Mitel RFP 12 Single Cell DECT

VOIP SYSTEM GUIDE

Release 1.0

VoIP System Guide
Release 1.0 - January

ABOUT THIS DOCUMENT

This document describes the configuration, customization, management, operation, maintenance and trouble shooting of the Mitel RFP 12 Single Cell DECT system (Mitel 112 DECT handset, base station, and repeaters).

AUDIENCE

This guide is intended for

- networking professionals responsible for designing and implementing the wireless networks, and
- network administrators and IT support personnel that need to install, configure, maintain and monitor components of the system.

WHEN SHOULD I READ THIS GUIDE

Read this guide before you install the system components and when you are ready to setup or configure SIP server, NAT aware router, advanced VLAN settings, base stations, and multi-cell setup. This guide describes how to deploy a fully functionally system.

IMPORTANT ASSUMPTIONS

This document was written with the following assumptions:

1. You have understanding of network deployment in general.
2. You have working knowledge of basic TCP/IP/SIP protocols, Network Address Translation, and so forth.
3. A proper site survey has been performed, and the administrator has access to the plans.

CONTENTS OF THIS GUIDE

The contents of this document are summarized in the table below:

SECTION	PURPOSE
System Overview	Describes the different elements in a typical VoIP Network
Make Handset Ready	Provides instructions on how to assemble handsets for use in the system
Install Base Station/Repeater	Provides instructions for installing base units and repeaters
Configure Communication Platform	Provides an overview of the configuration required on the MiVoice Business or MiVoice Office 250 platforms to support the handsets.
Configure VoIP System	Lists steps required to configure the system
VoIP Administration Interface	Describes the configuration interface and defines the parameters that are used to set up the system.
Firmware Upgrades	Provides the procedure of how to upgrade firmware to base stations and/or handsets and/or repeaters
Functionality Overview	Describes system functionality and features.
Basic Network Servers Configuration	Describes how to set up network servers.
VLAN Setup Management	Explains how to set up VLAN in the network
Local Central Directory File Handling	Describes the central directory file format and provides instructions on how to upload it.

ABBREVIATIONS

For the purpose of this document, the following abbreviations apply:

DHCP:	Dynamic Host Configuration Protocol
DNS:	Domain Name Server
HTTP(S):	Hyper Text Transfer Protocol (Secure)
(T)FTP:	(Trivial) File Transfer Protocol
IOS:	Internetworking Operating System
IPEI	International Portable Equipment Identity
PCMA:	A-law Pulse Code Modulation
PCMU:	mu-law Pulse Code Modulation
PoE:	Power over Ethernet

RTP:	Real-time Transport Protocol
RPORT:	Response Port (Refer to RFC3581 for details)
SIP:	Session Initiation Protocol
VLAN:	Virtual Local Access Network
TOS:	Type of Service (policy based routing)
URL:	Uniform Resource Locator
UA:	User Agent

REFERENCES/RELATED DOCUMENTATION

[1]: **112 DECT Phone (Universal) and RFP 12 Single Cell Base Station Installation Guide (part number 57011091):** provides instructions on how to make the required cable and power connections for the base station and charging cradle. It also provides instructions for installing the handset batteries.

[2]: **Mitel 112 DECT Phone (Universal) User Guide**: describes the features and functionalities provided by the Mitel 112 DECT Phone

[3]: **112 DECT Phone Quick Reference Guide for MiVoice Business**: provides instructions on how to use the features of the handset when it is connected to a MiVoice Business communications platform.

[4]: **112 DECT Phone Quick Reference Guide for MiVoice Office 250**: provides instructions on how to use the features of the handset when it is connected to a MiVoice Office 250 communications platform.

[5]: **MiVoice Business System Administration Help:** Refer to this online help system for instructions on how to program

- Mitel 112 DECT Phone as a "SIP generic device type" on the MiVoice Business system
- Mitel 112 DECT Phones into personal ring groups
- Support for Suite Services.

[6]: **MiVoice Office 250 Features and Programming Guide and Database Programming Online Help:** provides instructions on how to program the Mitel 112 DECT phone as a "SIP Phone" on the MiVoice Office 250.

INTRODUCTION – SYSTEM OVERVIEW

The MITEL RFP 12 Single Cell DECT system is a VoIP solution with support for up to 20 registered handsets and three repeaters.

HARDWARE SETUP

The base-stations are mounted on walls or poles so that each base-station is separated from each other by up to 10 meters (for indoor installation). Radio coverage can be extended using repeaters. Repeaters are range extenders only and cannot be used to increase local capacity.

The base-station antenna mechanism is based on a space diversity feature which improves coverage. The base-stations use the complete DECT MAC protocol layer and IP media stream audio encoding feature to provide up to five simultaneous calls.

COMPONENTS OF MITEL RFP 12 SINGLE CELL DECT SYSTEM

The system is made up of (but not limited to) the following components:

- Mitel 112 DECT Phone and charging cradle.
- Base station connected over an IP network and using DECT as air-core interface
- Repeater (optional)
- VoIP Administration Interface

MITEL 112 DECT PHONE

The phone is a lightweight, ergonomically and portable handset compatible with Wideband Audio (G.722), DECT, GAP standard, CAT-iq audio compliant.

The handset includes a color display with graphical user interface. It can also provide the subscriber with most of the features available for a wired phone, in addition to its roaming and handover capabilities.

