SARK

VOICE DATA AND INTERNET PLATFORM

SARK UCS/MVP VoIP/TDM PBX

Administrators Guide V3.1

SARK Version 3 Release 1-125

Aug 2011

Contents

Copyright Information

Introduction

The SARK UCS/MVP PBX server provides a resilient SIP/TDM PBX solution for system integrators and PBX resellers. It is based upon Digium's Asterisk switching platform running on either

- SME Server Linux
- PIKA Technologies Warp embedded Linux platform
- CentOS/Redhat EL5 Linux

The product has established a reputation for being easy-to-use with a very small footprint while being functionally able to compete with traditional proprietary PBX offerings at a much lower overall cost-of-ownership. There is also a high availability add-on which can give SARK users close to 100% uptime for their PBX (at the cost of deploying a second server).
SARK V3.1.0 is delivered as a series of Redhat RPMs ready to be installed onto an existing SME server 8.x or vanilla EL5; It is also available as a ready to install .iso image or as a complete ready-to-run system on regular Intel hardware or on the Warp PPC embedded platform.

One rather unique feature of SARK is its ability to automatically recognize and provision PnP SIP phones (principally from Snom, Yealink and Gigaset) with no human intervention and no special network setup. This means that, unlike competitive VoIP offerings, which can take several hours or even days to set up, SARK can be deployed into an unknown network (provided only that the network has a functioning DHCP server) with brand new factory set phones and require no initial set-up. The system will come up; provision the phones as they come on-line. This makes the system as easy and quick to install as a traditional TDM PBX, an important consideration when installing into small businesses where cost is often an overriding issue.

In addition, the on board SARK UCS/MVP software provides a feature-rich graphical workbench and decision engine designed to generate and run efficient PBX images. All adds moves and changes can be done remotely as soon as the system is installed.

Features Overview

SARK provides an easy to use graphical workbench and decision engine that controls and manages the PBX.

SARK UCS/MVP features

- Zero touch setup for PnP capable SIP phones
- Fast, automated installation
- Resilient High-Availability (option)
- Multi tenant support
- Add or change extension and voicemail accounts in seconds
- Integrated, extensible automatic provisioning service for all major SIP handsets
- Supports all Asterisk-supported trunk technologies
- Reduce long distance costs with LCR and powerful pattern-based outbound routing
- Route incoming calls based on time-of-day, DID, Caller ID or caller ID pattern
- Supports BLF, call parks and directed call pickup
- Create infinite level interactive Digital Receptionist (IVR) menus
- Design sophisticated recursive call groups
- True hot-desk support (option)
- Advanced on-board voice recording feature (option)
- Manage callers using ACD and Queues
- Detect and direct incoming faxes
- Automatic Backup and one-click Restore
- Powerful on-board firewall
- easy to use network management

SARK hardware platforms

There are 4 models in the SARK range. The range in capability from 8 channels and 20 endpoints up to 120 channels and several hundred end-points per node.

MODEL	**DESCRIPTION**	**Expansion Slots**	**MEMORY**	**Storage**
500	Embedded	2	256Mb	2Gb Flash
850	1U rack mount	1	1Gb	80Gb SATA
1000	1U rack mount	1	1Gb	80Gb SATA
1200	2U rack mount	3	2Gb	160Gb SATA

Fore more information on the SARK500 entry level system please see the *SARK500 admin guide*.

All SARK units are capable of running their own inboard telephony gear. Depending on the model, they can be fitted with up to 8xISDN2(BRI) channels or up to 120xISDN30 (PRI) channels (lines) per module. For more channels, the modules can be stacked into clusters.

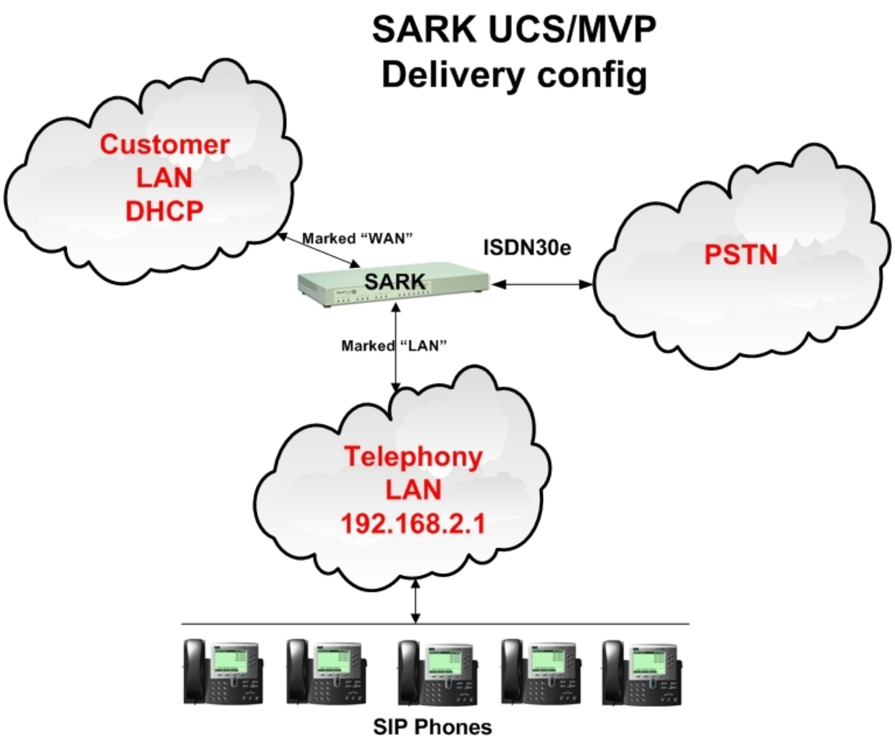
Modes of operation

Depending upon the model, SARK can run in one of two modes; either as a discrete network server as part of an existing network setup or as a server/gateway.

The S500 and S850 (which only have one NIC) always run as discrete network servers. The S1000 and S1200 can be delivered with twin Ethernet circuitry terminating in RJ45 sockets to the rear of the enclosure. These units can run in server/gateway mode. The sockets are marked “WAN” and “LAN”. The WAN socket connects upstream to one of the following

- Customer LAN
- cable or ADSL router

The LAN socket connects downstream to the phones. Unless you specify otherwise, single S1000/S1200 systems will be delivered pre-configured to run in Server/Gateway mode and set to request DHCP from the upstream network. The downstream LAN will be set to 192.168.2.0/255.255.255.0 with the SARK unit itself running at 192.168.2.1.



Changing the low-level system defaults

If you wish to change the factory default settings you can attach a screen and keyboard directly to the PBX server and log in as admin (with the Aelintra supplied password). This will run a wizard type application which you can use to change underlying settings such as the system mode, domain information and IP addresses.

Server Only

In server only mode, SARK is attached to an existing network and provides PBX, services to the network. Perimeter protection, internet sharing, caching, port forwarding and other services will be provided from an existing firewall/perimeter protection device or server. To run in this mode, the RJ45 socket marked LAN, should be connected to an available socket on your network LAN hub/switch using a standard RJ45 Cat5 cable. The RJ45 socket marked WLAN should not be connected. You should also forward the following ports to SARK from your firewall

PORT	NAME	TYPE
5060	SIP	UDP
10000->20000	RTP	UDP
4569	IAX2	UDP
443	HTTPS	TCP
45678	SSH	TCP

Server/Gateway

In server/gateway mode SARK UCS/MVP provides full perimeter protection (firewall) to the downstream network and manages all interactions to and from the upstream network. To run in this mode you should connect the WAN socket to your upstream network or Internet modem (either cable or ADSL). You should connect your LAN socket to an available socket on a network switch using a standard RJ45 Cat5 cable. If the upstream network has its own router then you should forward the following ports to SARK

PORT	NAME	TYPE
5060	SIP	UDP
10000->20000	RTP	UDP
4569	IAX2	UDP
443	HTTPS	TCP
45678	SSH	TCP

You can run your upstream router either in bridged or “no NAT” mode. In Bridged mode you will need a single public IP Address whereas in “no NAT” mode, you will need at least two public IP Addresses; one for the router and one for SARK.

Equipment Deployment

Unpacking

Your SARK UCS/MVP platform and ancillary components are carefully packed to your order at the factory. Enclosed with your shipment is a bill−of−material detailing each component in the shipment. Before doing anything else, check each component against the bill to ensure that all components are present and none have been damaged. Whilst every reasonable care is taken to ensure that the system reaches you in the same condition it left the factory, it is an unfortunate fact that occasionally a component may be damaged in transit. If you find a damaged item then you should immediately contact your Distributor/Reseller to obtain an rma number which will allow you to order a replacement.

Equipment Placement

Before beginning the installation proper, it is good idea to give some thought as to where you are going to site the system components, in particular, the server itself, the gateways (If any), the network switch and the IP telephones. Generally speaking, the server should be sited in a well ventilated location, away from high traffic areas in the workspace and ideally, above the floor. You should avoid stacking any other items on top of, or around, the casing to avoid overheating. Should the unit overheat as a result of restriction of the vents then this will automatically invalidate your warranty.

WARNING! ***NONE of the rack capable units may be mounted solely by the rack ears. You must ensure that there is adequate support at the rear of the unit. This can be done either by ordering the optional rack-mount rail kit from your supplier or by using a suitable rack tray.***

Maximum Cable lengths

- Unless your network switch manufacturer’s instructions state otherwise, the PBX server may be sited up to 100m (328 feet) from the network switch when using CAT5 or CAT5e UTP cabling, or 10m (33 feet) for stranded patch cable.
- When operating in Server/Gateway mode to an upstream router, the PBX server should be no more than 5m (16 feet) from the modem (cable or DSL).

- Analogue Telephone Adapters (ATA's) and SIP/IAX Gateways may be sited up to a maximum of 100m (328 feet) from the network switch when using CAT5 or CAT5e UTP cabling, or 10m (33 feet) for stranded patch cable. They may be up to 10m (33 feet) from any attached analog telephony equipment or carrier termination points (i.e the telephone company network terminators (NT)).
- IP telephones can be sited up to 100m from the network switch when using CAT5 or CAT5e UTP cabling, or 10m for stranded patch cable.
- If you have ordered any digital telephony cards as part of your system (ISDN2e or ISDN30e), they will have been predefined to your system with a line build out of up to 40M (133 feet).

Network Port Assignment

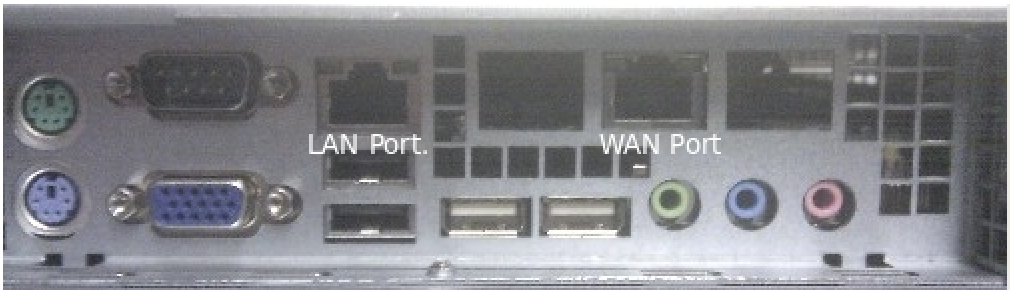
The Sark500 and SARK850 units are fitted with a single RJ45 Ethernet port.

SME 7.x (CentOS 4) units of the Sark650xp (discontinued), SARK850 and SARK1000 each have four (4) RJ45 Ethernet ports assigned as follows (when viewed, left to right, from the rear of the enclosure);

Port1 – unused
Port2 – LAN
Port3 – WAN
Port4 – unused

SME 8.x (CentOS 5) units Sark650xp SARK850 and SARK1000 each have four (4) RJ45 Ethernet port appertures assigned as follows (when viewed, left to right, from the rear of the enclosure);

Port1 – LAN
Port2 – unused
Port3 – WAN
Port4 – unused



The SARK1200 has two (2) RJ45 Ethernet ports assigned as follows (when viewed, left to right, from the rear of the enclosure);

Port1 – LAN

Port2 – WAN

ISDN Port Assignment

The S500 and The S850 can each be fitted with up to four (4) ISDN2e ports, while the larger machines can be fitted with up to eight (8) ISDN2e ports or up to four (4) ISDN30e ports. Ports are assigned as follows (when viewed, left to right, from the rear of the enclosure);

ISDN2e (S500) – 1, 2 and 3,4 (2 per daughter-board)

ISDN2e (S850, S1000, S1200) – 1,2,3,4,5,6,7,8

ISDN30e (S850, S1000, S1200) – 1,2,3,4

Notes ISDN QSIG and ISDN DASS

- In UK, only ISDN30e (QSIG) is supported. If you have older ISDN30 or DASS equipment then it will need to be upgraded.
- All SARK ISDN terminations are to RJ45.
- Eight-way (16 channel) ISDN2e cards use Siamese ports. They require made-up or pre-ordered split Cat5e patch cables.

Network Switch

The network switch should have enough ports to handle all of your IP connected telephones plus room for growth. It should be sited away from high traffic areas in the workspace and it should have sufficient front clearance to accommodate the RJ45 connectors from the UTP cables. You should also ensure that there is adequate access to enable easy addition/removal and rerouting of cables from time to time. UTP cables should be uniquely identified and marked at both termination points in order to facilitate easy tracing from device to switch.

If you intend to deploy a POE capable switch then you should ensure that its total power output is adequate for the overall load that the POE phones will impose. This information is available from the phone and POE switch manufacturers.

Power Up

Once you have decided upon a satisfactory location, install the network switch. Everything else will connect to this device so it’s the best place to start. If your workplace is already cabled for a computer network you may wish to assess whether you have sufficient access points to handle an integrated computer/telephone network. This may necessitate new cable runs and/or switch upgrades and it is best to do these now before any further equipment is positioned.

