITSP?

- For conferences, have Dial Plan rules been created to direct calls to the conference extension. Alternatively, do conference extensions represent incoming DID numbers?

- Have Dial Plan rules been configured to provide external call access utilizing the SIP Trunk gateway for your ITSP?

See the SCS 4.0 Device Configuration Gateways Guide for full configuration details include required firewall / NAT parameters.


SIP Trunks General Call Failure
Is the internal Session Border Controller available?
No
Ensure the SIP Trunk Server Role is enabled
Yes
Has the Public Port been defined?
No
Configure Public Port. The Public Port field allows you to specify a port as requested by your ITSP. The public port is the port exposed to the public network through your firewall settings
Yes
Which NAT facility has been configured on the SCS?
STUN
Reference the correct STUN Server
Public IP address
"Public IP address" field must be set to the Internet-facing IP address of the NAT / firewall device fronting the SCS server.
Has NAT traversal been configured on the SCS?
No
Navigate to Internet Calling where the Server Behind NAT option should be enabled.
Yes
For SIP Trunk Gateways, are you using the default templates in relation to your ITSP?
No
Configure the ITSP defined configuration parameters to be used. For example, specific parameters are required for Bandwidth.com configuration.
Yes
Has the SBCs SIP 'Incoming Call destination' field been defined as for example, the 'Operator' or an SCS extension number?
No
Remove any reference to the Operator or an extension number, then configure User Aliases referencing incoming DID numbers provided by the ITSP
Yes
Have Dial Plan rules been configured to provide external call access utilizing the SIP Trunk gateway for your ITSP?
No
Configure Dial Plan Rules

Problem: Mediant FXO Gateway – Inbound Calls do not terminate on SCS

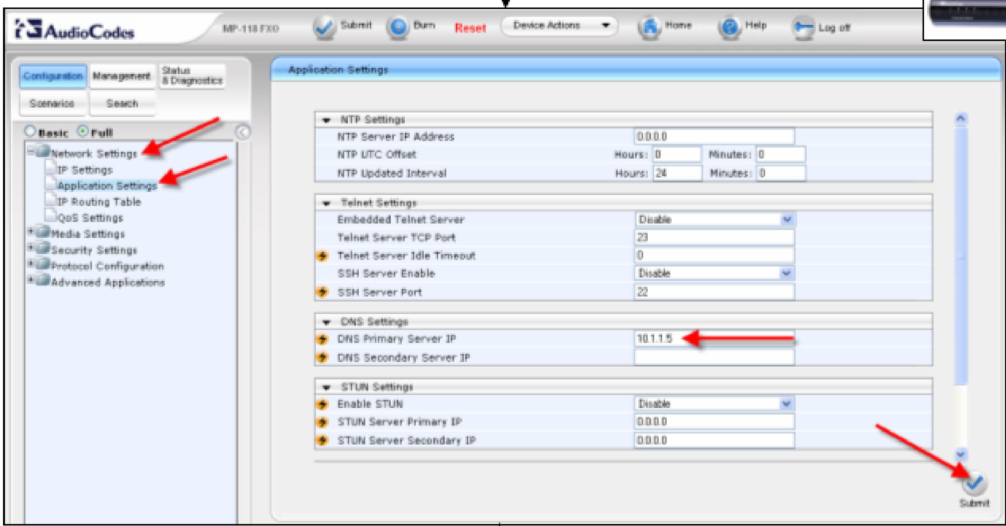
After the Gateway configuration is completed on the SCS, the ini file is uploaded to the gateway and the gateway restarted. However if you find that the data from the ini file has not propagated all of the gateway fields:

Solutions:

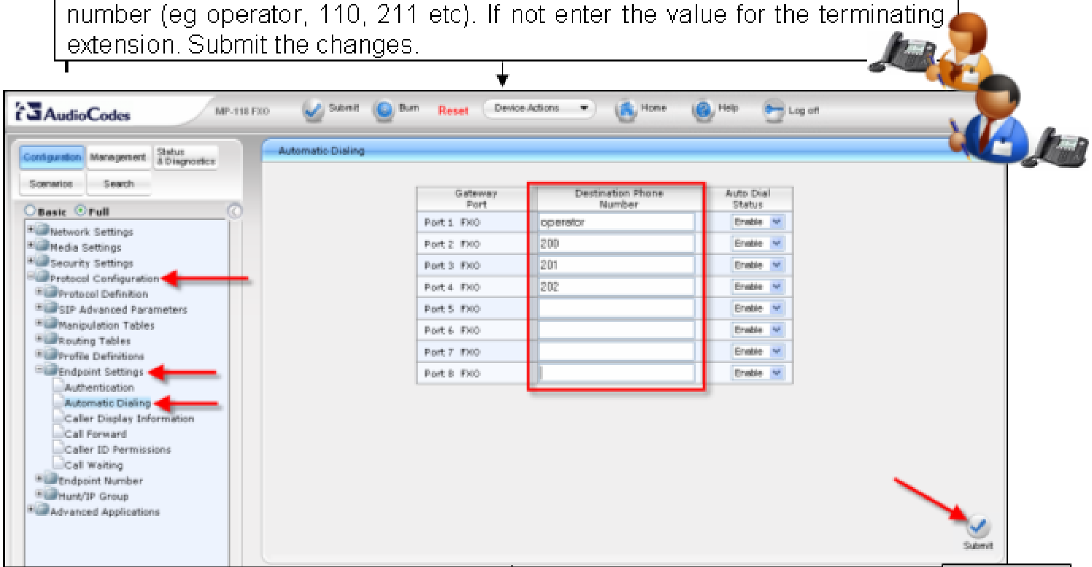
Check the following:

- Has the Primary DNS server been defined on the gateway?
- Does each port on the gateway have a corresponding value for the terminating extension number?

Login to the FXO gateway, click on **Advanced Configuration**, **Network Settings**, and **Application Settings** menu. Make sure the value for Primary DNS is present. If not enter the value for primary DNS. Submit the changes.

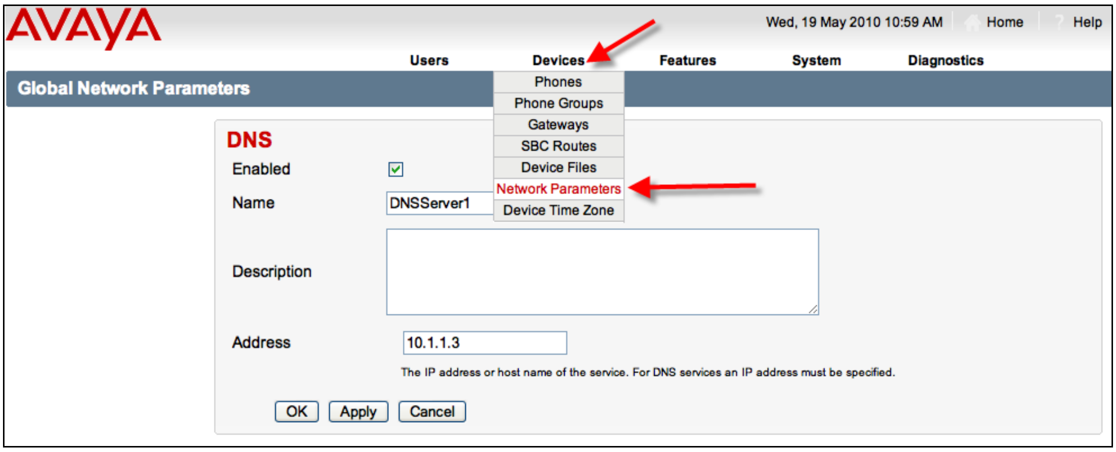


Select **Protocol Configuration**, **Endpoint Settings** and **Automatic Dialing**. Make sure each port has a corresponding value for the terminating extension number (eg operator, 110, 211 etc). If not enter the value for the terminating extension. Submit the changes.