BASE STATION

The Base Station converts IP protocol to DECT protocol and transmits the traffic to and from the wireless handsets over a channel. The base station has five available channels.

REPEATER

The base supports the IP DECT CAT-IQ repeater RTX4024. A repeater can be deployed to extend the range of a DECT handset. The repeater can also be utilized wherever there is a need to increase limited coverage or improve reception in remote areas.

The RYX4024 provides the following features:

- Up to three repeaters are supported per base station
- Wide band audio

- DECT encryption
- Automatic registration
- Maximum of three repeaters in daisy chain.

VOIP ADMINISTRATION INTERFACE

The VoIP Configuration Interface is a web based administration that you use

- configure the base station and relevant network end-nodes. For example, handsets can be registered or de-registered from the system using this interface.
- install software or firmware downloads onto base stations, repeaters and handsets.
- access system logs that can be used to troubleshoot the system.

WIRELESS BANDS

The bands supported in the VoIP are summarized as follows:

Frequency bands: 1880 – 1930 MHz (DECT)
1880 – 1900 MHz (10 carriers) Europe/ETSI
1910 – 1930 MHz (10 carriers) LATAM
1920 – 1930 MHz (5 carriers) US

SYSTEM CAPACITY

The network capacity of relevant components can be summarized as follows:

DESCRIPTION	CAPACITY
Single Cell Setup	1
Maximum number of repeaters per base station	3
Maximum number of handsets (SIP registrations) per base station	20
Single Cell Setup: Maximum number of simultaneous calls	5
Repeater: Max number of calls (narrow band)	5
Repeater: Maximum number of calls (G.722)	2

Note: Each base station supports up to 20 handsets and three repeaters.

MAKE HANDSET READY

This section describes how to prepare the handset for use.

PACKAGE INSPECTION

Before you open the package, examine it for evidence of physical damage or mishandling. If the package appears damaged, report it to the relevant support centre of the regional representative or operator.

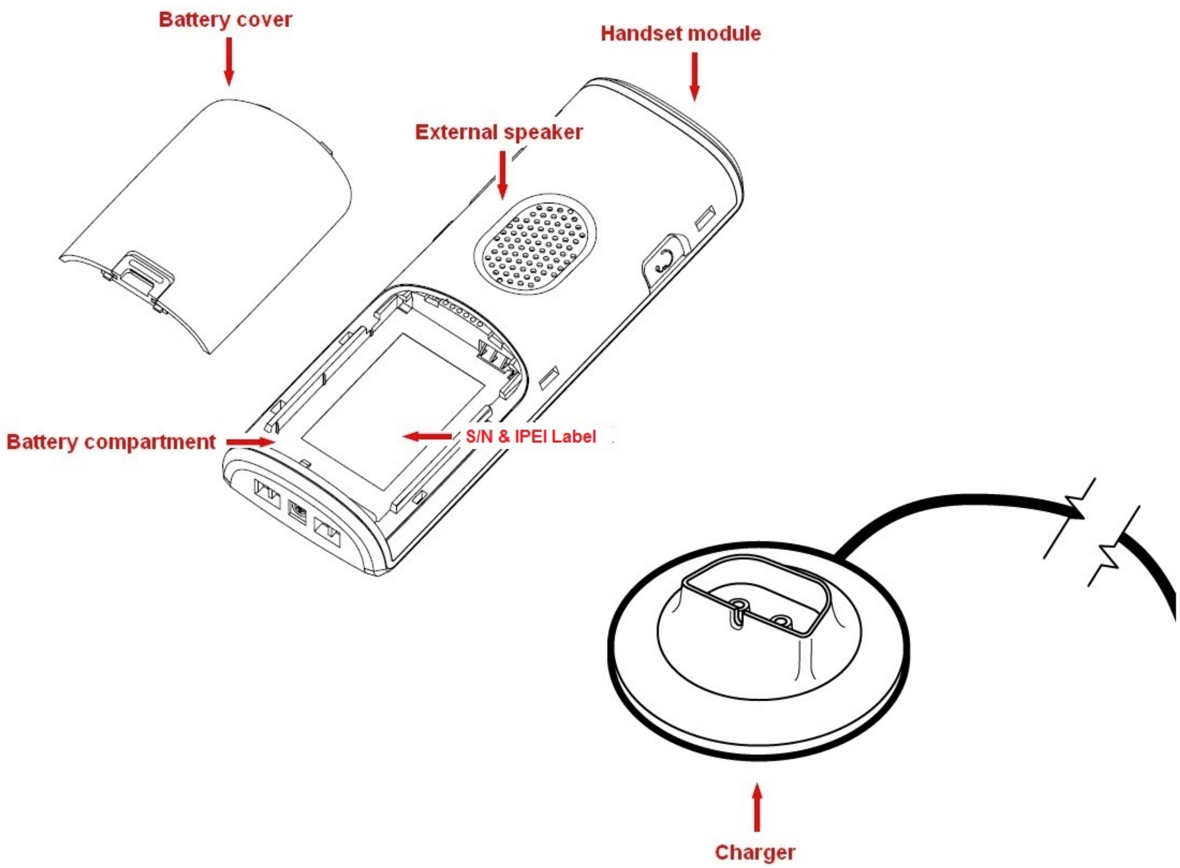
The following are the recommended procedure for you to use for inspection:

1. Examine all relevant components for damage.
2. If damage is detected, make a “defective on arrival – DOA” report to Mitel Customer Service. The Mitel Customer Service representative will initiate the necessary procedure to process the return. They will guide the network administrator on how to return the damaged package if necessary.
3. If no damage is found then unwrap all the components and dispose of empty package/carton(s) in accordance with country specific environmental regulations.