Next, install the SARK UCS/MVP server platform. Attach the LAN socket on the rear of the SARK UCS/MVP enclosure to the network switch using a Cat5e (RJ45) UTP or braided patch cable (depending upon distance). Attach the WAN Socket to your upstream network switch or router. Bring up the network switches and the SARK UCS/MVP server. The server will take about 3 minutes to boot and run through its startup checks. Your SARK UCS/MVP PBX is now ready to be tailored to your requirements. Depending upon the support subscription you have with your supplier this will either be carried out locally by yourself, by your reseller or remotely by your distributor.

Logging into the system

The SARK UCS/PBX GUI manager is browser based. You can connect using any modern browser (I.E., Firefox, MSIE, or Chrome) with the following URLs

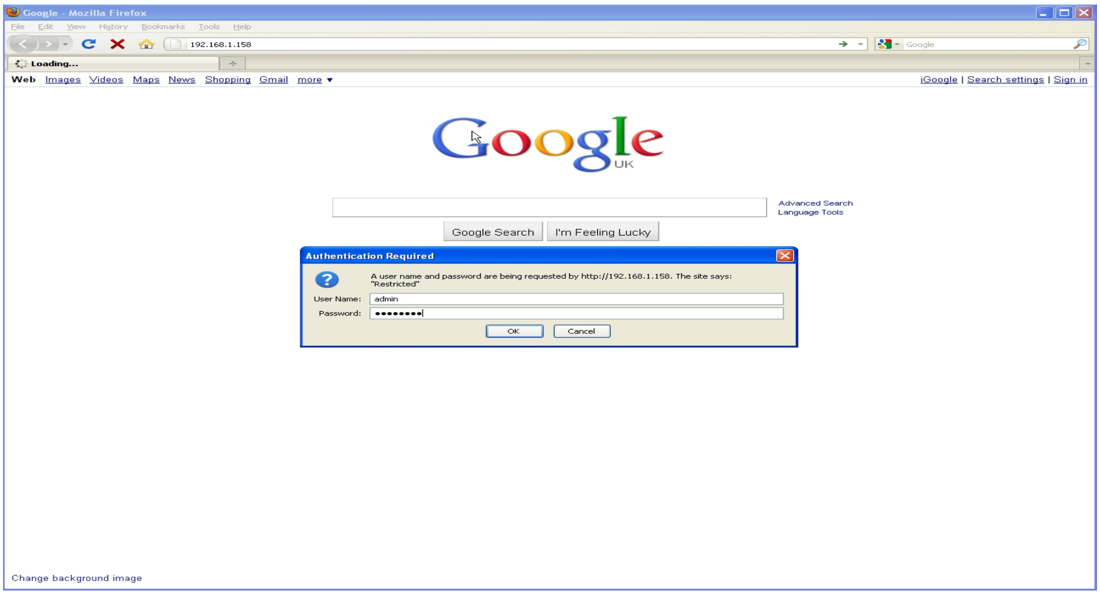
https://*local ip-address*/sark

The SME Server "*server-manager*" component is used to manage the underlying Linux platform. You can connect to it using

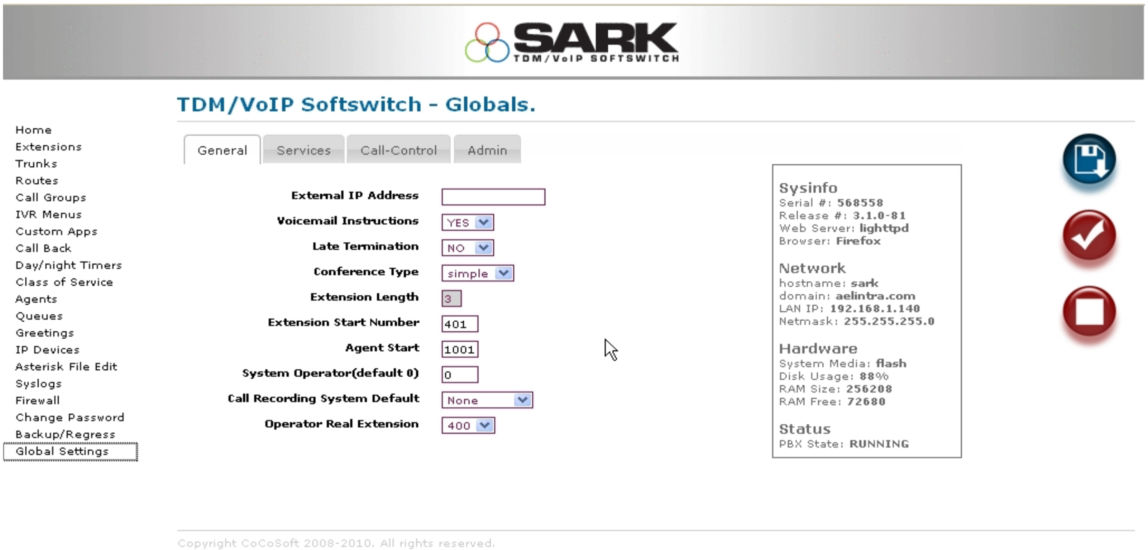
https://*local ip-address*/server-manager

The user-id is *admin*. The system password will either be found on a label on the PBX packaging or will be communicated to you by your reseller. Entering the user-id and password will display the SARK UCS/MVP home panel.

To log on to SARK you will need to know the IP address of the appliance. Type the IP address of the appliance in the address bar of any Web browser on the same subnet. The SARK login appears.



Type the user name and password in the appropriate text box. Click the OK button. The SARK 'globals' page appears.



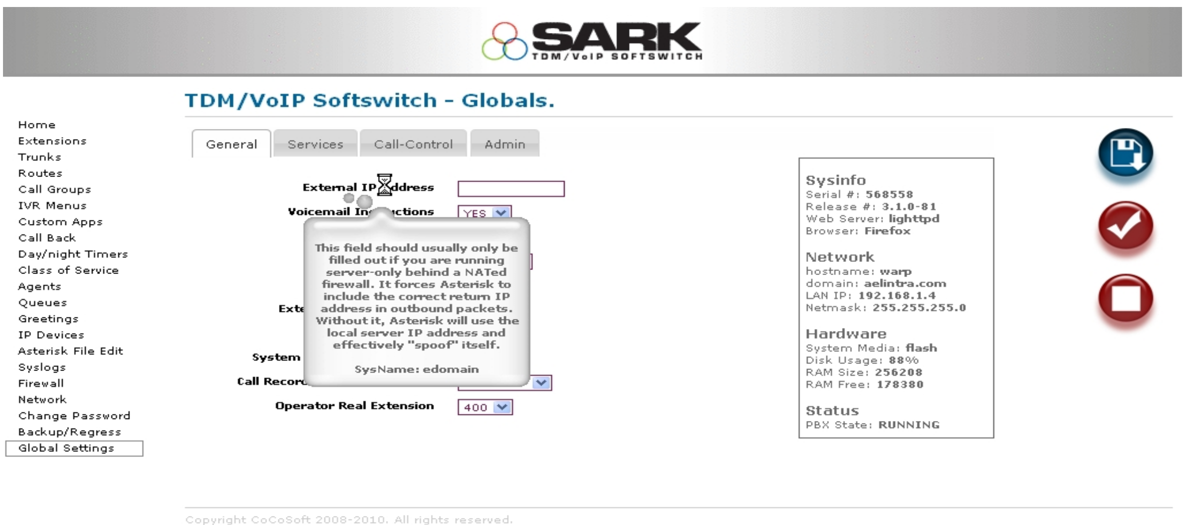
The System Statistics section (to the right) shows general status information.

Using SARK

The SARK browser pages follow a standard layout. The figure below shows a typical SARK Web page.

Navigation is handled by the column to the left of the screen. Modifiable data appears in the data window in the centre and information and action buttons appear to the right. All data fields have instant help (see below). To save your changes, press the save (disk icon) button. To commit your changes (i.e. bring them into service), click the tick, or checkmark, button; this will cause SARK to regenerate the underlying Asterisk configuration files and issue a soft reload to the PBX.

System Help



Every name field in the system has context sensitive help associated with it. All you need do is hover the cursor over any name field for an explanation of the field's function.

System Buttons

The system buttons are clustered to the right of each data panel.   The available buttons are as follows;

NEW button.   Used to create a new object instance

SAVE button. Used to save a change

ACTION button. Used to perform an action.

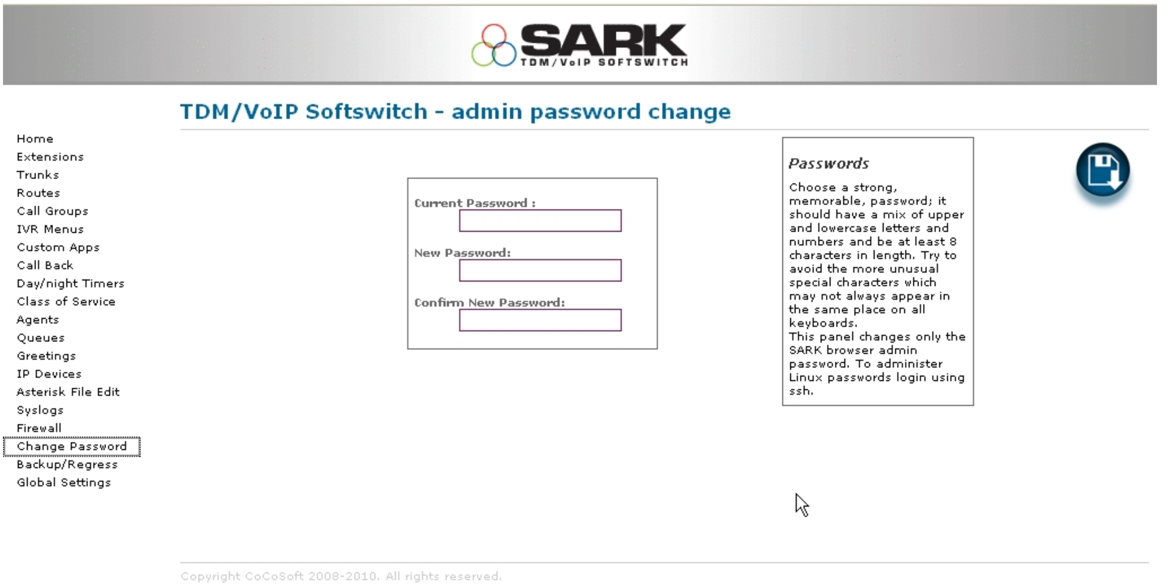
DELETE button. Used to delete an object instance.

COMMIT button. Used to “enliven” your changes by updating the PBX running instance

CANCEL button. Used to cancel the current operation and return to the parent screen.

Changing the Browser Password

For security reasons, we recommend that you change the default browser password immediately using the change password panel.



The system requires a password of at least 8 characters and you should try to use a mixture of upper and lower case and at least one numeric character. This panel is only responsible for the maintenance of the browser password. It does NOT change the root password of the box.

Changing the root user Password for SARK.

The root password can be changed by visiting the underlying SME Server Linux platform. You can connect to it using

https://*local ip-address*/server-manager

Documentation for SME server can be found on the SME server Wiki here

http://wiki.contribs.org/SME_Server:Documentation

The default set-up (PnP install)

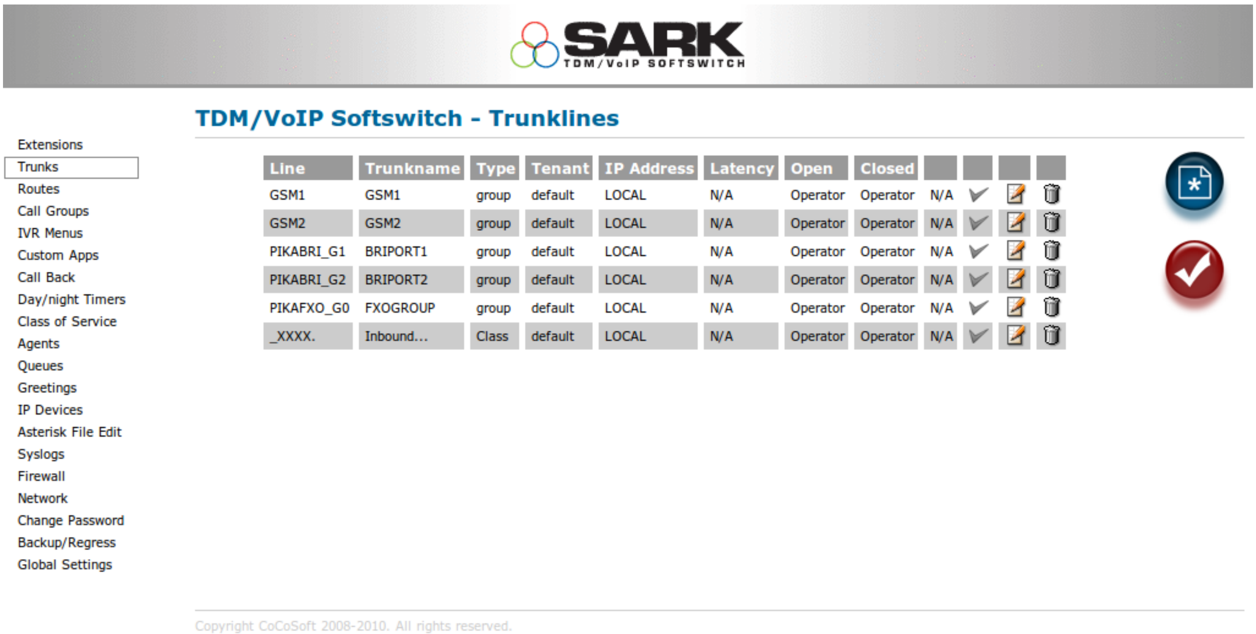
SARK is initially set-up to allow you to install it and be up and running within just a few minutes of powering it up. Provided you deploy SIP PnP capable phones (such as Snom, Yealink or Gigaset), they will be automatically configured and registered on-the-fly when they are powered-up.