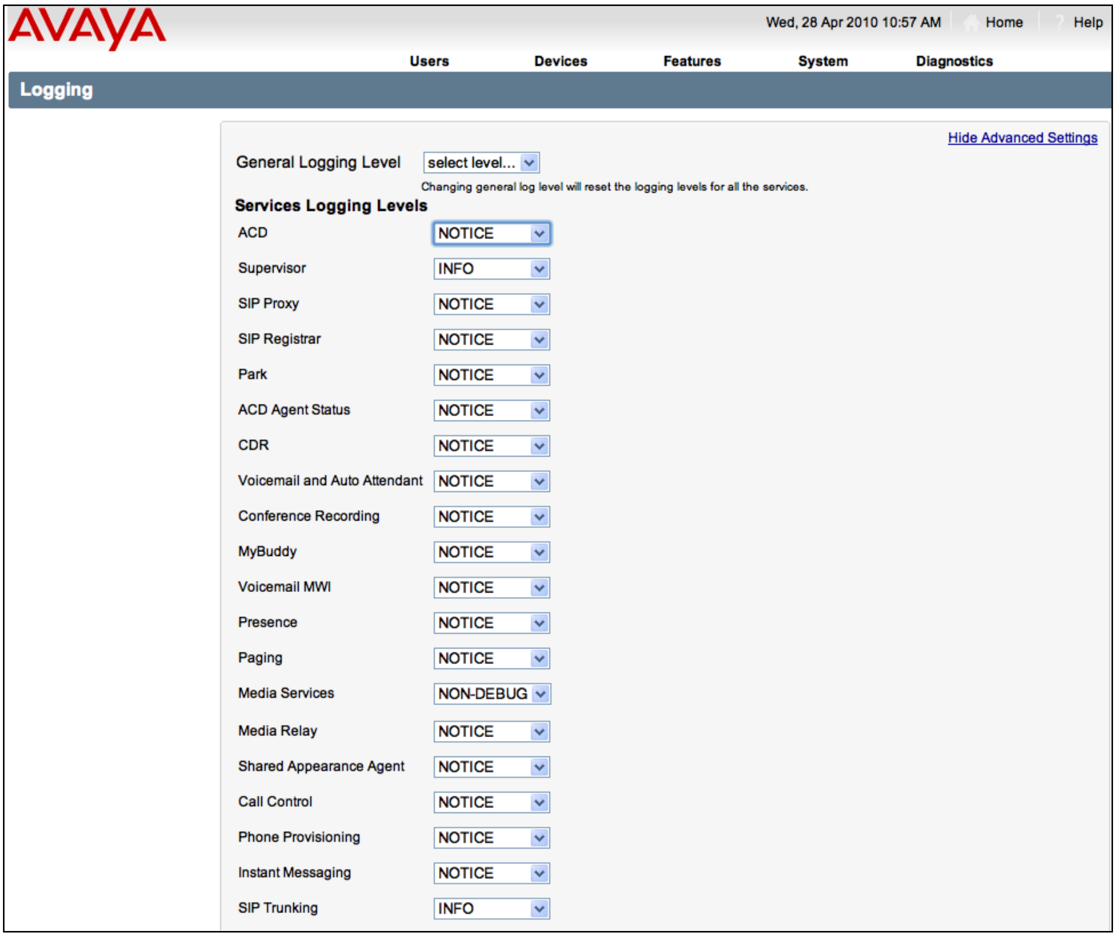
Burn to **Flash Memory** any configuration changes made to the gateway.

The Primary & Secondary DNS server settings configured on the SCS under Devices > Network Parameters are propagated to all gateway devices and ini files for those devices. Consequently, these DNS settings will be those used by the gateway device. For Static IP Address configuration of an gateway device, DNS settings must be defined, otherwise calls to and from the device will fail. Please refer to the *Propagating DNS Settings to Gateway Devices* section of this guide.



Logging Levels

The SCS logging level parameters determines the amount of information stored in a system snapshot. Most of the time the system should run at *NOTICE* level. During troubleshooting increase the logging level temporarily before taking system snapshots. Reset logging level back to *NOTICE* once the problem is resolved. The most detailed logging level is *DEBUG*, the least detailed -*EMERG*.



As a general guideline:

You should not have to use the DEBUG logging level unless advised to do so by technical support. It is generally never required in a production installation. The INFO logging level is more than adequate and will produce dramatically less log data.

Whenever possible, set the proxy logging to INFO as the majority of messages pass through the proxy. Therefore, it is invaluable as a data collection point. As long as a system has a reasonable size disk, leaving the proxy at INFO level will only have a negligible impact on system performance.

Collect snapshot data while the problem is occurring, not after you've found a solution to the problem.

Limit the log data to a reasonable period of time when the problem is occurring; if possible, it's best to capture a window from before the problem started to after it is known to have occurred, but support rarely need more than a few minutes of data either side of the event if it can be narrowed down that much.

Avaya 3456 UC Client

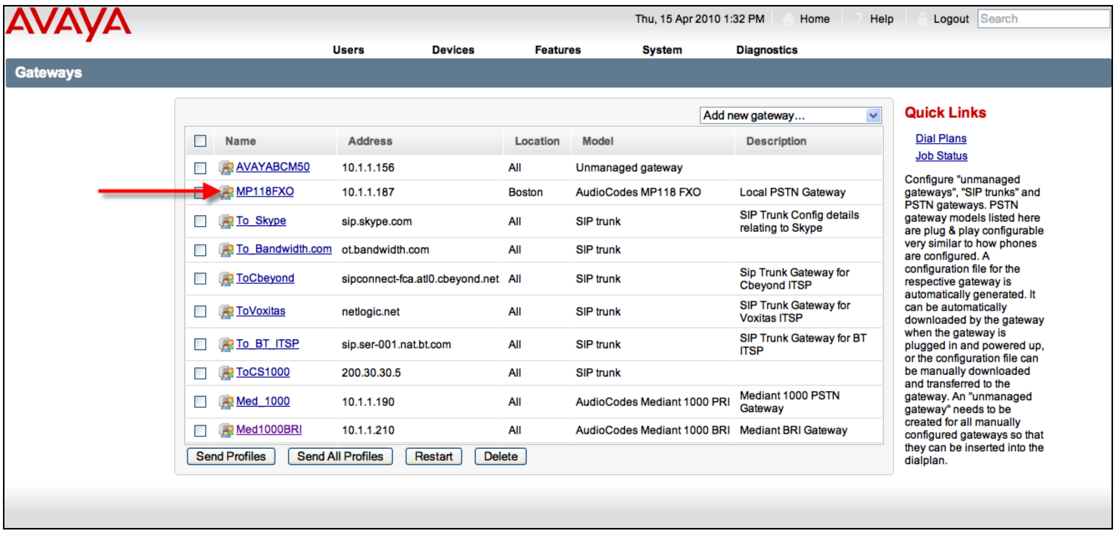
The Avaya 3456 will not upload contacts from SCS phonebook if Internet Explorers proxy is in use. Internet Explorer's Proxy settings must be disabled or exceptions for the SCS address must be put in place in order for the 3456 to gain access to the Phonebook. This is because non-Microsoft products take their connection settings from IE.