CONTENTS

Ensure that the following components where provided in the handset package before proceeding with the installation:

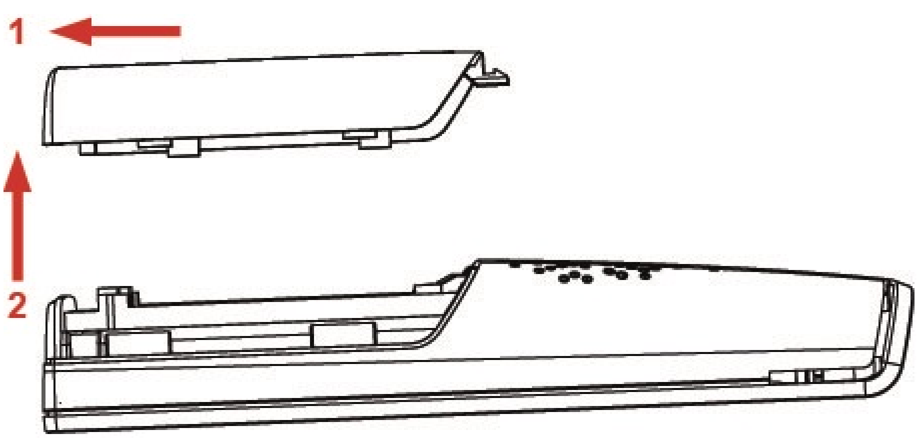
- 1 x handset and battery cover
- 2 AAA batteries
- 1 x charging cradle with wired A/C adapter



BEFORE USING THE PHONE

OPEN BACK COVER

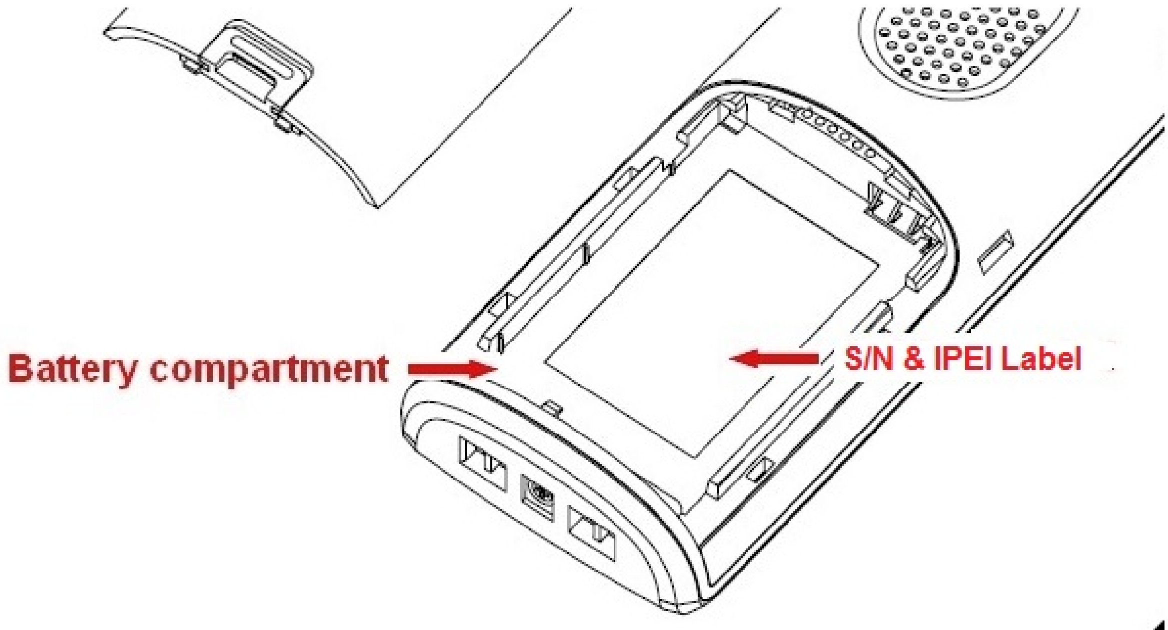
1. Press down the back cover and slide it towards the bottom of the handset.
2. Remove back cover from handset.



RECORD HANDSET SERIAL NUMBER (IPEI NUMBER)

The International Portable Equipment Identity (IPEI) of each handset is printed either on a label located behind the battery or on the packaging label. Remove the handset back cover, take out the battery (if installed) and record the IPEI number.

You need this number to enable service to the handset. You must program it into the system database via the VoIP Administration interface.



INSTALL THE BATTERY

1. Never dispose of a battery in a fire; otherwise it will explode.
2. Never replace the batteries in potentially explosive environments, for example close to flammable liquids or gases.
3. ONLY use approved batteries and chargers from the vendor or operator.
4. Do not disassemble, customize, or short circuit the battery.

CHARGE THE BATTERY

Each handset is charged using a handset charger. The charger is a compact desktop unit that automatically maintains the correct battery charge levels and voltage.

The handset charger is powered by AC power adapter that supplies 5VDC at 1000mA. The AC power adapter is supplied from 110-240 VAC.