Once connected to the ISDN lines, the SARK is ready to receive calls. As phones are powered up and configured, they are automatically added to a special ring-group called the 'RINGALL' group. Any calls arriving over ISDN will be automatically sent to the RINGALL group, which will ring all of the phones, and 'first to pick-up' will get the call. The RINGALL group can be removed as and when you move to more sophisticated routing and ACD configurations but initially it just allows you to get up and running very quickly. Also by default, outbound calls will initially be routed via the ISDN hunt group.

Of course, you will probably want to progress to more sophisticated call distribution and routing and you may wish to deploy VoIP trunks and perhaps remote phones. All of these things can be accomplished using the SARK browser-based interface. The following sections we will cover some of these topics in more detail.

Adding Trunks

Outbound trunks for your installed hardware and a general inbound trunk class are automatically installed on the platform so there is nothing to do to activate them. You will probably wish/need to create additional inbound and outbound routing (see Routes below) to handle DDI's, ACD and IVR requirements.



If you are running FXO channels, (or BRI without DNID presentation) then inbound calls will automatically be delivered to the 'operator' entry specified in the globals panel. The system default for the operator is to point to a ring group called RINGALL which simply rings all phones; you can, of course update this to point to another call-group, queue or IVR.

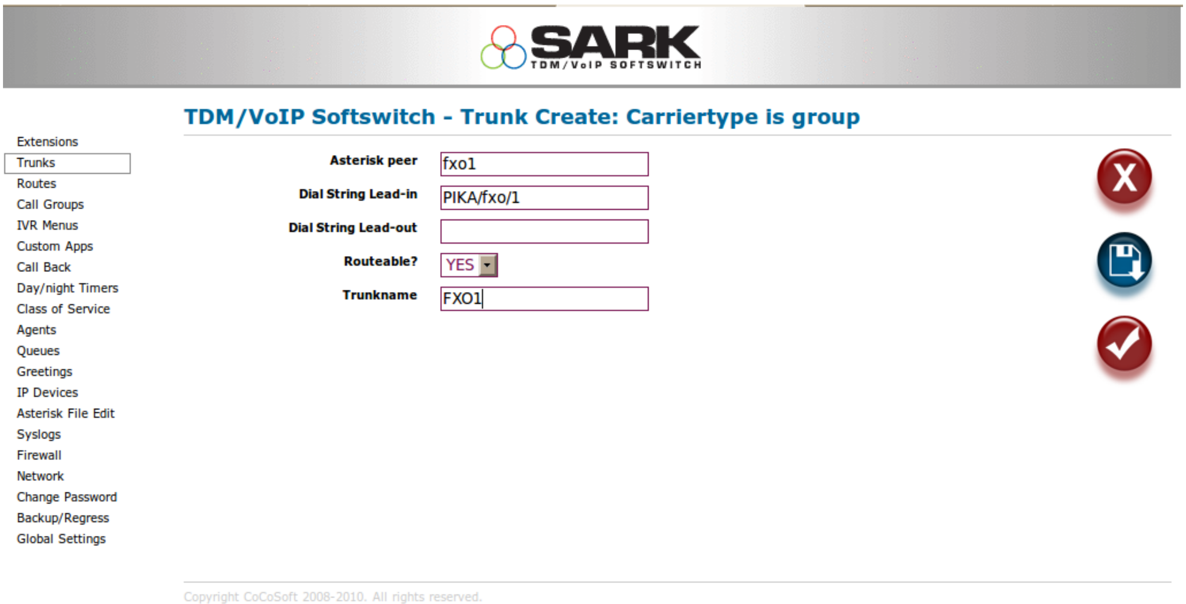
The routing of inbound calls falls into one of two categories; you can route by the Dialled Number ID (DNID) if you have digital lines with DNID enabled or you can route by channel name/number in the case of FXO lines.

To route inbound Digital calls with DNID enabled,simply create one or more DiD (DDI) trunks to route the inbound calls. (see the next section). You may need to confirm with your telephone line supplier (PTT) how many digits will be presented in the DNID (it may be 3 or more digits depending upon your carrier's practice).

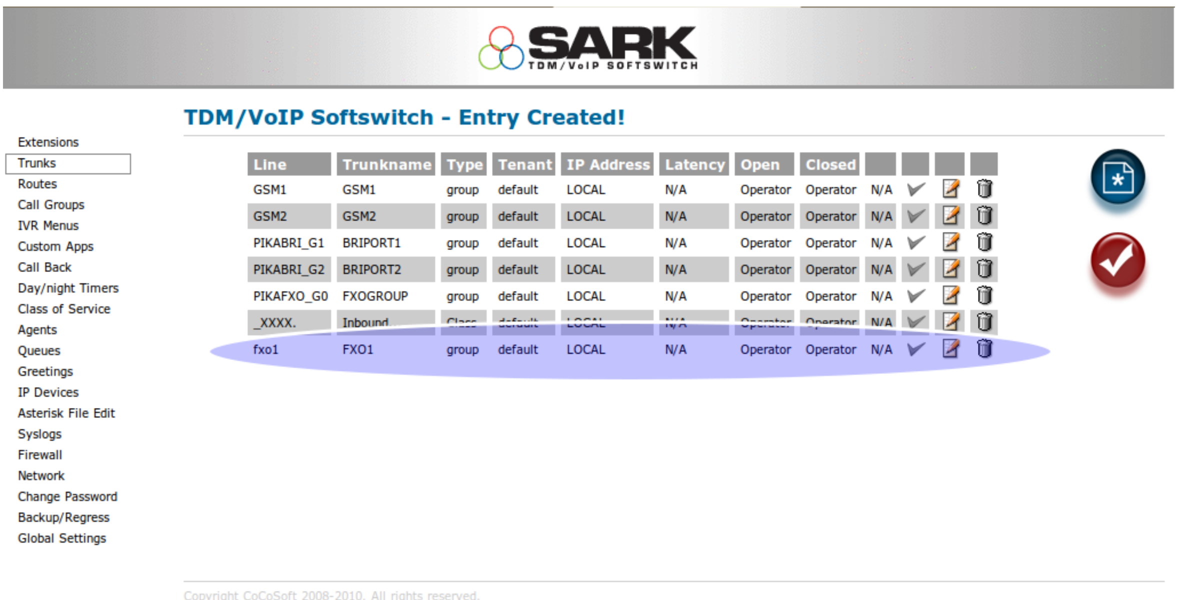
To route individual FXO channels you can set up a custom trunks and name them as follows:-

- for FXO, use fxo{*n};* where {n} is the port number on the tdm card

The following shot shows the creation of a trunk to handle calls to and from channel 1 on the FXO card.



N.B. It is important that you set the *routeable?* Variable to 'YES'. This will allow you to route calls arriving on this channel. This will create a trunk like the one highlighted below.

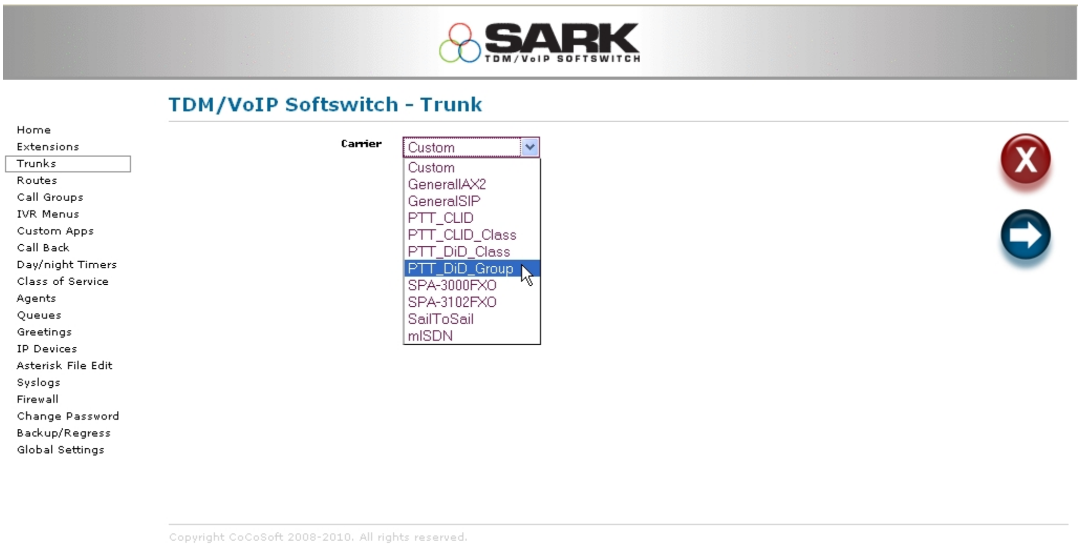


The trunk can be routed by clicking the edit button and filling out the 'open' and 'closed' route destinations in the normal way.

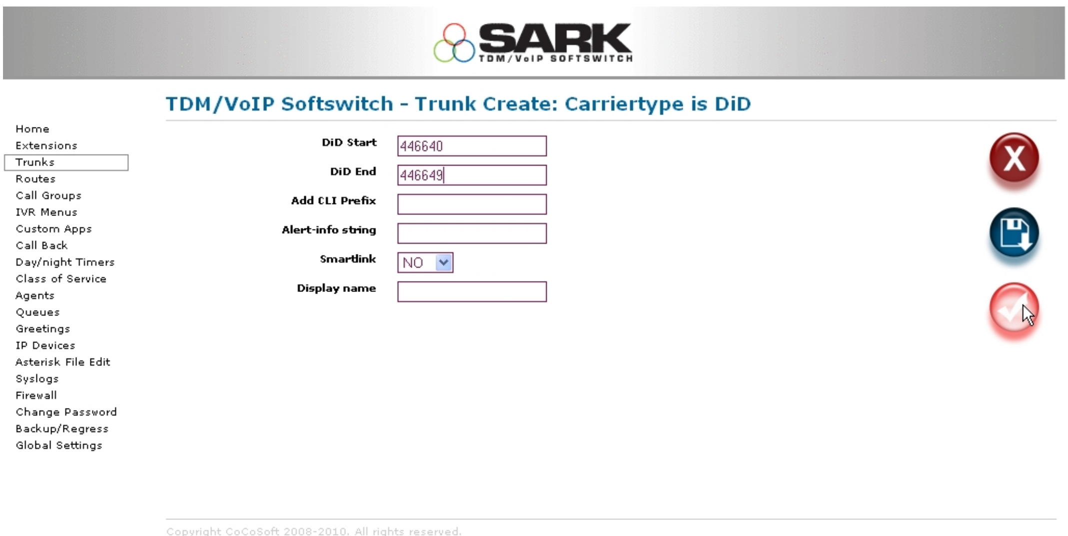
Adding a DDI (or DiD) Trunk

Digital (ISDN) and VoIP (SIP/IAX2) inbound calls are usually routed by testing the 'Dialed Number ID' (DNID). To confuse matters further; in digital systems these numbers are often allocated in blocks by the telephone company and known as DiD numbers (Direct Inward Dial) or DDI numbers (Direct Dial In). SARK has a special trunk construct to manage and route these numbers. It is called a *PTT_DiD_Group* trunk and you can define a set of one or more contiguous numbers using this trunk type.

Let's add an example DiD group with the range 446640 to 446649. To do that we can create a trunk object called a PTT_DiD_Group. Click the new button on the trunks panel and then choose "PTT_DiD_Group" from the drop down.

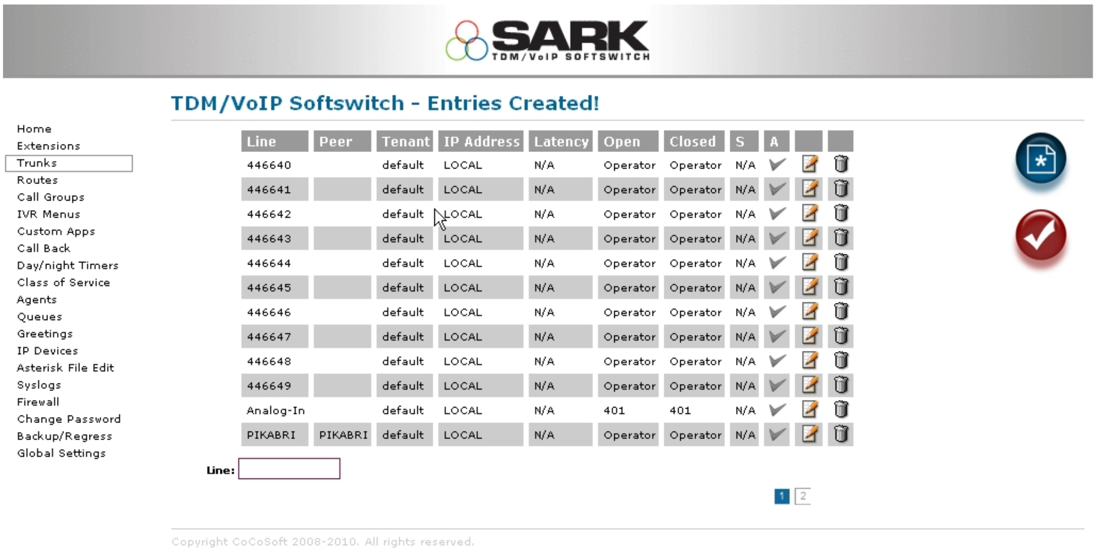


Now fill out the number range...