SAS Stand Alone Survivability

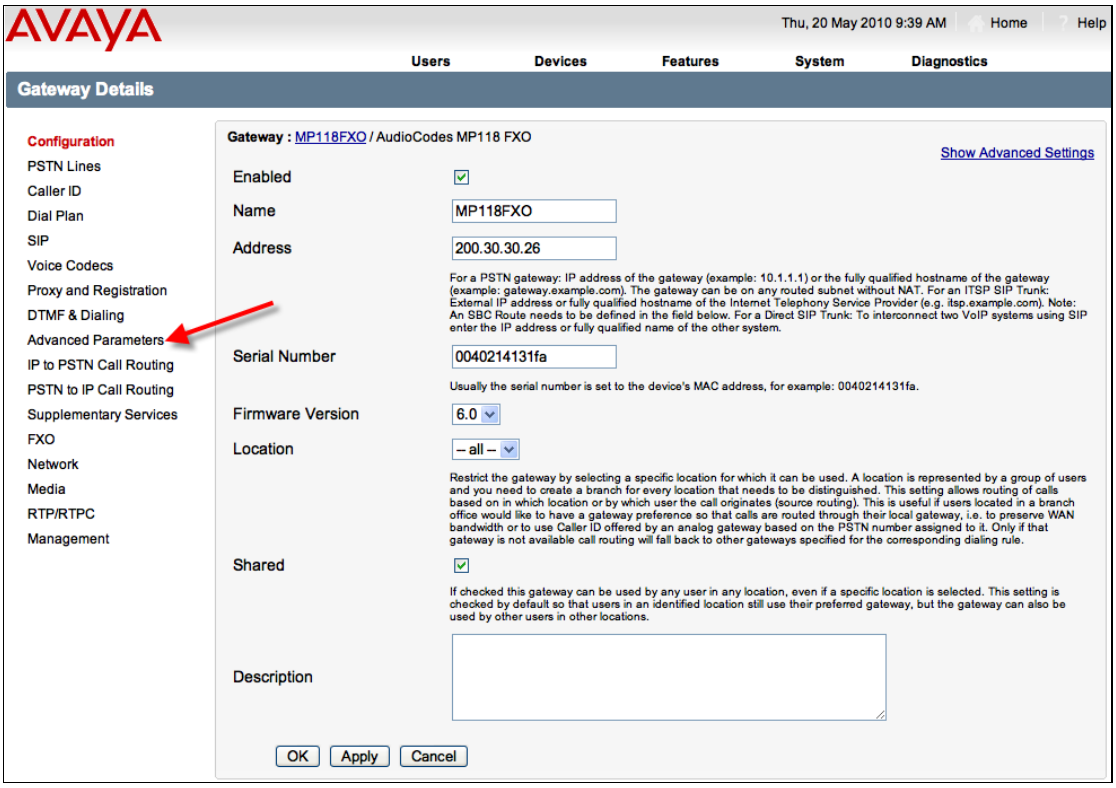
Problem: When configuring SAS with AudioCodes gateway firmware prior to version 5.6, if the SCS fails external calls may also fail. The FXO gateway attempts to route to the SCS instead of making an external call.

1. Login to the SCS. From SCS Home Page select **Devices** followed by **Gateways**.

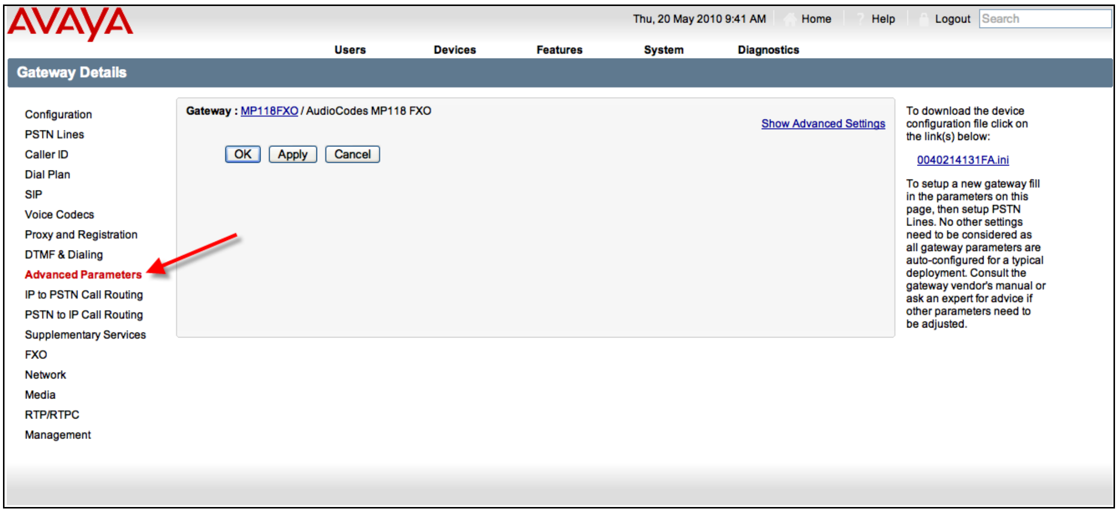
2. Select the Gateway to be configured with the SAS feature.