When charging the batteries for the first time, it is necessary to leave the handset in the charger for at least 10 hours before they are fully charged and the handset is ready for use.

For correct charging, ensure that the room temperature is between 0°C and 25°C (32°F and 77°F). Do not place the handset in direct sunlight.

The battery displayed in the top right of the screen indicates the charging status.

USING THE HANDSET

For instructions on how to use the handset features, refer to the Mitel 112 DECT Phone (Universal) User Guide available on the Mitel Customer Documentation site.

INSTALL BASE STATION/REPEATER

The following sections how to install the base station.

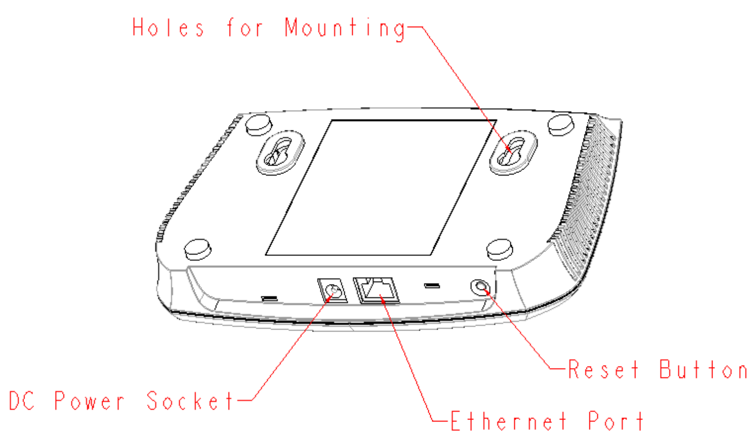
PACKAGE INSPECTION

Before you open the package, examine it for evidence of physical damage or mishandling. If the package appears damaged, report it to the relevant support centre of the regional representative or operator.

PACKAGE CONTENTS

Ensure that the following components where provided in the base unit package before proceeding with the installation:

- 2 x mounting screws and 2 x Anchors
- 1 x Category 5 cable (Ethernet cable)
- Base unit
- Power supply adapter



Back View of Base Station Unit

BASE STATION MECHANICS

The base station front panel has an LED indicator that signals the different functional states of the base unit and occasionally of the overall network. The indicator is off when the base unit is not powered. The table below summarizes the various LED states:

LED STATE	STATUS
OFF	No power
FLASHING GREEN	Initialization in progress
SOLID GREEN	Ethernet connection is available (Normal operation)
FLASHING ORANGE	No IP address
SOLID ORANGE	Reset required
FLASHING RED	Factory setting in progress OR Ethernet connection not available OR Handset registration/deregistration failed.
SOLID RED	Factory reset warning after a long press (10 seconds or more) of the Reset button OR Error condition. Replace base station if error condition persists.

BASE STATION – RESET FEATURE

To reset the base station unit, press the small Reset button on the back of the unit. You can also reset the base station from the VoIP Administration Interface.

INSTALLING THE BASE STATION

1. Record the MAC address of the base station. The MAC address is listed on the bottom panel of the base.
2. Determine the best location that will provide an optimal coverage taking account the construction of the building, architecture, and building materials.
3. Mount the base station on a wall to cover a range of 50 meters (164 feet) for indoor installations or 300 meters (984 feet) for outdoor installations. We recommend the base station be mounted an angle on concrete, wood, or plaster pillars and walls for optimal radio coverage. Do not mount the base units upside down because it significantly reduces radio coverage.
4. Mount the base unit as high as possible to clear all nearby objects (for example: office cubicles and cabinets). If necessary, extend coverage to remote offices or halls with fewer telephony users by installing repeaters.
5. When you fasten the base stations to the pillar or wall, ensure that the screws do not touch the PC board in the unit. Secondly, avoid all contact with any high voltage lines.

DETERMINE IP ADDRESS OF BASE STATION

To identify the IP address of the base station:

1. On the handset press the round “Menu” button to access the main menu:

2. Dial ***47***. “Searching” is displayed. Depending on the number of active base stations and the distance to the base it can take up to 5 minutes to find a base.
3. If there are multiple base stations available, use the down/up cursor to select the MAC address of the desired base. The base IP address is displayed.
4. Record the IP address.
5. Configure 112 DECT Phone on Communication Platform.

CONFIGURE COMMUNICATIONS PLATFORM

PROGRAM MIVOICE BUSINESS PHONES

Before you register the handset with the base station, complete the following MiVoice Business programming tasks. Refer to the MiVoice Business System Administration Tool online help for instructions:

1. License the Mitel 112 DECT Phone (handset) as a SIP device.
2. Program a user and handset extension in the “User and Services Configuration” form as a “Generic SIP Phone”.
3. Access the SIP Device Capabilities form. Program a SIP Device Capabilities index number using the standard defaults with the exception of the following options. In the SIP Device Capabilities form tabs, set the following options to **Yes**.
   - Replace System based with Device based In-Call Features
   - Enable Digit Collection In Busy Or Alerting State
   - Allow Display Updates
   - Enable Distinctive Ringing
   - Prevent the Use of IP Address 0.0.0.0 in SDP Messages.
4. Use the Search field in the “User and Device Configuration” form to locate the directory numbers that will be assigned to the handsets. Click the **Service Details** tab and assign the SIP Device Capabilities index number to each handset.