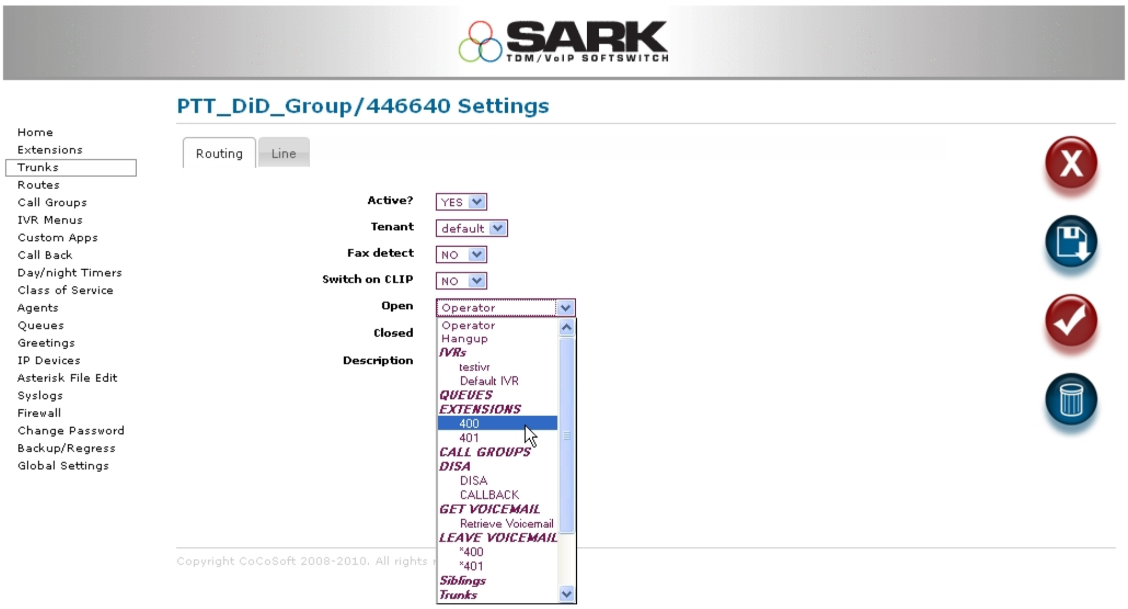


Click Commit to create the Trunks. Of course, the set of numbers in your Group can quite legally consist of a single number, in which case you would leave the end box blank. N.B. Even though the update screen requests positive confirmation of a DiD

Group create, it is not unknown for a digit to be entered incorrectly causing hundreds or even thousands of DiDs to be created. Not to worry, if this happens you can simply regress SARK to the commit BEFORE you made a mistake.(see the section on Backup/Regress).



Our trunks have been created and we can now route them to their destinations by clicking the edit button on each trunk.



Route the inbound calls by clicking the open and closed inbound route drop downs and choosing a destination from the available system endpoints.

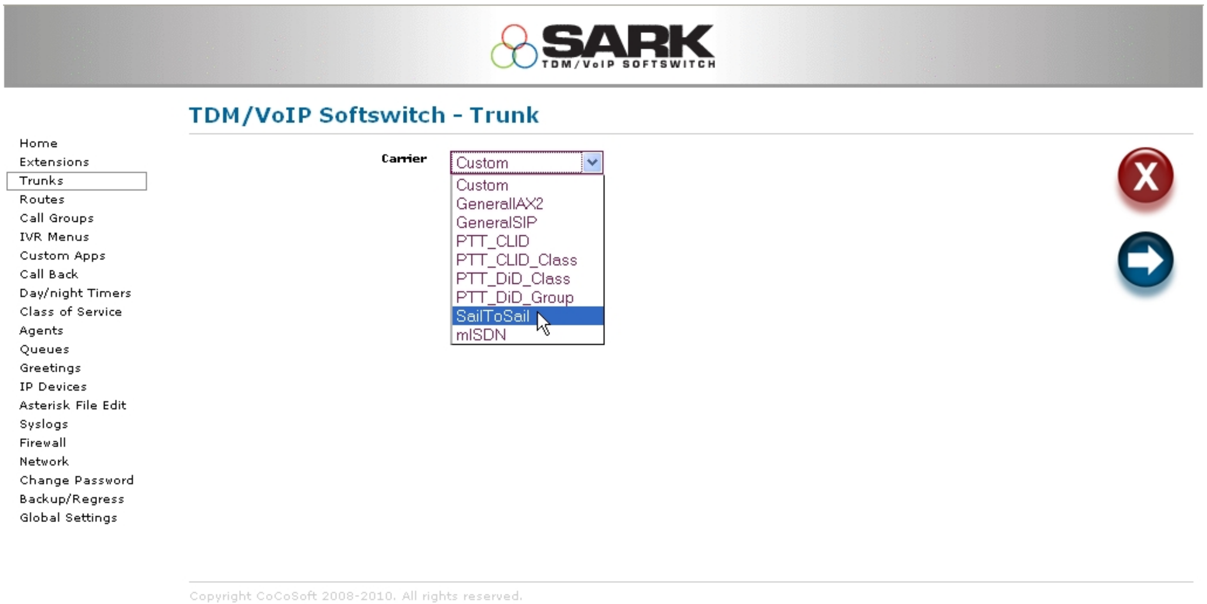
Smartlink

SARK has a flag called "smartlink" which you can set on when you create a DiD group. This is useful when you first create a set of extensions and then create your DiD trunks later. Smartlink will match the numbers of each extension to the right hand side numbers in the DiD group. For example, if you had an extension range of 400 to 420 and a DiD range of 668400 to 668420 then SARK will automagically route inbound calls on 668400 to extension 400; calls on 668401 to 401 and so on. This can save a lot of work when there are lots of extensions to be routed during system setup.

Adding an IAX2 "Sibling" Trunk

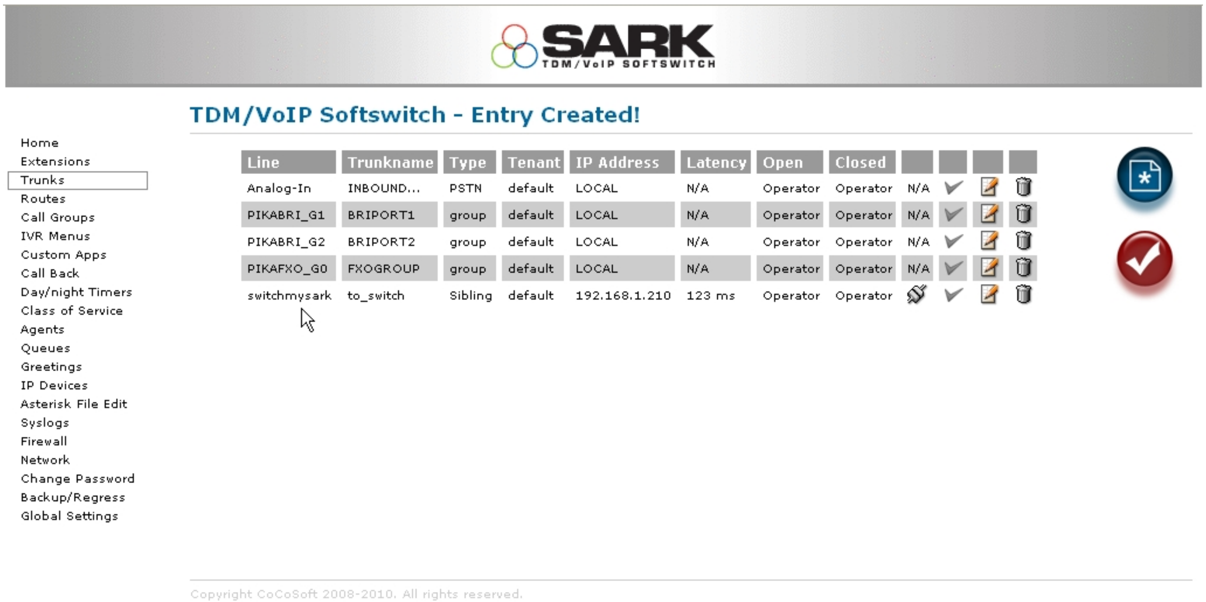
Sibling trunks provide a convenient way of routing calls between SARK instances. In this way, you can easily and quickly build a network of interconnected PBX's which route calls to one another depending upon the number dialed.

To create a Sibling trunk choose SailToSail from the trunk type dropdown in Trunk create

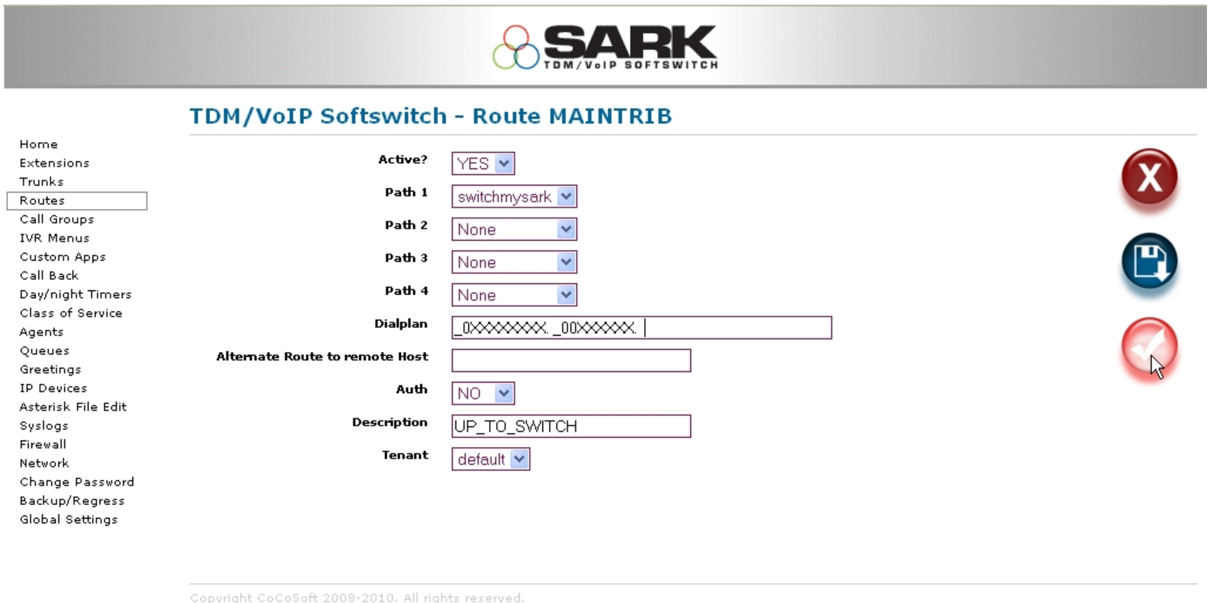


Now fill out the link information. In the Sibling name box enter the hostname of the PBX you wish to link to (just the short name not the FQDN). Fill out the IP address and include a password (this will be the same on both sides of the link). If the Sibling is remote (i.e. not in the same subnet) then you may want to have SARK create a firewall rule for it. In the example below, the other machine is in the same subnet so there is no need to create a rule.

Now click on save or commit to create your new trunk….

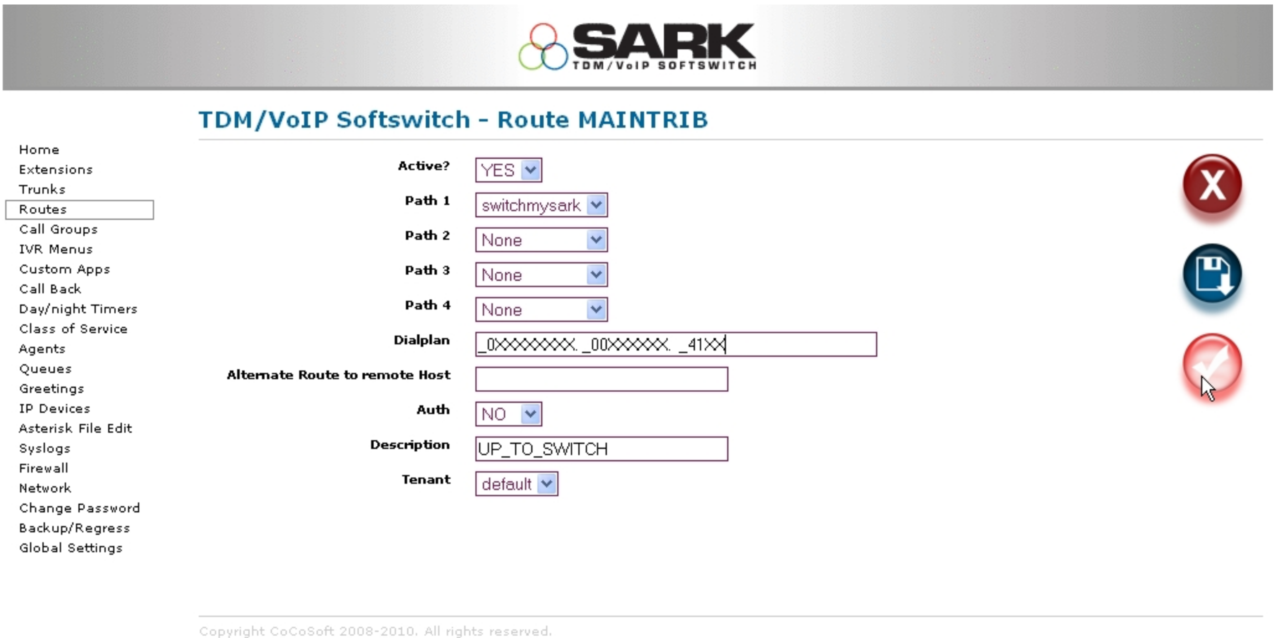


SARK has created a trunk for you with a peername which is the concatenation of your hostname and the remote hostname. You must now login to the remote PBX and create a mirror-image Sibling trunk to receive calls and send calls back. Once done, you can create a route to send calls up to the other PBX. In this example, we want to use the remote PBX as our outbound media server (perhaps for PSTN line consolidation) so we will send all of our outbound calls up to it. Here is a route that will do that…



Now, whenever we dial a PSTN number on the Sark500 it will be routed up to the other SARK PBX (perhaps a larger model) for termination onto the PSTN.