3. The gateway's configuration details will be displayed. Click the **Advanced Parameters** link.

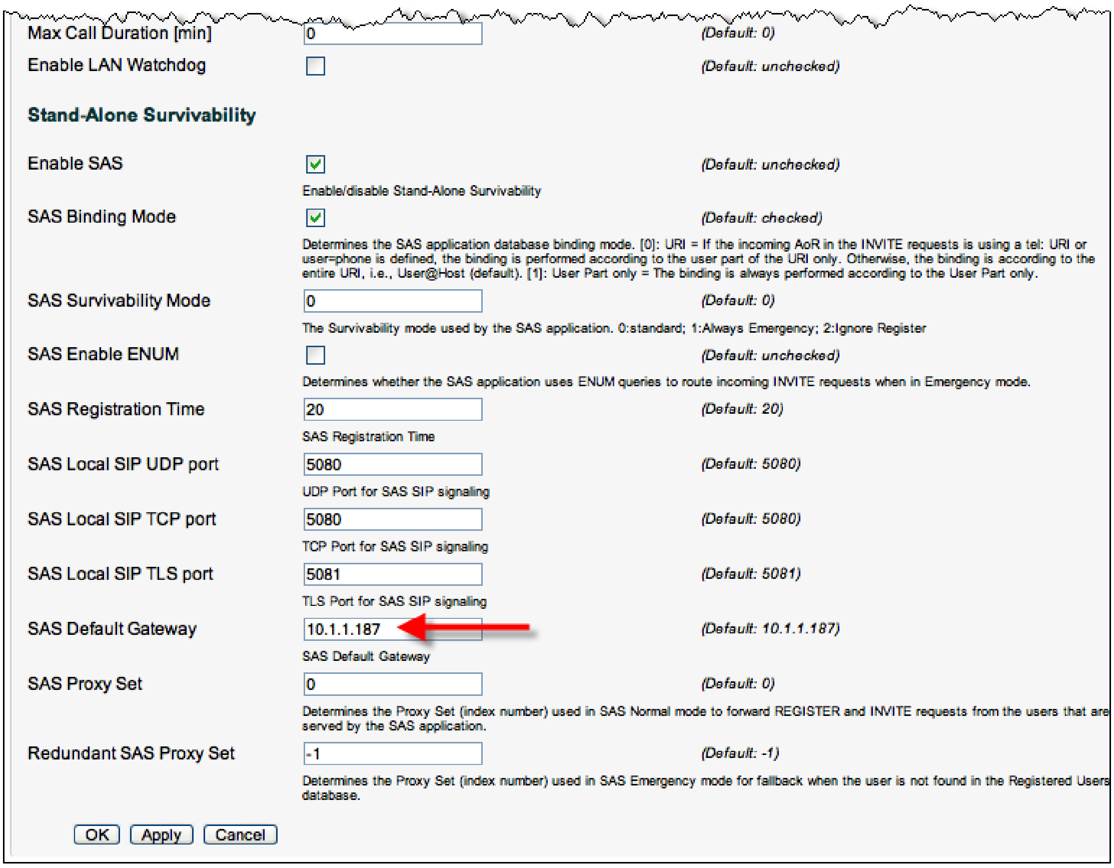


4. If the Advance Parameters are not displayed, click the **Show Advanced Parameters** link.

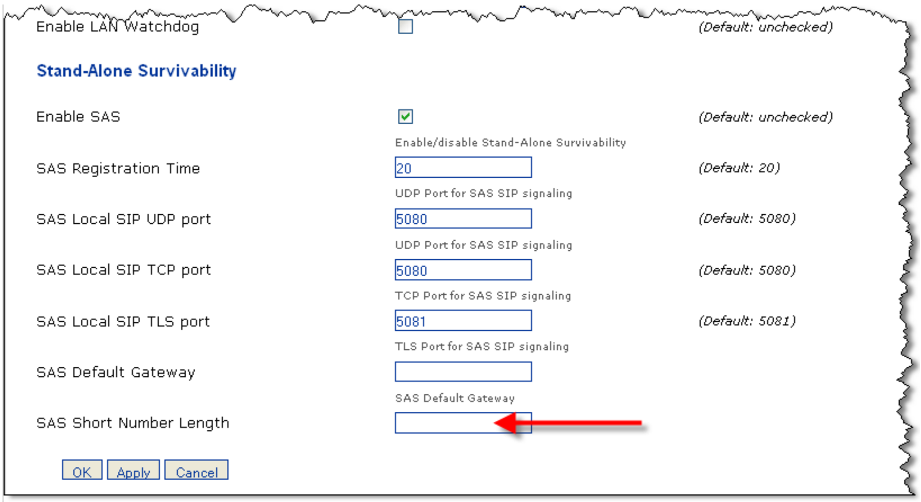


5. The SAS configuration parameters are located at the bottom of the **Advanced Parameters** page.

6. In the SAS Default Gateway field, enter the IP address of the device that has access to the PSTN. In this example, the device is an AudioCodes FXO Gateway.



Note: For firmware versions pervious to version 5.6, the SAS Short Number Length field will be displayed. The **SAS Short Number Length** determines the length of the suffix used for Stand-Alone Survivability (SAS) Short Numbering support. The dialed number is compared to the registered number. This will be the number of digits to be passed to the gateway. For example, if an IP phones registers with 9 01244 670200 the parameter would be set to 11 (digits). The valid range is 0 to 63 characters.



Please refer to the SCS 4.0 Device Configuration gateways TBG for details relating to SCS SAS Configuration with gateway firmware version 6.0.

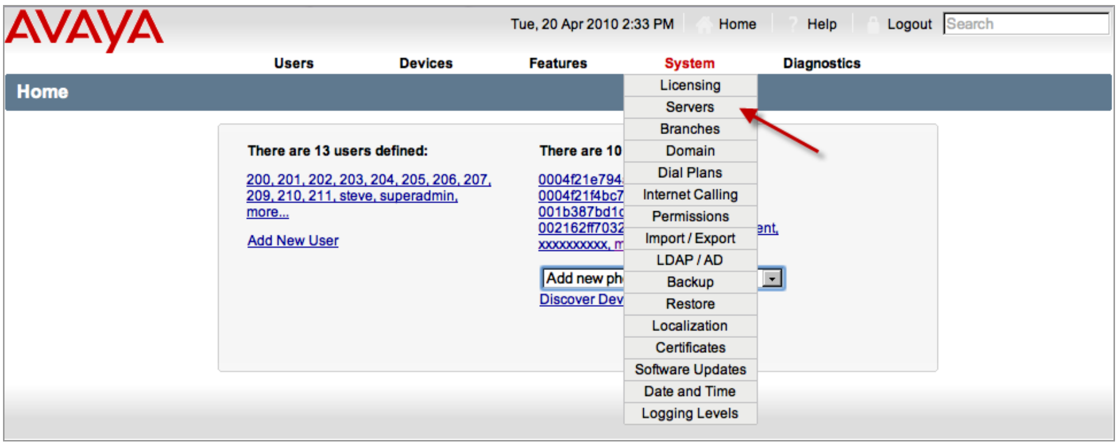
Instant Messaging

Problem: Users cannot log in to Instant Messaging clients.

Solution

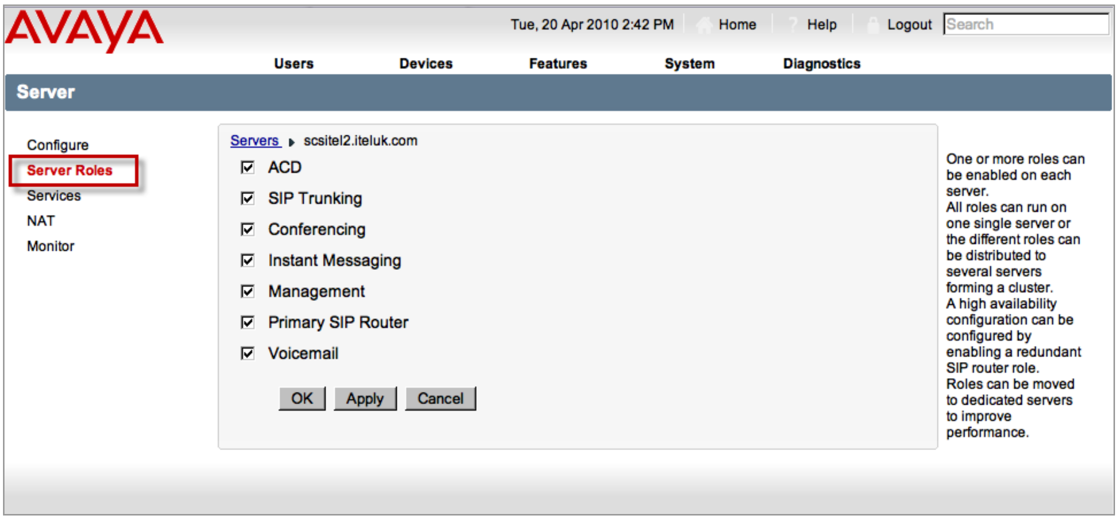
First ensure that the Instant Messaging server is running:

1. From within the SCS administrator interface, open the **System** menu and select **Servers**.

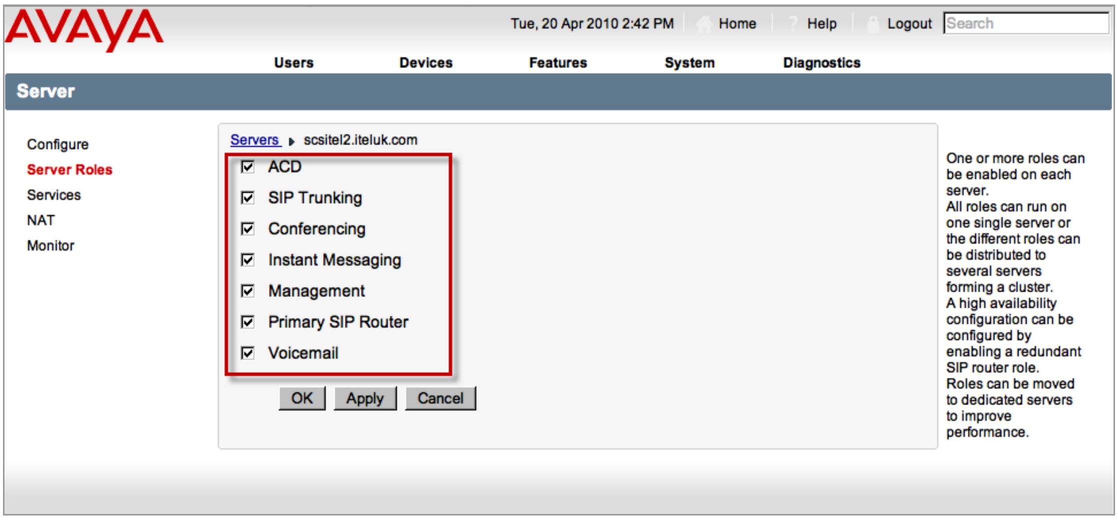


2. Select the server on which the IM service is situated. On some networks, some services will be distributed across several different servers. In this example all SCS service run from the same server.

3. Click on the **Server Roles** menu, located on the left-hand side of the screen.



4. A list showing all available roles is displayed. Roles that are ticked are enabled. Ensure that the **Instant Messaging** role is ticked. By default all roles should be enabled by default.



5. Click **Apply** followed by **OK** to confirm any changes made.

Note: If you do make a change to this screen you will be asked to restart services. Click on the purple link that appears at the top of the screen to got to the service restart page. Tick the check-boxes of any services listed and then click the **Restart** button.

6. You will be returned to the server selection page.

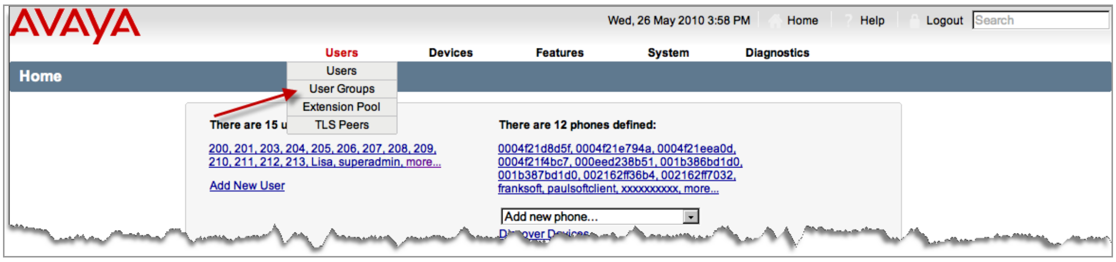
Once you have ensured that the Instant Message role is enabled, ensure that users are entering the correct IM password. If IM passwords have not been configured then they will be the same as the users' IM IDs.

Problem: MyBuddy not present in users' IM clients

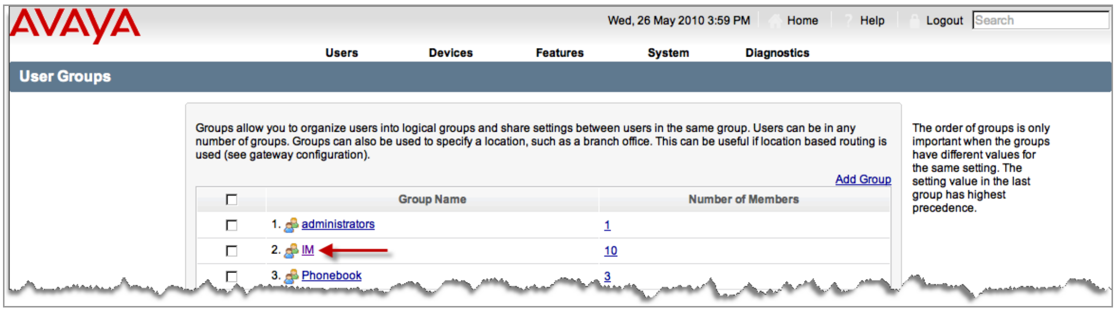
Solution:

If Instant Messaging group are members of a group:

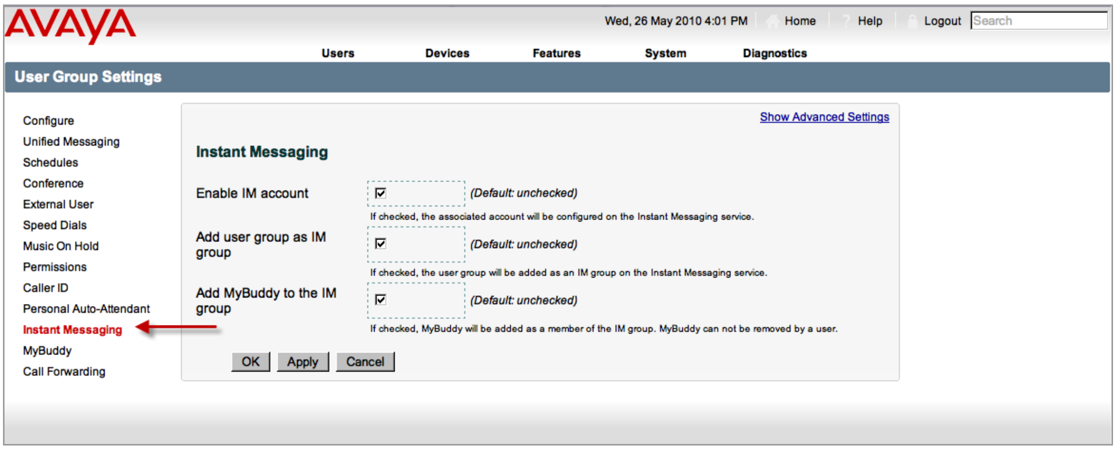
1. Open the **Users** menu and select **User Groups**.



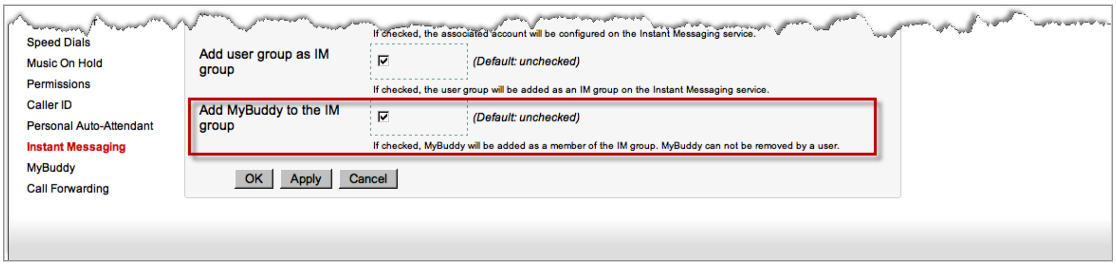
2. Click on the Instant Messaging group.