5. In the “Multiline Set Keys” form of the MiVoice Business System Administration tool, configure the handset with a second multi-call appearance of the prime line with the Ring Type set to “Ring”. Refer to the System Administration Tool online help for instructions.
6. You can optionally configure a

   - Mitel desktop phone and a handset in a Personal Ring Group, or
   - Mitel desktop phone and a handset for Suite Services (typically, used in a hospitality environment).

CONFIGURE A PRG WITH CALL HANDOFF (OPTIONAL)

Personal Ring Groups (PRGs) allow you to associate two or more devices for a single user under a common, prime directory number (DN). The devices ring simultaneously (Ring All) when the prime directory number is called. You can use PRGs to twin a person's desktop phone and his or her Mitel 112 DECT Phone together. The desk phone is considered the prime extension, which is referred to as the pilot number or prime member of the group. The cordless handset is programmed as a non-prime member of the group.

You can also program and label a **Handoff** key on the user’s desk phone. Users can press the **Handoff** feature key to

- push a call that is in progress from their desktop phone to their Mitel 112 DECT Phone, or
- pull a call that is in progress from their Mitel 112 DECT Phone to their desktop phone.

The **Handoff** key is only supported on Mitel desktop phones. It is not supported on SIP devices and you cannot program it on a Mitel 112 DECT Phone.

Refer to the “Ring Groups Personal” and “Handoff (Personal Ring Groups)” topics in the “Features” book of the MiVoice Business System Administration Tool online help for programming instructions.

CONFIGURE FOR SUITE SERVICES (OPTIONAL)

Suite Service provides the ability to group a number of telephone lines through interconnected hotel/motel rooms, or suites, for the purposes of billing and shared telephone service. Refer to the following online book in the MiVoice Business System Administration Tool online help for a detailed description of Suite Services and programming instructions: System Applications > Hospitality > Suite Services.

MIVOICE OFFICE 250 SIP PHONE PROGRAMMING

Before you register a handset with base station, complete the following MiVoice Office 250 Database Programming tasks. Refer to the *MiVoice Office 250 Features and Programming Guide* and *Database Programming online help* for detailed instructions:

1. Ensure that you have a valid Category F license available for each handset that will be connected to the base station.
2. Program each handset as a “SIP Phone” (or part of a SIP Phone Group).

CONFIGURE DYNAMIC EXTENSION EXPRESS (OPTIONAL)

Dynamic Extension Express (DEE) allows you to associate two or more devices for a single user under a common main extension number. You can use DEE to “twin” a person's desktop phone and his or her handset together. The desk phone is considered the main extension, while the cordless handset is programmed as a secondary destination.

You can also program and label a DEE Handoff key (default feature code is 388) on the user’s desk phone. Users can press the DEE Handoff feature key to push a call that is in progress from their desk phone to their handset.

For programming instructions, refer to the DEE topics in the latest *MiVoice Office 250 Features and Programming Guide* and *Database Programming Online Help*.

CONFIGURE VOIP SYSTEM

This section describes basic configuration of the system. See VoIP Administration Interface on page 26 for descriptions of the system parameter settings.

LOGIN TO VOIP SYSTEM ADMINISTRATION INTERFACE

1. Connect the base station to a private network via standard Ethernet cable (CAT-5).

2. Use the IP Search function on the handset to determine the IP address of the base station:

- Press the center Menu button on the handset to access the main menu:

- Dial **∗47∗**. “Searching” is displayed. Depending on the number of active base stations and the distance to the base it can take up to 5 minutes to find a base.

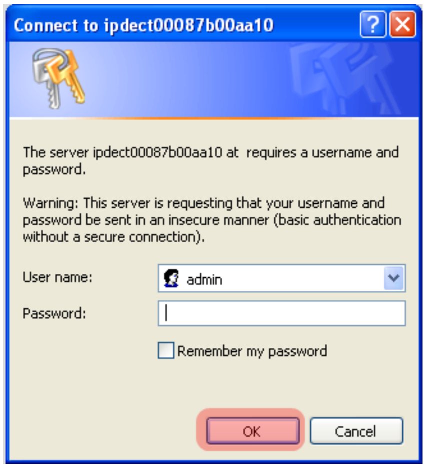
- If multiple base stations are available, use the up/down Menu button to highlight the MAC address of the desired base. Press **Select**. The base IP address is displayed.

- Record the IP address.

3. Open a standard internet browser (for example, FireFox)

4. In the browser address bar enter http//<IP Address of Base Station>.
Username: **admin** (default)
Password: **admin** (default)