Perhaps we also want to allow extension-to-extension calling between the two PBXs. We can extend our route dial plan to include that also. Let's say, for example, that the extensions on the remote PBX are 4 digits in length and always begin with "41". We can modify our route as follows…

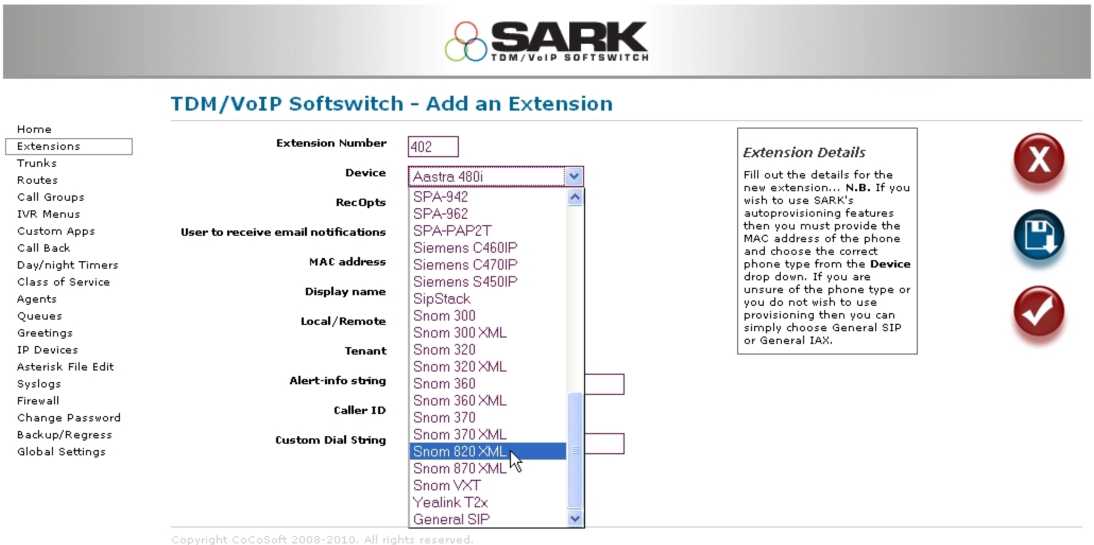


We've added the dialplan ***_41XX*** which will route any 4 digit dials beginning 41 up to the other PBX for termination. We would probably also create a dialplan on the remote PBX to route 3 digit numbers beginning 4 back to us (because throughout this guide, our examples use 3 digit extensions on the local PBX, beginning at 401).

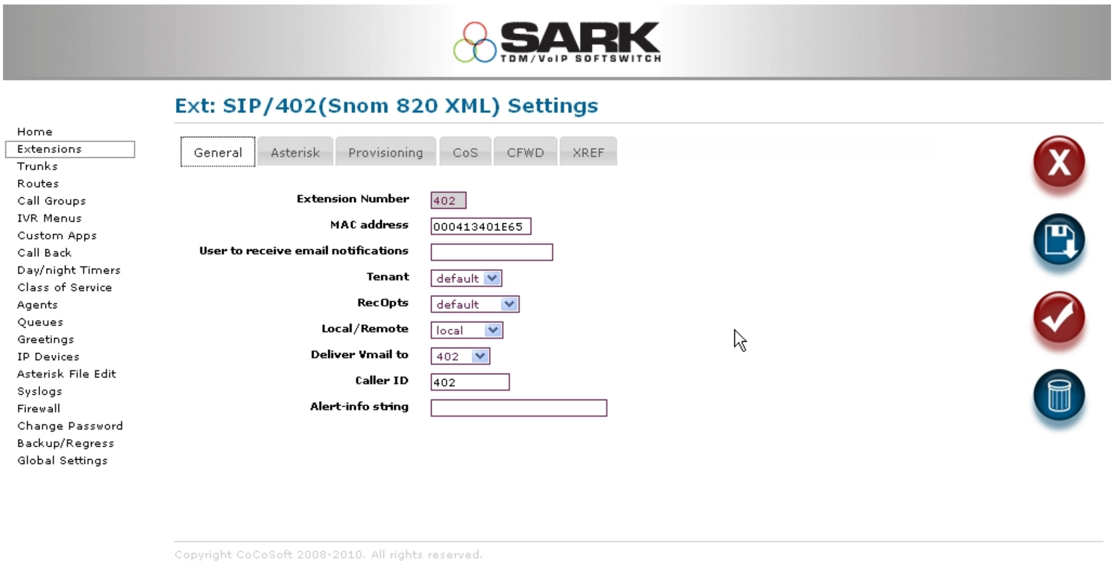
Adding Extensions

Extensions for the FXS channels are already defined in the system when it leaves the factory. There is nothing further to do. However, you will almost certainly want to define SIP extensions to the system.   If you have SIP Multicast (sometimes called PnP) capable handsets you can use SARK500's ZTP auto-configure feature to set up your phones (see the ZTP/PnP section below). For non-PnP-capable handsets you can add new extensions using the extensions panel ...

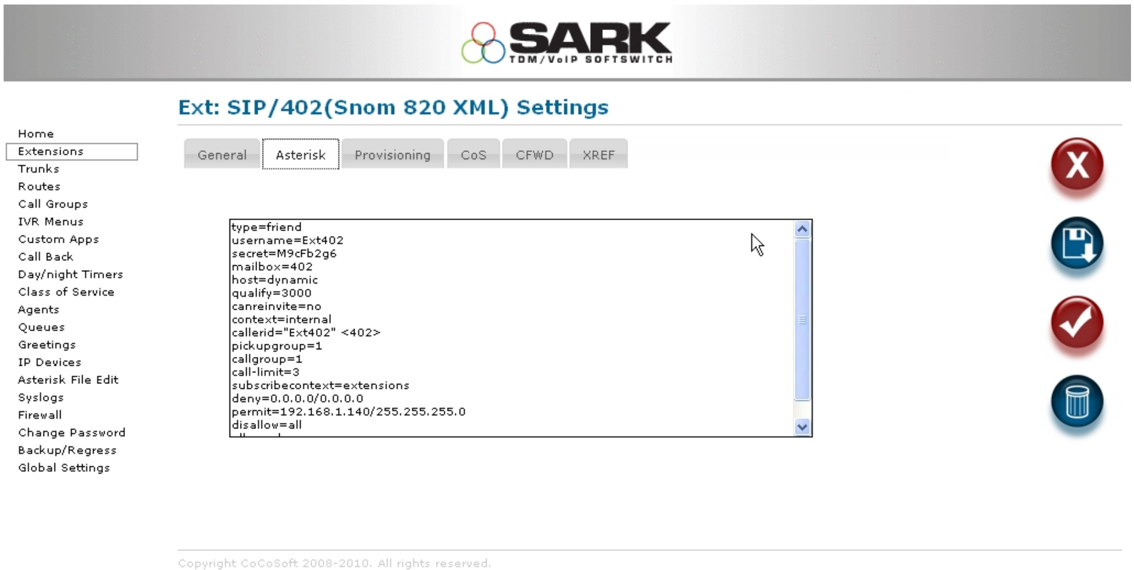
To add an extension; click extensions at the top of the navigation menu.   Then click the “new” button to create an extension.



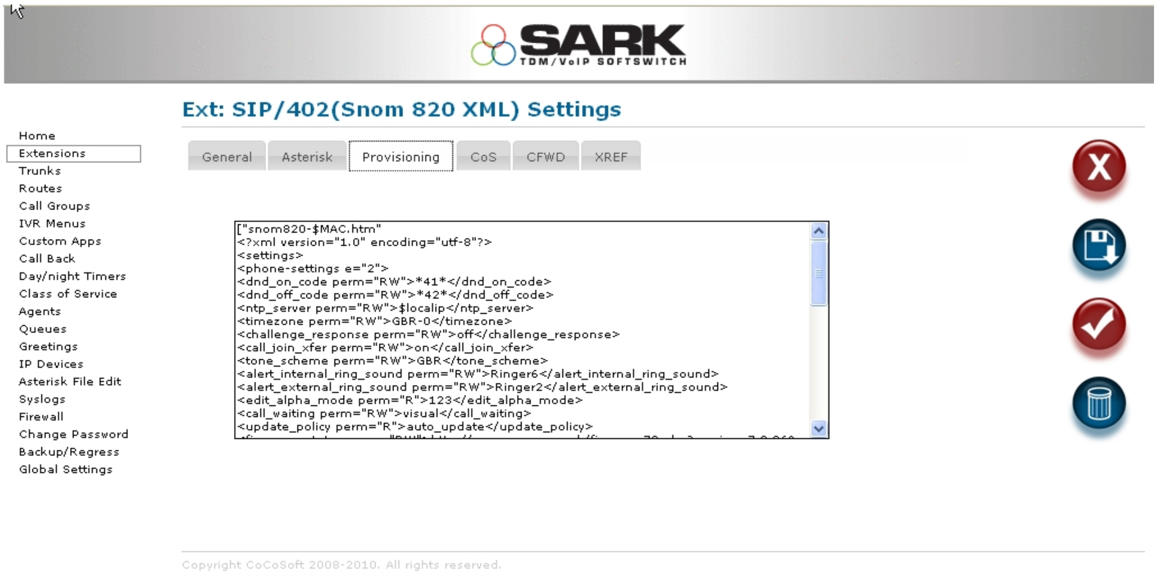
Choose the phone type from the device drop-down. Fill out the details for your phone and (optionally) enter the MAC address if you want SARK to automagically generate a TFTP provisioning file for your phone type. SARK has a fairly extensive phone database and it can provision most commercially available phone types.   Click the Save button if you have several entries to create or simply click the Commit button to create this entry and regenerate the Asterisk files immediately.



SARK will create the necessary Asterisk entries with automatic randomly generated passwords and the correct ACL checking for your subnet…



…And it will also generate the correct provisioning data for the phone type you chose…



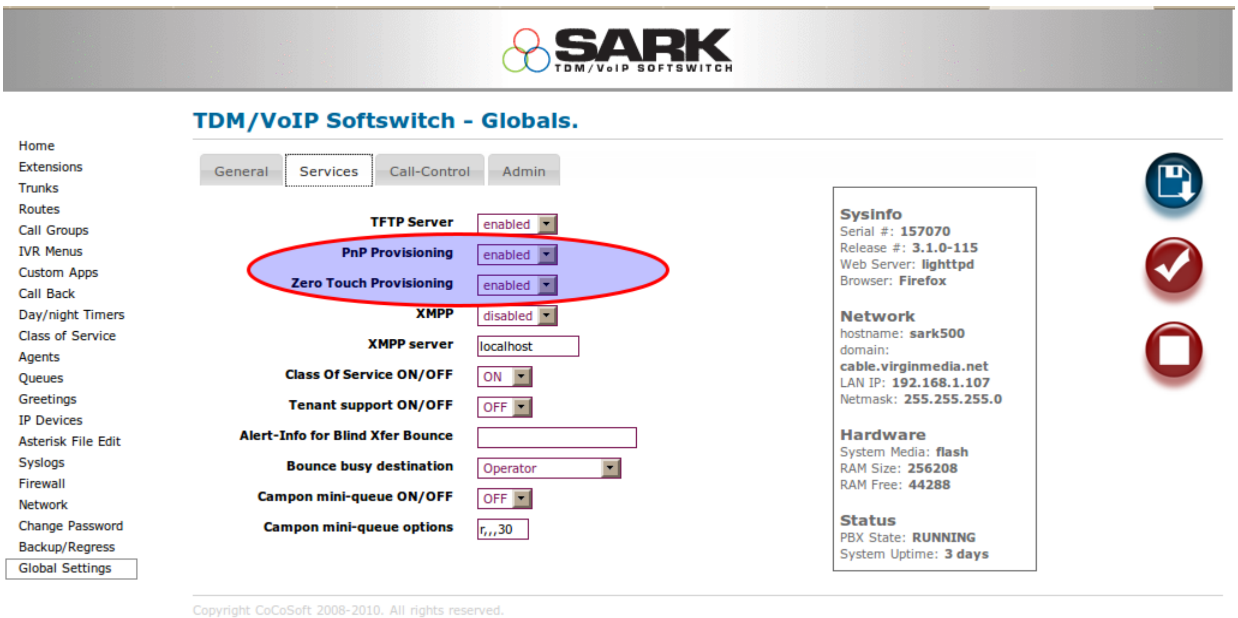
You may freely modify any of these entries SARK has generated for you and save them back to the database. You can also freely create your own provisioning templates and profiles allowing you to tailor the SARK provisioning platform to suit your individual needs.

Automatically adding extensions with ZTP/PnP

The SARK500 can automatically create extensions and provisioning data on-the-fly for phones which support SIP Multi-cast provisioning. This has a couple of major benefits for users of SIP phones that are SIP/PnP aware:-

- There is no need to run DHCP option 66, and no need to run an on-board DHCP server.
- The provisioning stream is synthesized by the listener on-demand
- No tftp or ftp files are stored on the server.
- New phones can optionally be provisioned and defined to asterisk on-the-fly by the listener/builder.
-

Turn on ZTP/PnP in globals panel.



'PnP Provisioning' (or SIP Plug 'n Play) turns on the SIP Multicast listener. This allows SARK to asynchronously tell a SIP phone where its provisioning file is located *without* the need to modify the existing DHCP server or to run an on-board DHCP server or even to run the SARK unit at a static IP address.

'Zero Touch Provisioning' (ZTP) works in tandem with PnP. When ZTP is enabled SARK will not only inform a phone where its provisioning data is but it will also build the data on-the-fly and update Asterisk at the time the phone first requests it. What this means is that you can simply power up a PnP aware phone and SARK will automatically create an extension for it in the SARK database, inform the phone where the provisioning data is and finally, regenerate Asterisk so that it is aware of the new extension. Thus the phone will come up, be automatically provisioned, register with Asterisk and be immediately ready to make and receive calls. This is very useful for medium to large roll-outs because it needs no prior set-up.