3. Click on the **Instant Messaging** menu.



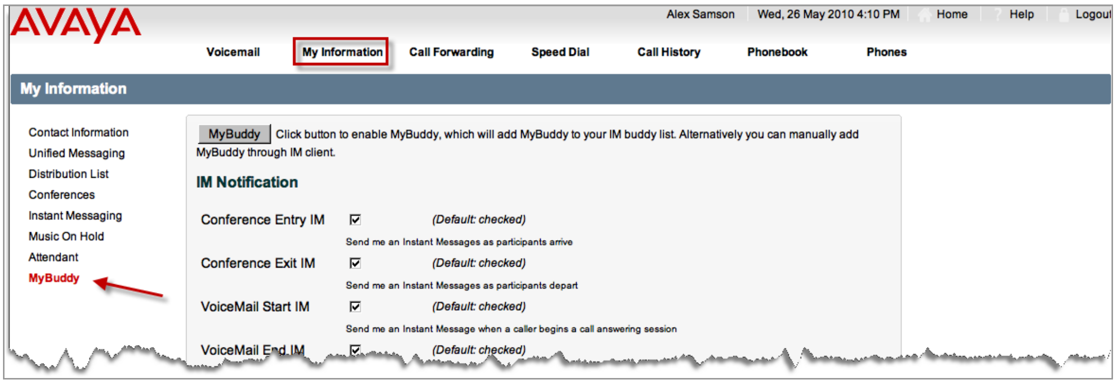
4. Ensure that the **add MyBuddy to the IM group** option is enabled by ticking the check-box.



5. Click **Apply** followed by **OK**.

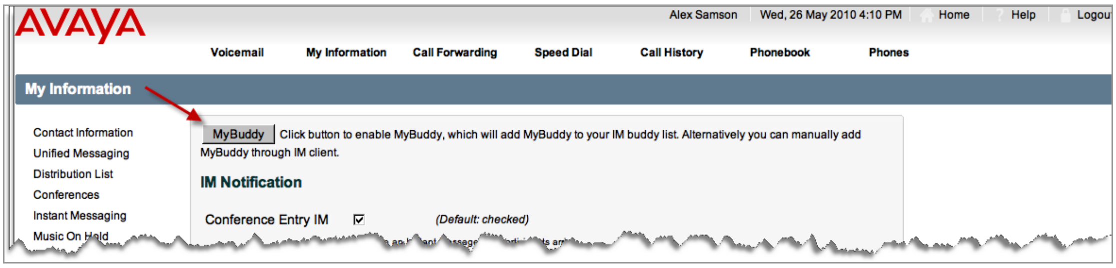
If IM users are not grouped on your network each user will have to enable MyBuddy from within their own SCS user portal:

1. Log in to the user interface and click on **My Information**.



2. Click on **MyBuddy**.

3. Click the **MyBuddy** button at the top of the screen to enable MyBuddy.



4. Click **Apply**.

Problem: MyBuddy and/or other SCS IM Buddies do not appear in Gtalk.

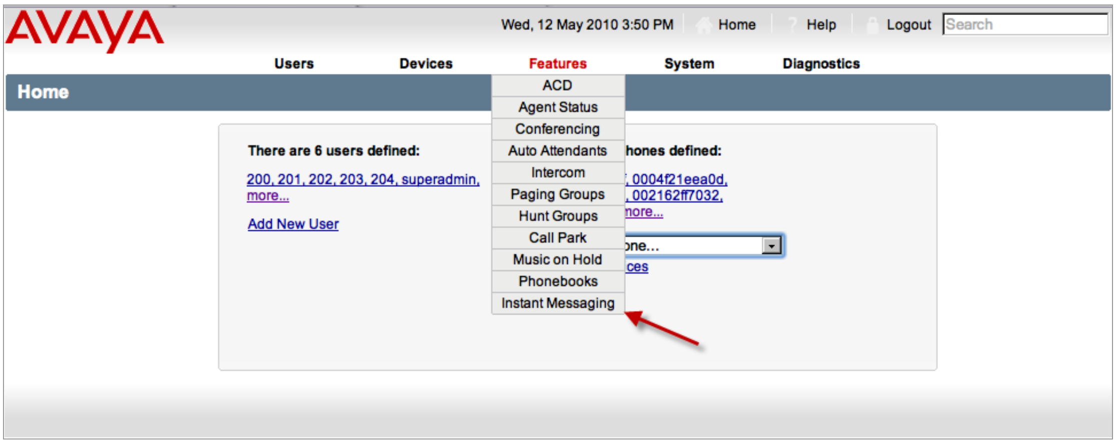
Solution:

There are two solutions that you might try for this issue, the first of which is server related, the second relates to user account settings.

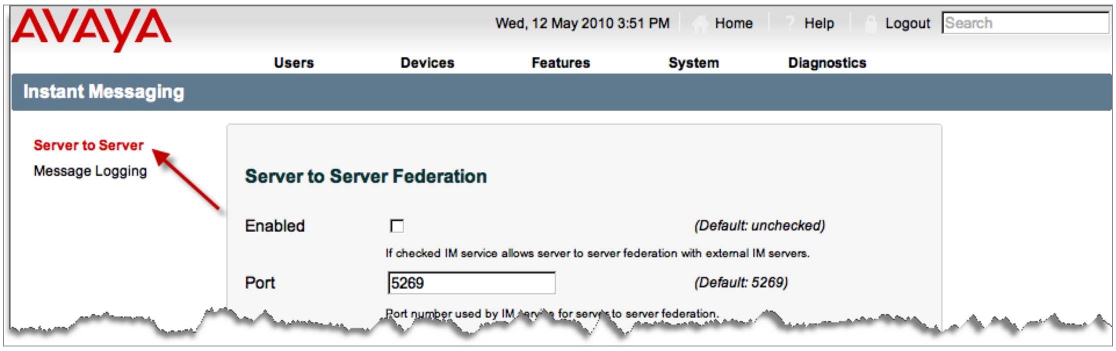
First, check that IM federation is enabled:

To configure Federation:

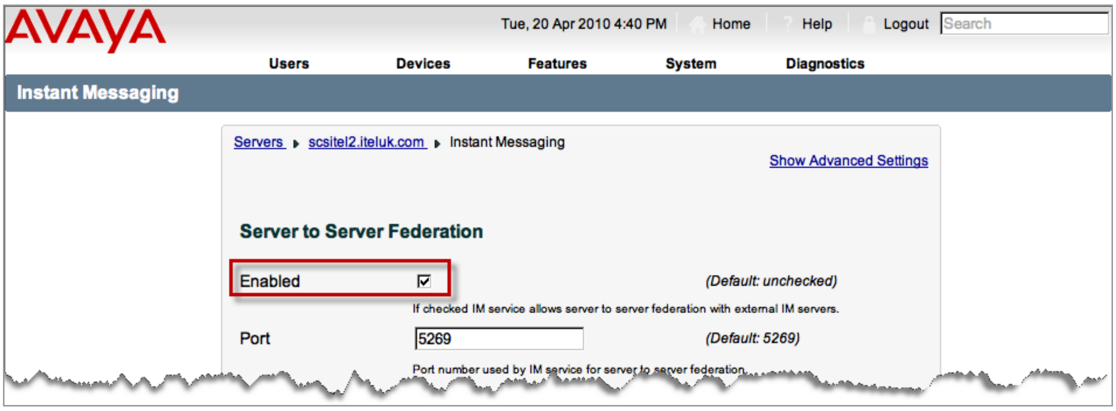
1. Open the **Features** menu and select **Instant Messaging**.