5. Click **OK**.



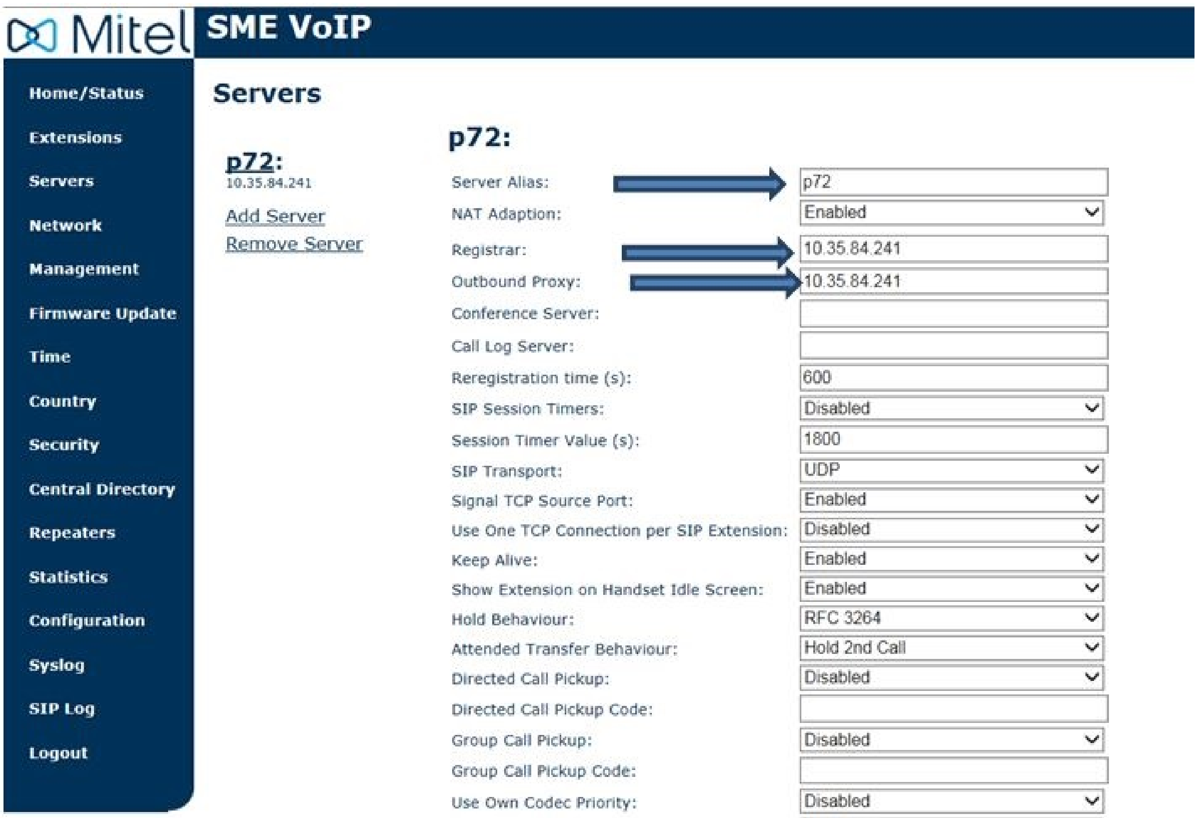
6. The browser displays the Welcome page of the VoIP Administration interface. It lists the base station information.

CONFIGURE SYSTEM PARAMETERS

From the VoIP Administration interface, perform the following configuration:

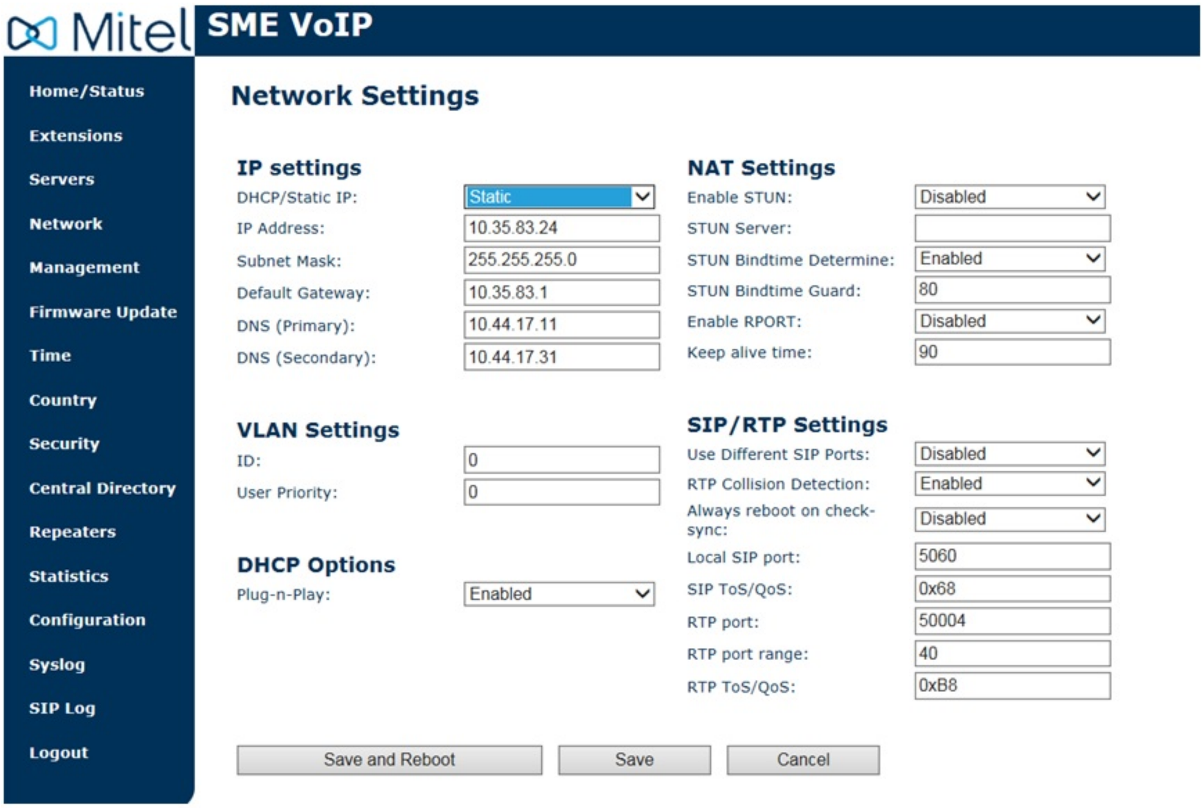
1. Click **Servers**.