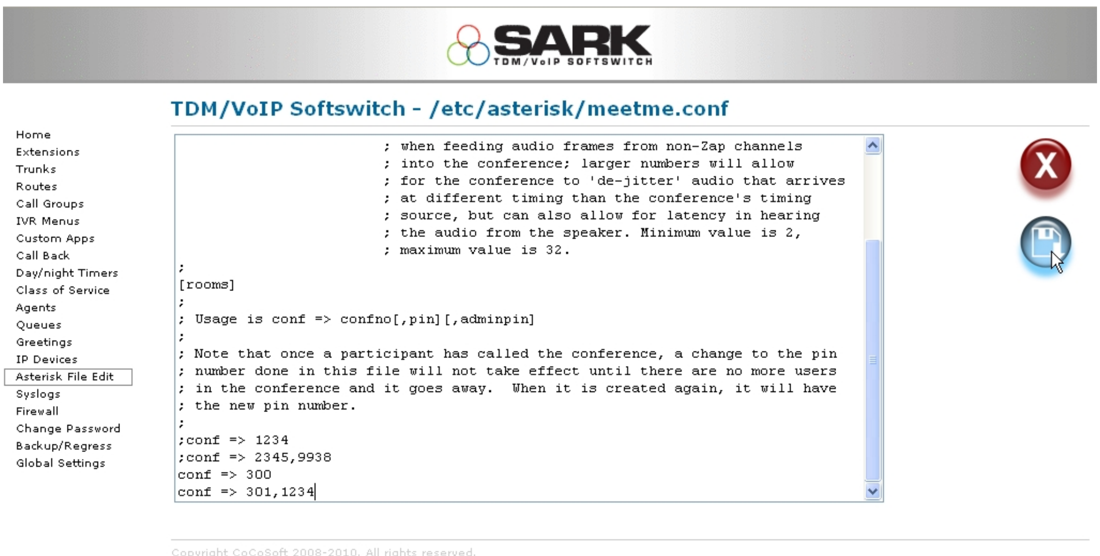
For security reasons, you should only run ZTP during initial system installation or when you have new phones to roll-out. The remainder of the time it should be switched off.

In order to be able to run multiple PBX servers in the same subnet, the Multicast listener must be able to selectively reply to only those PnP aware phones which it "owns" (i.e. are defined to it). For this reason, unless ZTP is enabled, SARK will only respond to requests from phones for which it already has an entry in its database. It recognizes individual phones by their MAC addresses. This mode of operation is much the same as regular DHCP 66 type provisioning; i.e. only phones which have been predefined to the system will be provisioned. In this way, multiple servers may all be listening for Multi-casts and each can respond to its own group of phones without disrupting other listeners.

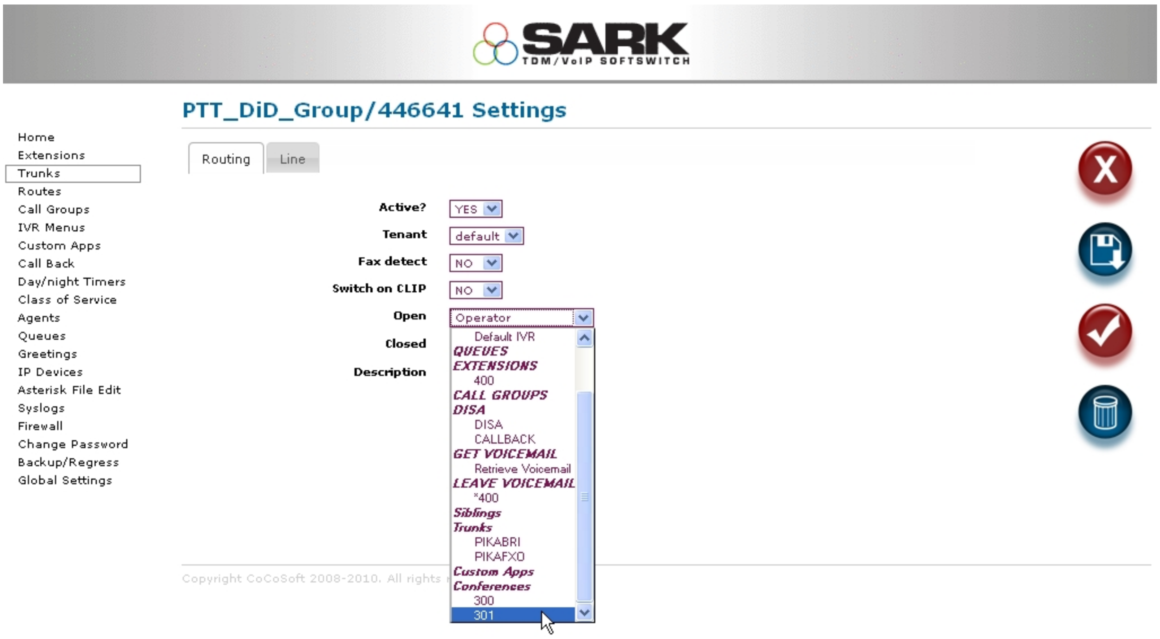
Conferencing

Conference rooms 300-303 are predefined to the system at the factory. If you want to add other rooms or change the conference room number you can modify the underlying Asterisk ".conf" file directly (it is called *meetme.conf*).   As a general rule, SARK keeps its management of Asterisk files to a minimum. You can directly modify most asterisk files just using the Asterisk Edit panel…

To modify a conference room simply choose the meetme.conf file and make your changes directly. In the example below we've just added conference room 301 and now we are about to save it back.



Once the conference room has been created in this way we can either dial it directly from any extension or we can select it in a route (it will auto magically appear in all end-point drop downs)… Below we route a DiD trunk to our new conference room so we can host a conference with an external callers.



Interactive Voice Response

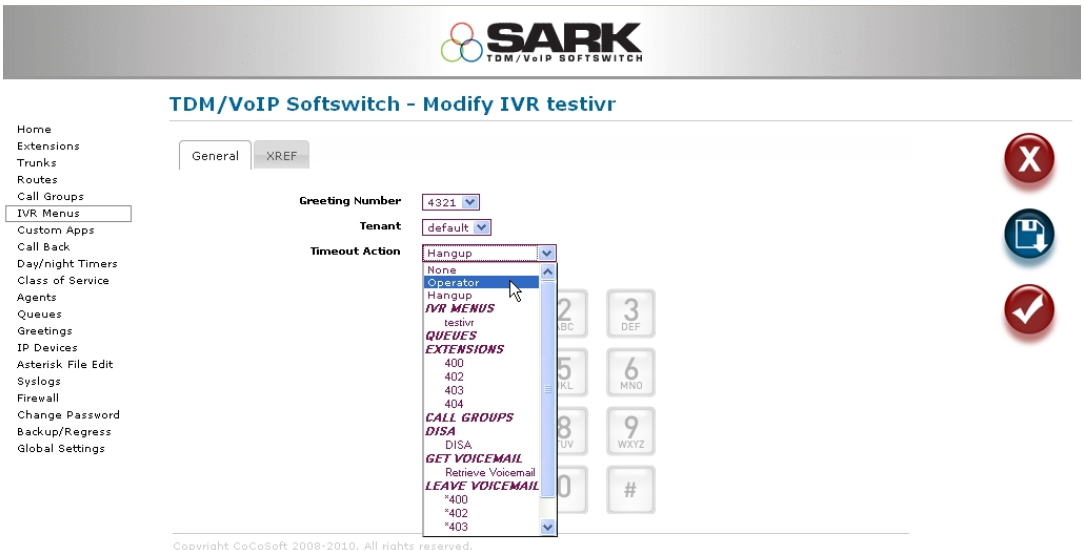
To create an IVR, you must first create a system greeting.. Simply go to any phone and dial *60*+nnnn, where nnnn is a 4 digit number that we will associate with our recording. –

60*4321

The auto attendant will lead you through the process of creating a recording. Let's work an example and record a message like this…

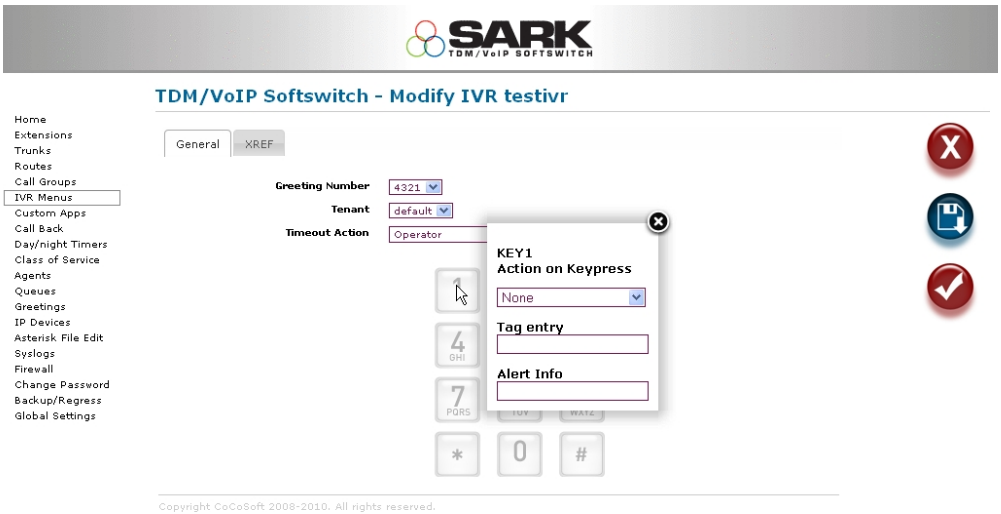
'Welcome to ABC Widget Corporation. Press 1 for sales, press 2 for accounts or please hold for an operator'

We can now go ahead and create our IVR. Choose the IVR panel from the left hand menu and then click "New" to create a new IVR.

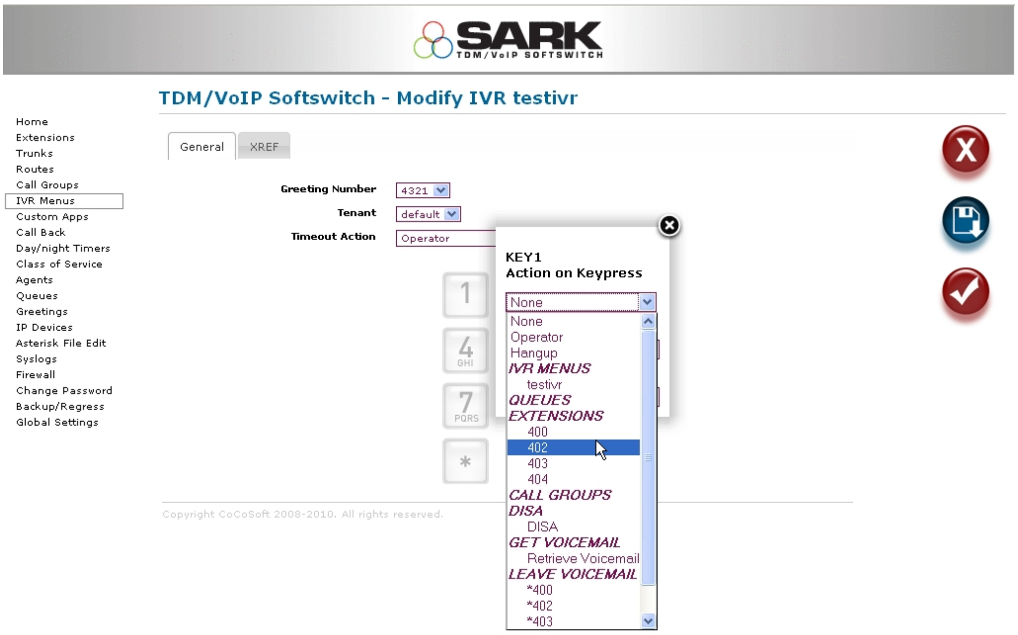


We choose our greeting (4321) from the drop down and then decide what to do if the caller does not press a key. Our greeting said "…or please hold for an operator", so we can choose "Operator" from the timeout drop down.

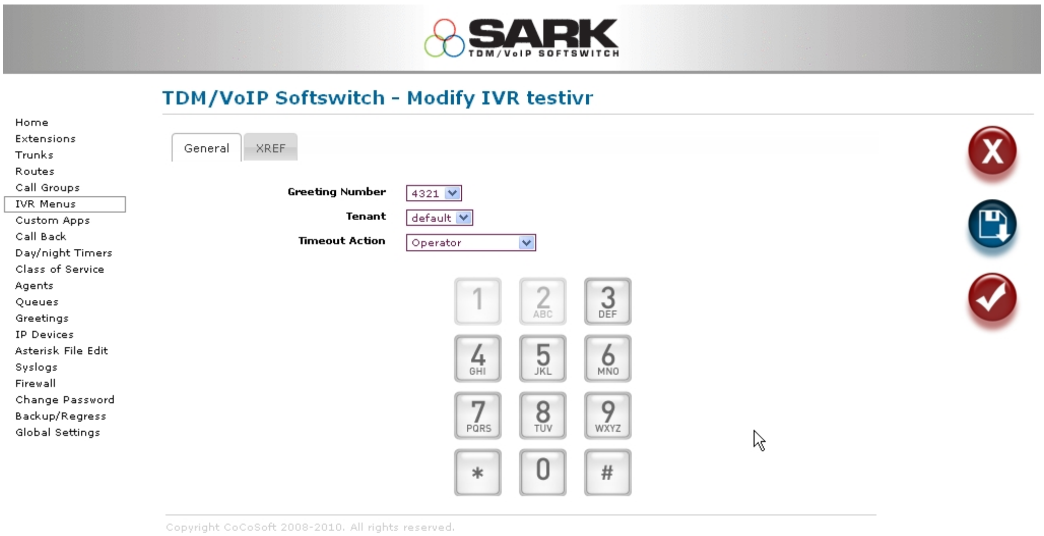
We can now choose our key-press operations by clicking on the keypad graphic and choosing an endpoint from the drop down.