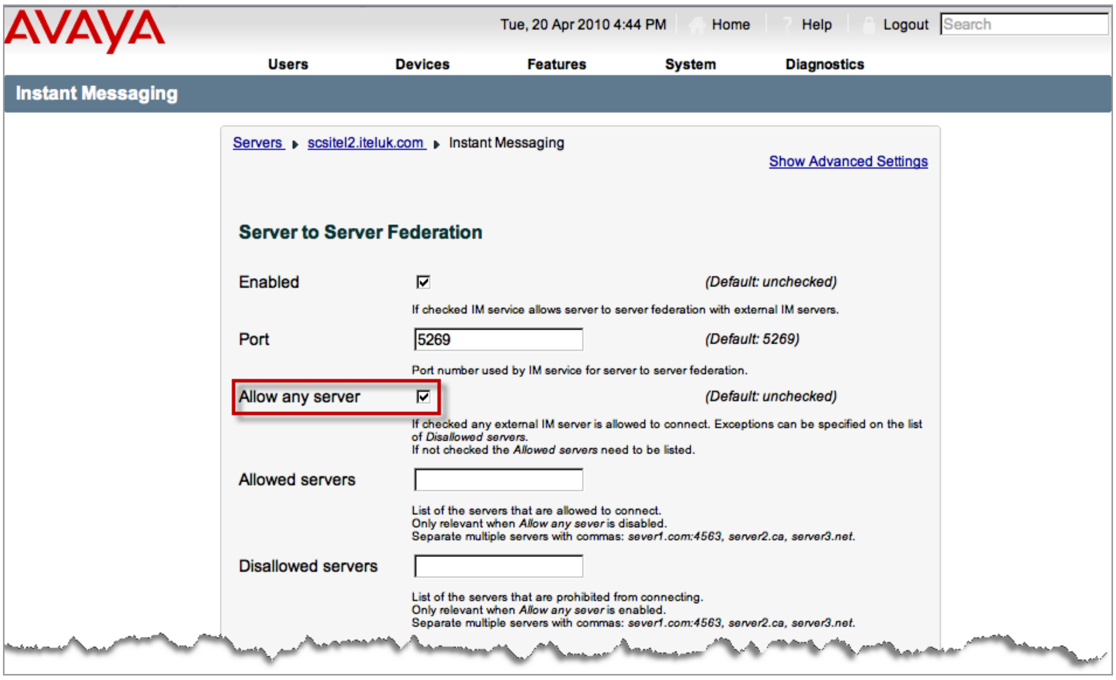
2. Click on **Server to Server**..



3. Enable federation by ticking the **Enable** check-box.



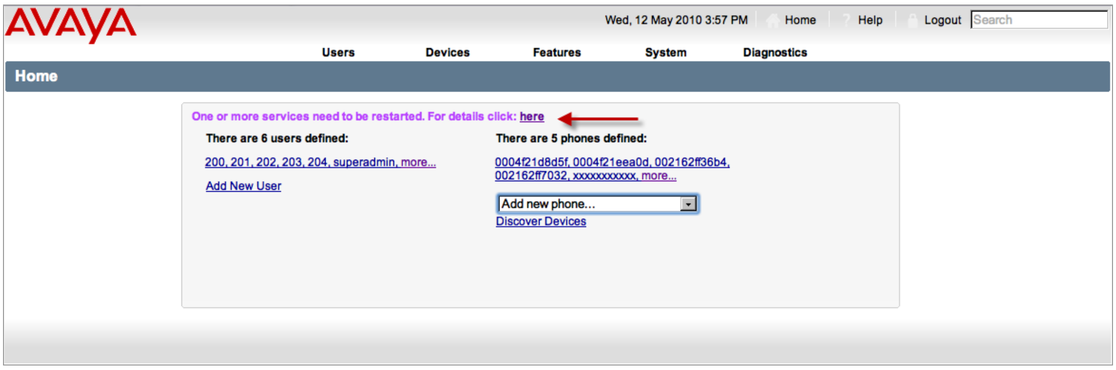
4. Next, decide which IM servers will be allowed communication with the SCS. If all servers are acceptable simply tick the **Allow any server** check-box.



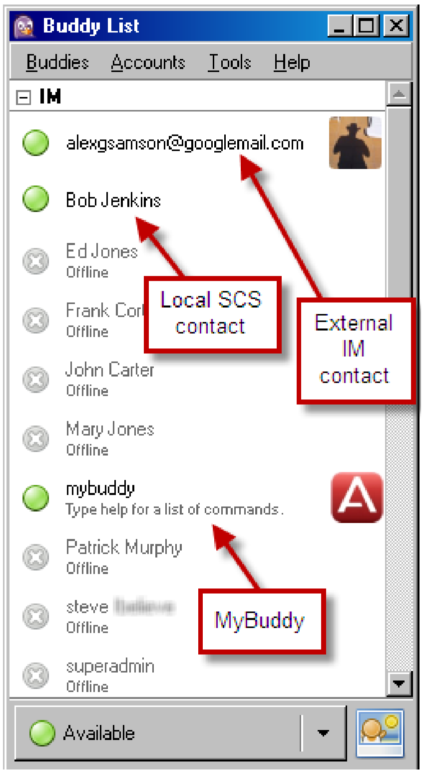
Use the **Disallowed servers** field to define any servers that are exceptions to the 'Allow any server' clause. This is a useful feature if, broadly speaking, all servers are allowed but there are a few that you would like to block. For example, you may wish to allow all IM servers except Google Talk, in which case you would enter *gtalk.com* in the Disallowed servers field.

5. Click **Apply** followed by **Home** to continue.

6. Restart any necessary services by following the pink **here** link.



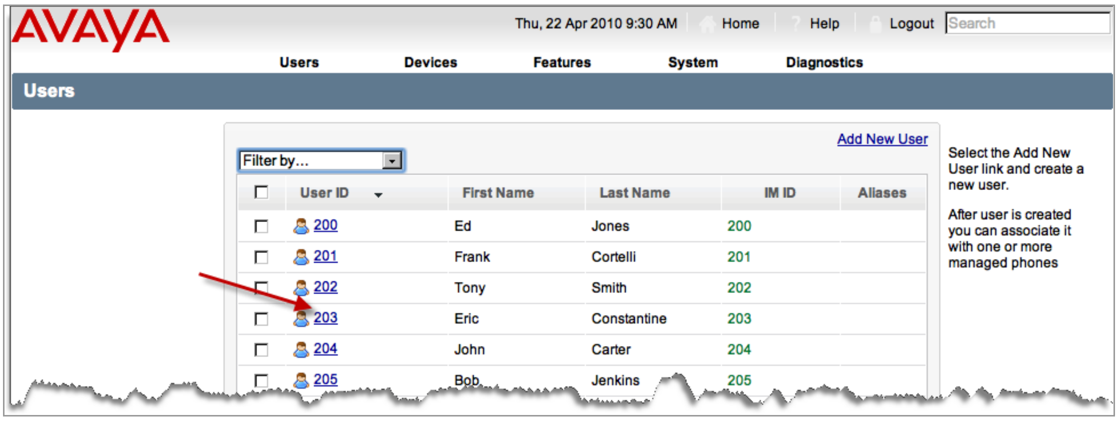
The SCS IM service can now be used to message contacts on other messaging services outside of its own domain.



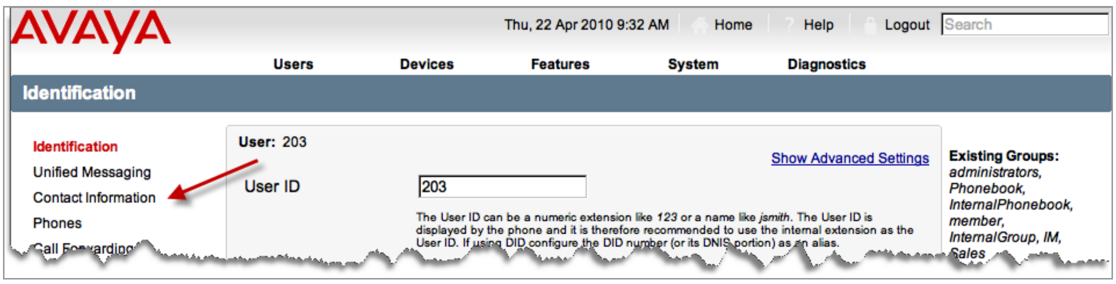
If the problem persists once you have checked IM Federation settings, check whether an alternate IM account has been defined within the user's SCS profile:

1. Navigate to the user account in question by opening the **Users** menu and selecting **Users.**

2. Select a user.



3. Click on **Contact Information**, located on the left-hand side of the screen.



4. Toward the bottom of the contact information form you will find a field called **Alternative IM account**. Enter the user name and domain of the user's secondary IM account in this field – for example *ericcon@googlemail.com*.