    - Enter the name of the MiVoice communications platform in the “Server Alias” field.
    - Enter the IP address of the MiVoice communications platform in the “Registrar” and “Outbound Proxy” fields.
    - Click **Save**.



2. Click **Network**:

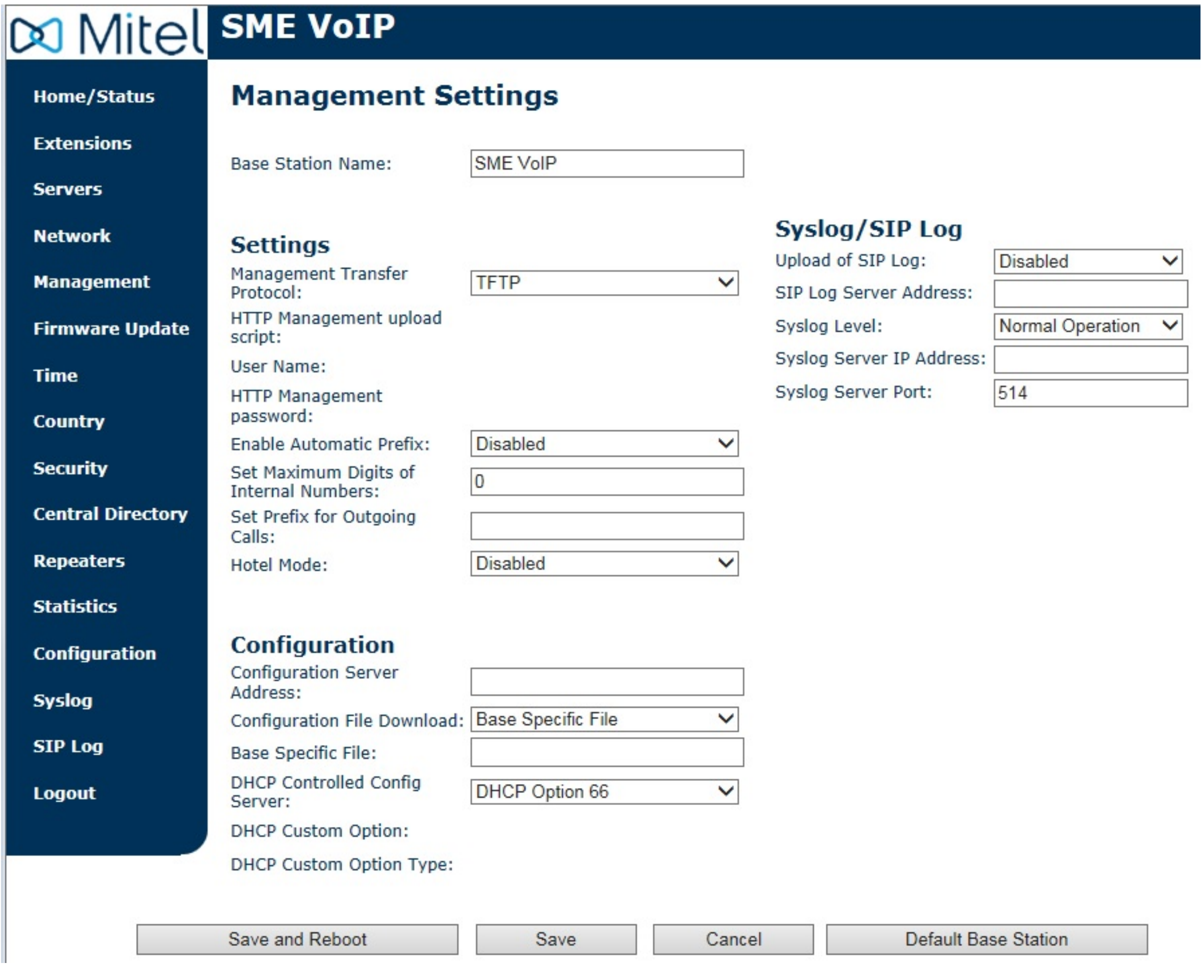
- Set **DHCP/Static** field to “Static” (recommended).
- Enter the IP address of the base station.
- Enter the IP address of the Default Gateway (if required).
- Click **Save**.