And....



Finally, after committing the IVR, if we return to the screen we see .that SARK has updated the graphic to show at a glance which keys are in use…

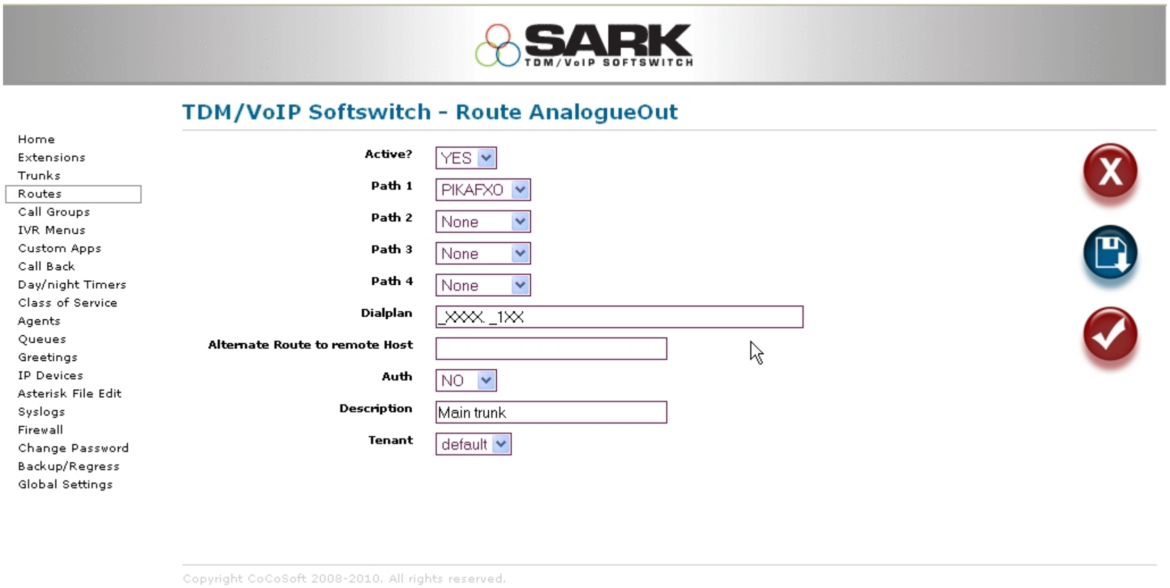


The IVR is now ready to use.

Adding Routes

Within SARK, an outbound route consists of a set of dialplans and up to four outbound pathways (Trunks). The SARK HPE processing engine will choose the first available route which matches the dialed number ID (DNID) .

To add a route, click the link Routes in the left navigation menu and then click the “new” button.



You can configure up to four trunks for each outbound route. They will be successively tried in the event that a trunk fails or refuses to honor the Dial. The dialplans are conventional Asterisk dialplans and you can code as many as you wish using white space as a separator.

Click Save or Commit to save your new route into the database and/or bring it into service.

Firewall

IN SME based system, the firewall is set automatically. In its default configuration, only the following ports are opened:-

HTTP (TCP 80)	WAN
HTTPS (TCP 443)	LAN
NTP (TCP 123)	WAN
SSH (TCP 45678)	WAN
TFTP (UDP 69)	LAN
SIP (UDP 5060)	WAN
RTP (UDP 10000:20000)	WAN
IAX2 (UDP 4569)	WAN

However, you can change/restrict these settings; either in your external firewall or by modifying the SME firewall settings.

Firewall guidelines

- Close port 5060 to the WAN unless you intend to conduct remote SIP operations (using a SIP carrier or remote SIP phone(s)). With many SIP carriers it isn't necessary to open 5060 at all because they will keep the port alive from the time you register. Check with your carrier.
- Close port 4569 to the WAN unless you intend to conduct remote IAX2 operations (using an IAX2 carrier or a remote IAX2 device).
- Close the RTP ports (Usually 10000-20000) to the WAN unless you intend to conduct remote SIP operations.
- ONLY open the firewall to SIP endpoints you know (unless the far end is using a Dynamic IP which changes often, in which case try to limit access to just that range, even if it is quite large, or consider using a VPN - see below).

SME Server Firewall

In SARK-3.1 we define the objects ''sailSIP'' and 'sail'IAX'' in the SME server database in order to manage the ports. To modify the default settings you must log in using ssh. The default ssh port is TCP 45678 but you can change this in the remote-access section of the server-manager.

Closing SIP and IAX2 ports in the SME server firewall

[]# config setprop sailSIP status disabled
[]# signal-event remoteaccess-update

[]# config setprop sailIAX status disabled
[]# signal-event remoteaccess-update

Restricting SIP and IAX2 port access in the SME server firewall

You can also add an *AllowHosts* statement to control external access;

[]# config setprop sailSIP AllowHosts 111.111.111.111/0,222.222.222.222/24
[]# signal-event remoteaccess-update

In this way you can limit access to just those remote extensions and trunks you want to allow in. The other alternative is to deploy your SAIL/SARK box behind a good quality firewall which can control access to the ports on behalf of the PBX. For frequently changing IP addresses such as home workers or road warriors we would recommend bringing them in over VPN if you can. Adding openvpn to SME server itself or to your firewall server is straightforward and you can then use softphones on VPN connected PC's or hardphones which can run openVPN (Snom 370,820,870 can all run openvpn).

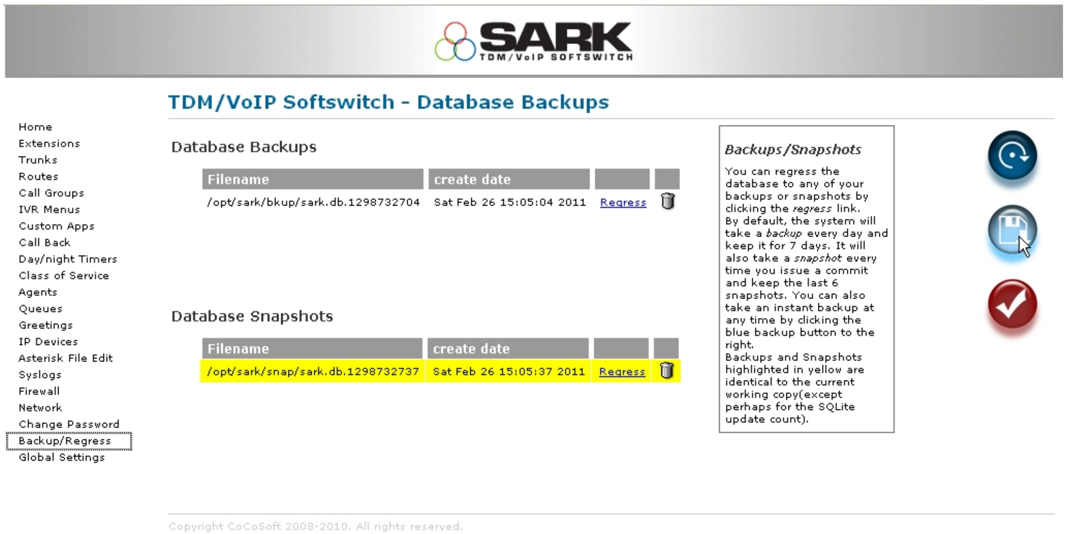
Finally, you should make sure that you put strong passwords and ACLs onto any IAX to IAX trunks you have that span the internet.

Remote phones

If you can, use a phone type which supports VPN tunneling. Snom 370, 820, 870 all support openvpn and you should also be able to run softphones over a VPN. If you can't, then implement strong passwords and ACL checking in the SIP definition for the remote IP address.

Backup/Regress & Save to USB

SARK will automatically spawn backups every night. It will keep up to 7 on-board backups and you can "regress" to a backup simply by clicking on it.   It will also take an "Instant Backup" (called a snapshot) every time you issue a commit. You can take a commit (or issue an explicit backup) before you begin a piece of work or make a change and then perhaps regress to the start version if you are not satisfied with the end result or if you make a mistake during configuration. You can view your current snapshots & backups by choosing Backup/Regress from the Navigation menu.

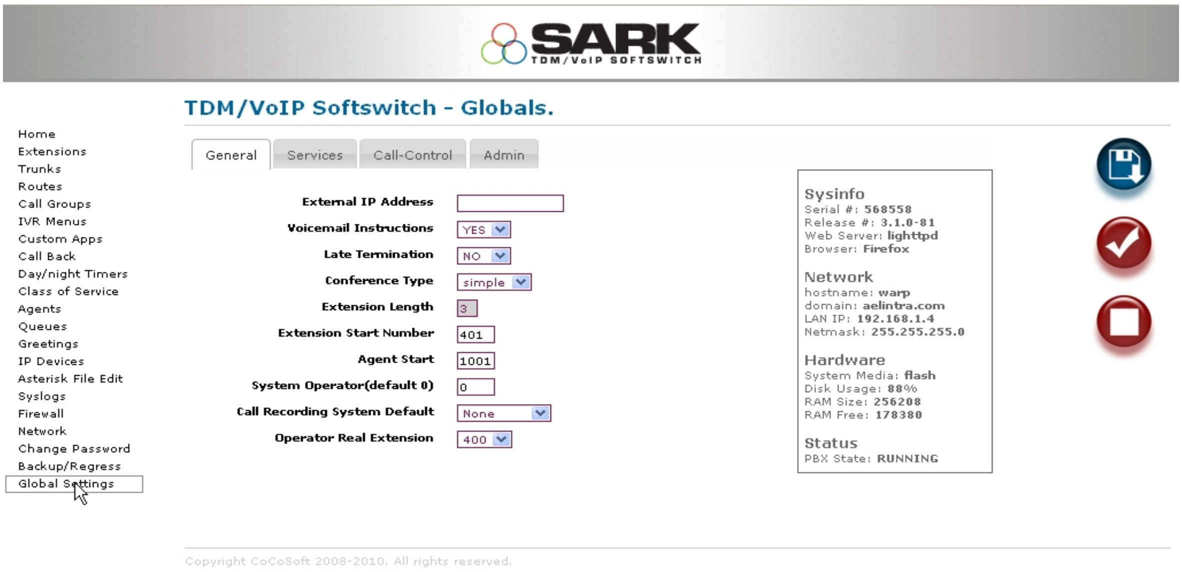


To regress to an earlier database version simply click the regress link next to the backup or snapshot you wish to use. Regression is non-destructive because SARK will automatically take a backup of the current database immediately before the regression. Thus you can freely "regress the regression" if required. Regressions and snapshots which are identical to the current working copy are highlighted in yellow.

You can save all of your backups and snapshots to an external USB drive.   Insert the USB drive into the USB slot on the rear of the appliance and click Backup/Regress.   An additional "save to disk" button will appear (see the image above). Clicking on the button will save all of your snaps and backups into a pair of time-stamped tar files on the USB drive.   You can now remove your backup and store it in a safe place.

Global Settings

The Global Settings Web page allows you to configure global PBX settings. In the left navigation menu, click Global Settings. The following Web page appears.

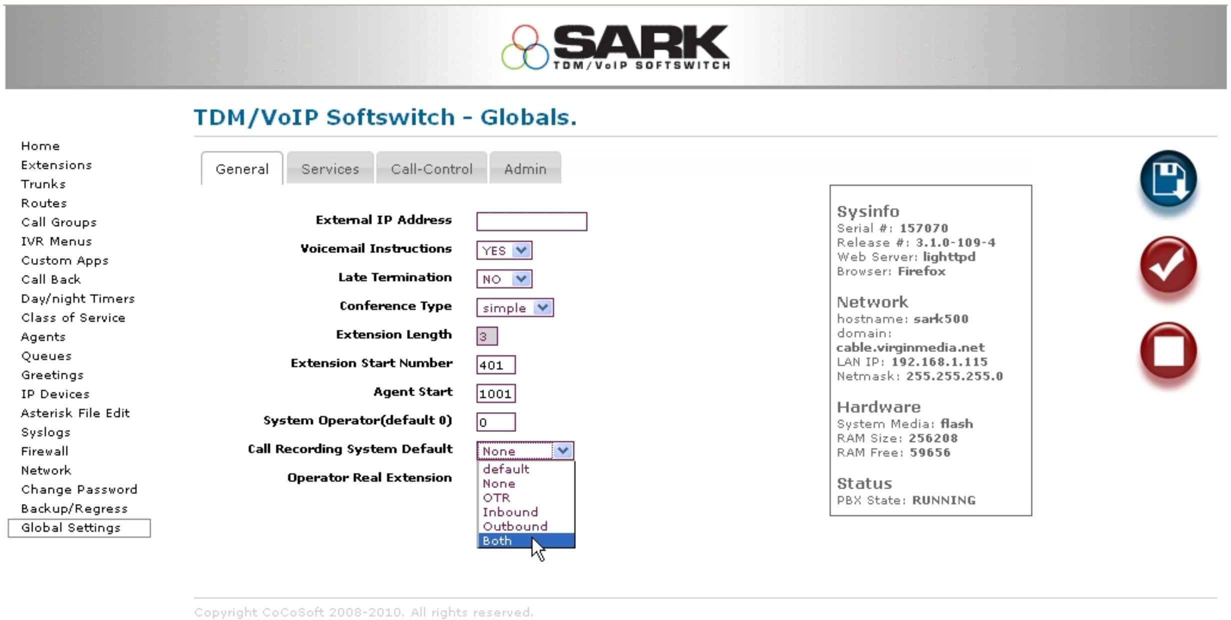


You can click through the various tabs to set the system up to your requirements.

Call Recording

SARK has several different settings for call recording which you can choose to suit your requirements. However, before you begin call recording, you should be aware that in most countries and jurisdictions there are legal implications whenever you record a call and that neither Aelintra Telecom nor its distributors or resellers will be responsible in the event that you use the recording features in an unlawful manner. If you are in any doubt regarding the legality of your proposed recordings then you should seek legal advice *before* you begin.