5. Click **Apply** followed by **OK**.

The user can add MyBuddy or any other SCS-based IM contact to their external IM account. When adding an SCS contact to a non-SCS IM client, you must specify the full IM ID, including the domain name, for example: *mybuddy@scshost.scsdomain.com*.

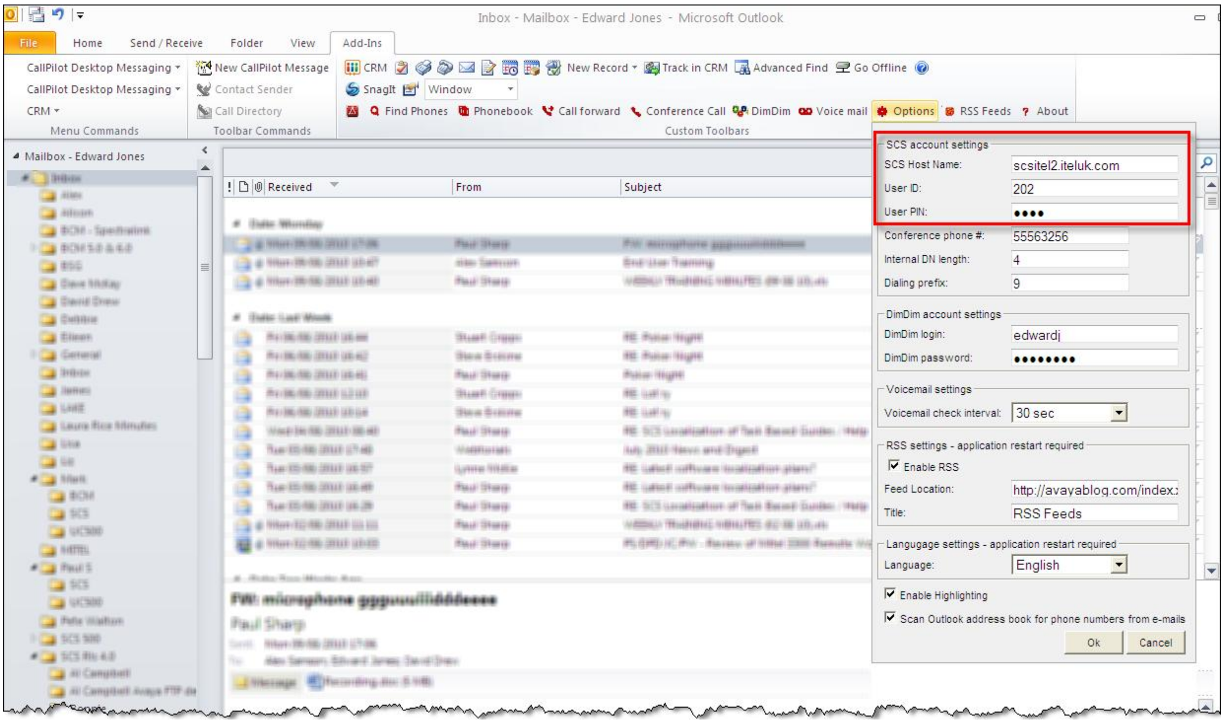
Note: Clicking the **MyBuddy** button found in the user portal on the 'MyBuddy' page will not activate MyBuddy in an external IM account. MyBuddy must be added manually like any other contact using the client's 'add contact/buddy' process.

SCS Toolbar

Problem: Once installed, the toolbar does not register and function with the SCS.

Solution:

Ensure the SCS Host name has been entered correctly under the Toolbar's **Options** menu. The SCS user's login credentials should also be added.



Problem: The Toolbar does not recognize UK numbers when numbers are dialed using the Toolbar application.

Solution:

With this release, the toolbar only recognises the North American telephone number format.

Below is a list of recognizable phone number formats of USA and Canada:
+1szzzsxxxsxxsxx
+1s(zzz)sxxxsxxsxx
(+1szzz)sxxxsxxsxx
1szzzsxxxsxxsxx
1s(zzz)sxxxsxxsxx
(1szzz)sxxxsxxsxx
zzzsxxxsxxsxx
(zzz)sxxxsxxsxx

x - digit or character in upper case
zzz - area code
s - separator symbol: " " (spacer character), "-" , "." , "" (no characters)

Avaya Support – Pre Contact Checklist

Before contacting SCS Avaya support, you may wish to consider and gather certain information which may assist the support team and lead to a quicker solution to the problem.

If possible, before contacting support:

- Provide a full description of the issue including appropriate screenshots of the SCS interface.
- A list of solutions/actions you have taken to attempt to resolve the issue.
- Note the release number of the SCS software installed.
- Confirm whether the SCS is in a High Availability or standalone environment.
- Confirm whether DNS A-Record/SRV records have been configured and utilised for the SCS installation.
- Confirm whether DHCP option 120 / option 66 in use in the SCS network.
- Create a diagnostics Snapshot relating to the configuration / problem issue.
- If appropriate, provide details relating to any gateways utilised, including firmware levels relating to PSTN gateways. For example, AudioCodes gateways.
- If appropriate, provide details relating to any SIP Trunk gateways utilised.
- If appropriate, provide details relating to the IP Phone models used in the SCS environment.

SCS Community Portal

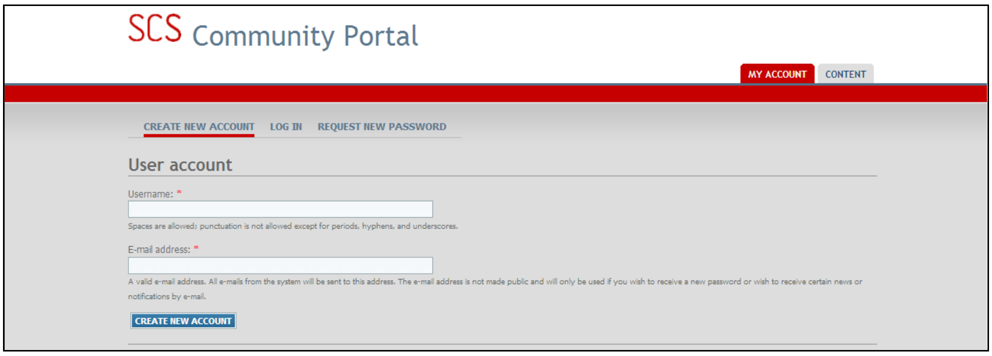
The SCS Community Portal has a large amount of information including demonstrations and documentation relating to SCS 4.0. SCS administrators can register with a community account, and gain access to documentation, training and SCS related software.

Information on many SCS topics can be found within the SCS community portal. Information is also shared across the community and questions relating to the SCS can be raised with other community members.

The SCS Community Portal can be accessed via this web page.

http://scsavaya.com/

SCS administrators would first register with the Community portal.



Once registration is confirmed, access to the portal is available.