You can specify the default type of call recording you want to make at the system level and you can override this setting for each individual endpoint. The system setting is in the *Globals* panel under the *General* tab.



Whatever you choose in this section will be inherited by any endpoint which has its call recording preferences set to *default*. You can also override this directive by visiting the edit panel for an endpoint and setting its preference to some value other than *default*.

Recording process

All voice capture is done directly to /var/spool/asterisk/monitor. Immediately after a recorded call ends, a task is called to off-load the recording from *monitor* to a staging dataset (MONITOROUT). The default is /var/spool/asterisk/monout and you can use a cron updater to move the recordings over the network if required. Recordings are named as follows:-

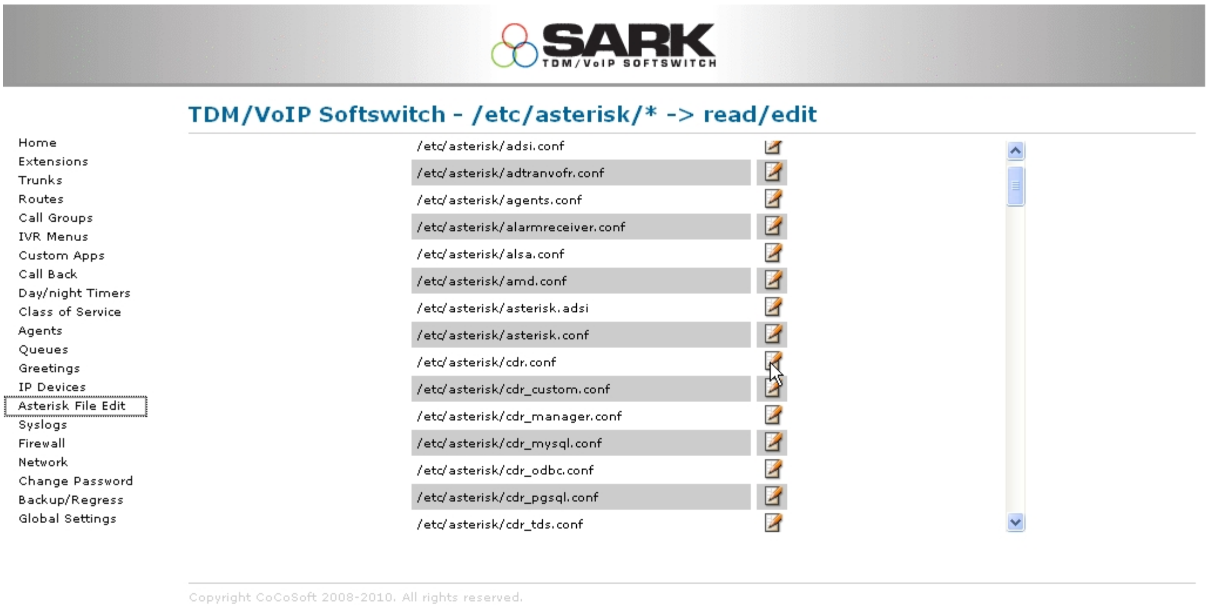
> ***{Linux Epoch}-{DNID}-{CLID}.wav***

An example calling from extension 5099 to a test number; 01924 566170, looks like this

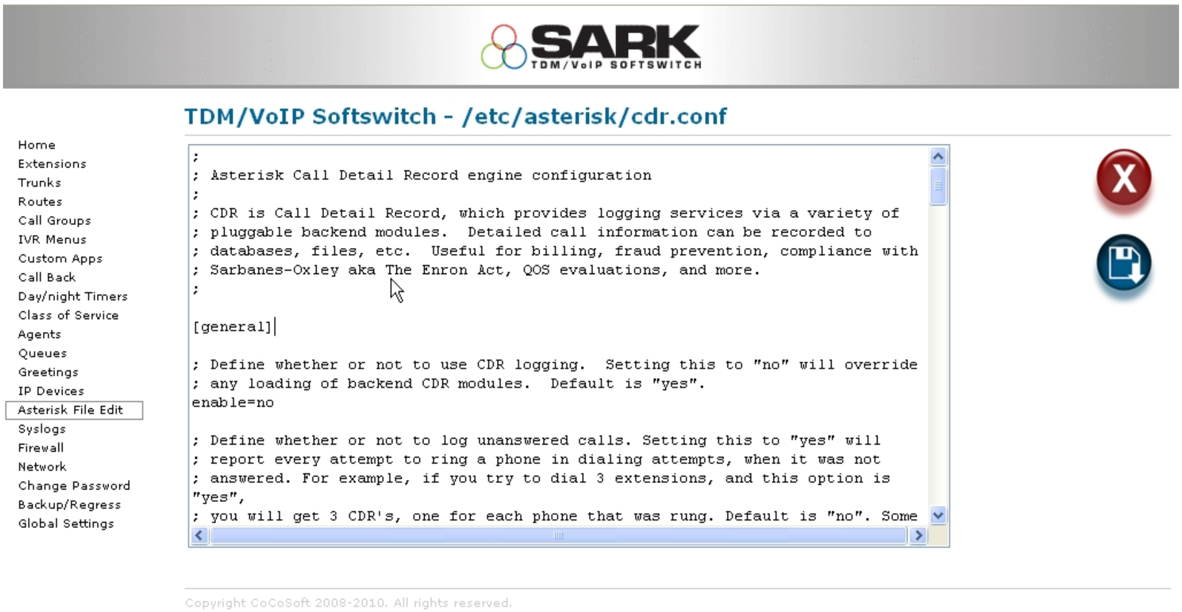
> ***1263728106-01924566170-5099.wav***

Asterisk File Edit

You can freely modify most of the Asterisk ".conf" files to suit your needs. There are a some files which SARK maintains and it won't allow you to modify them directly but even those files have user include files that you can use to create and maintain your own settings. To change an Asterisk file simply select it using the Asterisk file edit panel.

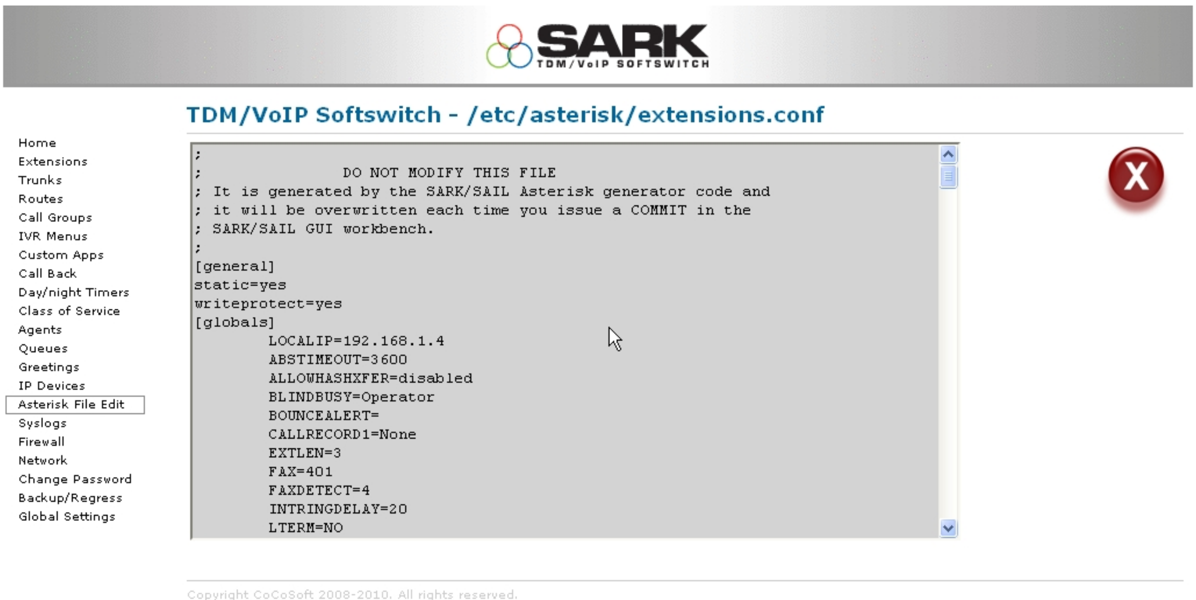


In the above example we have chosen to edit the Asterisk cdr.conf control file...



We can now freely edit the file and save our changes by clicking the save button. If it is a change which requires an Asterisk restart then Asterisk can be stopped and started from the Global Settings panel.

If you choose a file that SARK maintains, then the content will still be viewable but it will be "grayed out" and you won't be able to save or update it. One of the files which SARK manages is called extensions.conf...



As you can see from the above, when you display a system managed file, the "Save" button is not presented and the content is set to read-only.

SARK Service Codes

TRANSFERS, PARKING & GROUP PICKUP				
Key	**data**	**function**	**Availability/Terminal Type**	**Comment**
# #	extension	Blind Transfer	internal	Immediately transfer a call - use with analogue phones - usually turned off
*1	none	One Touch Record(OTR) or One Touch Retrospective Record(OTRR)*	internal	Activates call recording This is an in-band request. Actual key sequence may vary - refer to site administrator
*2#	extension	Attended Transfer	internal	Dial callee then transfer - use with analogue phones - usually turned off
Transfer Key	extension	Transfer	All SIP phones	Either blind or attended depending upon the phone type
*##*5#*	none	Call Park	internal	Parks the call into the first free park - usually used with BLF parks
*8	none	Call Pickup	internal	Pick up ringing call on same group
*8	extension	Directed Call Pickup	internal	Pick up specific ringing call - usually used with BLF and Visual Call Pickup on Snom or Aastra
Hold	none	Hold	SIP phones which have a hold function or key	Hold call and play MOH
*Message Light/Mail Icon *50**	none	Pick up voicemail	internal	Connect to Voicemail
300 - 307	none	Conference Rooms	internal	Actual key sequence may vary depending upon extension number choice and other factors

499	none	Broadcast directly to the overhead page amps using line out	internal	Check with your administrator to see if this feature is activated – Actual key sequence may vary depending upon extension number choice
700 - 702	none	Parked call pickup	internal	Actual key range may vary depending upon extension number choice- refer to site administrator
* +*extension*	none	dial or transfer to an extension's Voicemail	internal	Useful to transfer a call direct to an extension's voicemail box.
**+ *extension*	none	dial or transfer to an extension's MiniQueue (camp-on)	internal	Used to transfer a call to a busy extensions “camp-on” queue.

*OTRR Requires Advanced recording feature to be installed.

Diverts

DIVERTS				
Key	data	function	Availability/Terminal Type	Comment
20	none	Call Forward Immediate to Voicemail Toggle (DND)	internal	sets feature on/off
21+ext	none or extension	Call Forward Immediate (CFIM) Toggle	internal	Use with no extension to turn off
22+ext	none or extension	Call Forward on Busy/No Answer (CFBS) Toggle	internal	Use with no extension to turn off
23	none	Clear All Call Forward Instructions (CLACF)	internal	clear all call forward instructions for this extension
27+ext	extension	Follow Me (RCFIM)	internal	Direct a remote extension's calls to the local station - requests your vmail passwd
12+ext	extension	Temporarily forward operator calls to this extension	master user	Useful in small office environments during operator rest/break periods

Permissions

PERMISSIONS				
Key	data	function	Availability/Terminal Type	Comment
24	none	Allow Call Forward to External Numbers	master user - requires password	
25	none	Deny Call Forward to External Numbers	master user - requires password	
30	none	Set Master Timers to Automatic (default)	master user - requires password	Incoming calls will be checked against time of day
31	none	Set Master Timers to global "CLOSED"	master user - requires password	Incoming calls will be routed to closed handler
32	none	Set Master Timers to global "OPEN"	master user - requires password	Incoming calls will be routed to open handler

Voicemail

VOICEMAIL				
Key	data	function	Availability/Terminal Type	Comment
50	password	Local Voicemail	internal	connect to voicemail from own station
51	Extension & password	Remote Voicemail	internal/external	Connect to voicemail from another station

Miscellaneous operations

Miscellaneous				
Key	data	function	Availability/Terminal Type	Comment
26+n	none or ring delay	Set ring delay (seconds)	internal	if no ring delay is specified the ring will not timeout
40+group	none, pagegroup (call group) or extension	Page	internal	Use with no extension to page all phones
52	none	Echo test	internal/external	
55	none	Time and date	internal	
56	none	Check my extension number	internal	

System Greetings

System Greetings				
Key	data	function	Availability/Terminal Type	Comment
60+greet	4-digit greeting number	Record a system greeting	internal	Record a system greeting
61+greet	4-digit greeting number	Listen to a system greeting	internal	

Agents and Queues

Agents/Queues				
Key	**data**	**function**	**Availability/Terminal Type**	**Comment**
65	Agent Number/Password	Log on as an agent	internal	
66	Agent Number/Password followed by #	Log off as an agent	internal	
67	Agent Number	ChanSpy Function	master user - requires password	Allows a supervisor to anonymously listen to agents servicing Queues
68	extension	ChanSpy Function	master user - requires password	Allows a supervisor to anonymously listen to an extension

NANP Supported Service Codes

Key	data	function	Availability/Terminal Type	Comment
*60	none	Time and date	internal	
*65	none	Check my extension number	internal	
*72	Extension	Call Forward Immediate (CFIM)	internal	
*73	none	Cancel Call Forward Immediate (CFIM)	internal	
*78	none	DND ON	internal	
*79	None	DND OFF		
*90	extension	Call Forward on Busy/No Answer (CFBS)	internal	
*91	extension	Cancel Call Forward on Busy/No Answer (CFBS)	internal	
*97	password	Local Voicemail	internal	connect to voicemail from own station
*98	extension/password	Remote Voicemail	internal/external	Connect to voicemail from another station
*99	Greeting Number	Listen to a greeting	internal	