3. Click **Management**.

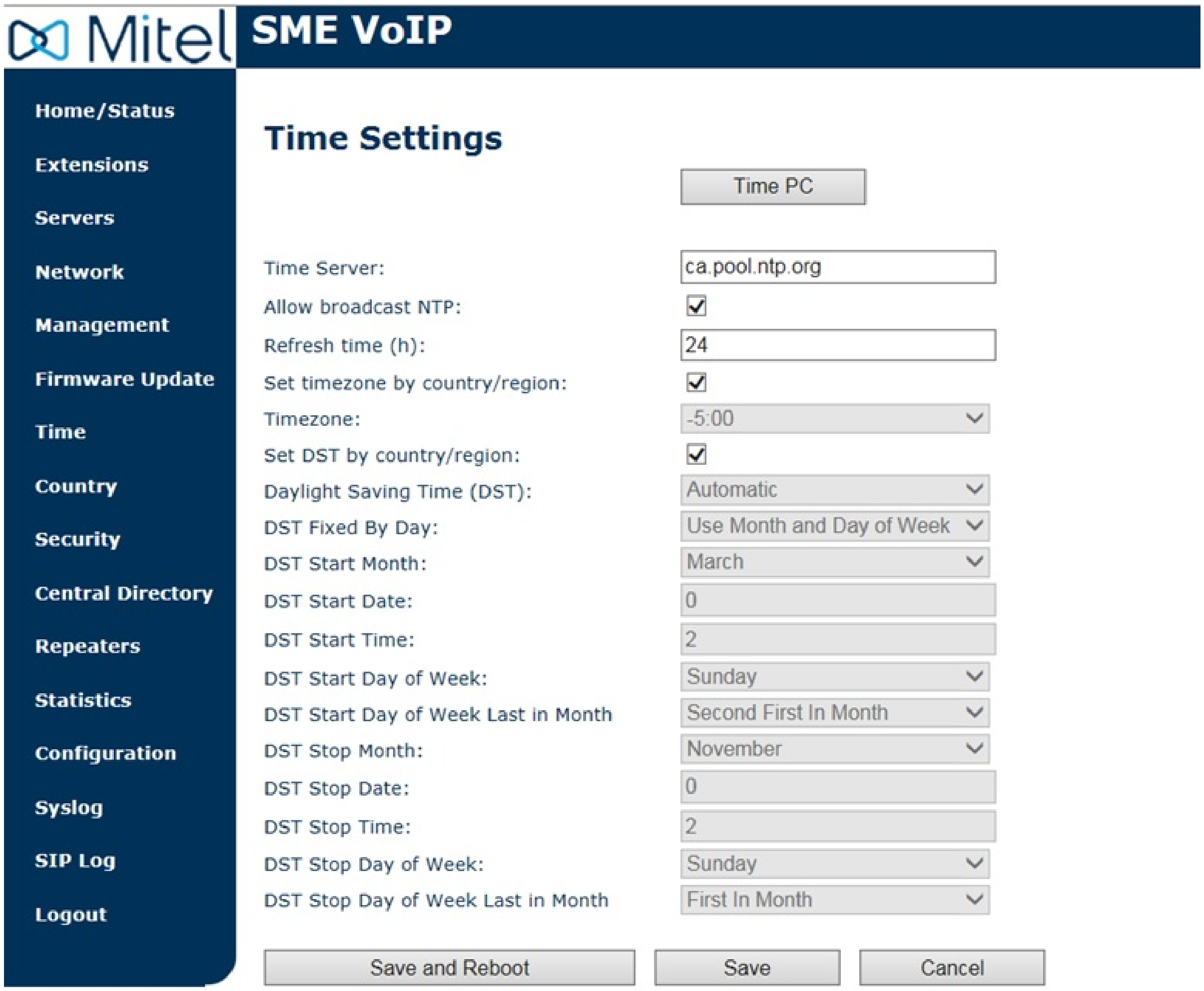
- If you are deploying the handsets in a hospitality (Hotel/Motel) environment, enable Hotel Mode. Note that when this option is enabled, it changes default handset PIN from 0000 to 9351 and the PIN is required to access the **Settings** menu.

- Click **Save**.



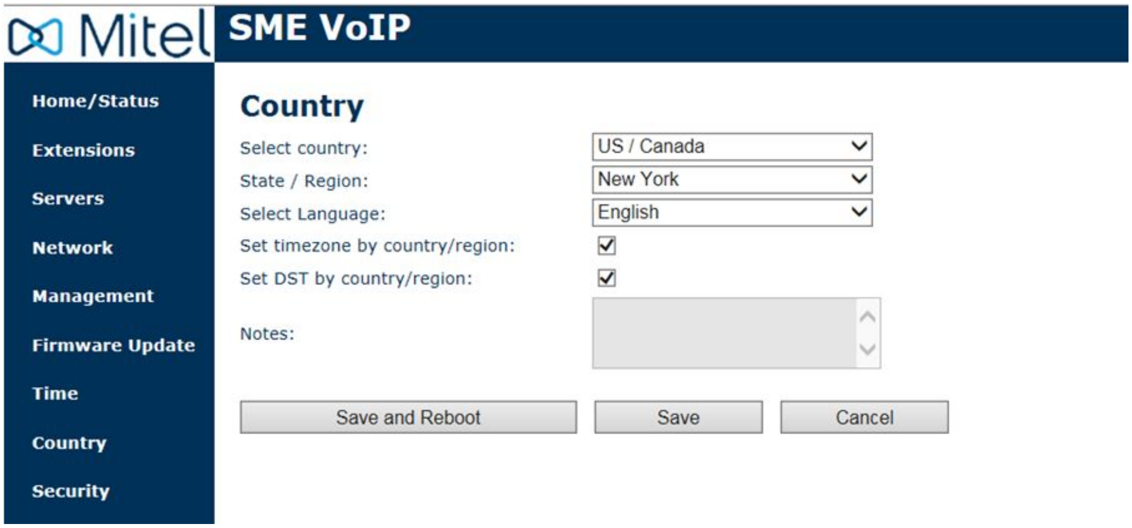
4. Click **Time**.

- Set the system time.
- Click **Save**.



5. Click **Country**.

- Set the country settings.
- Click **Save**.



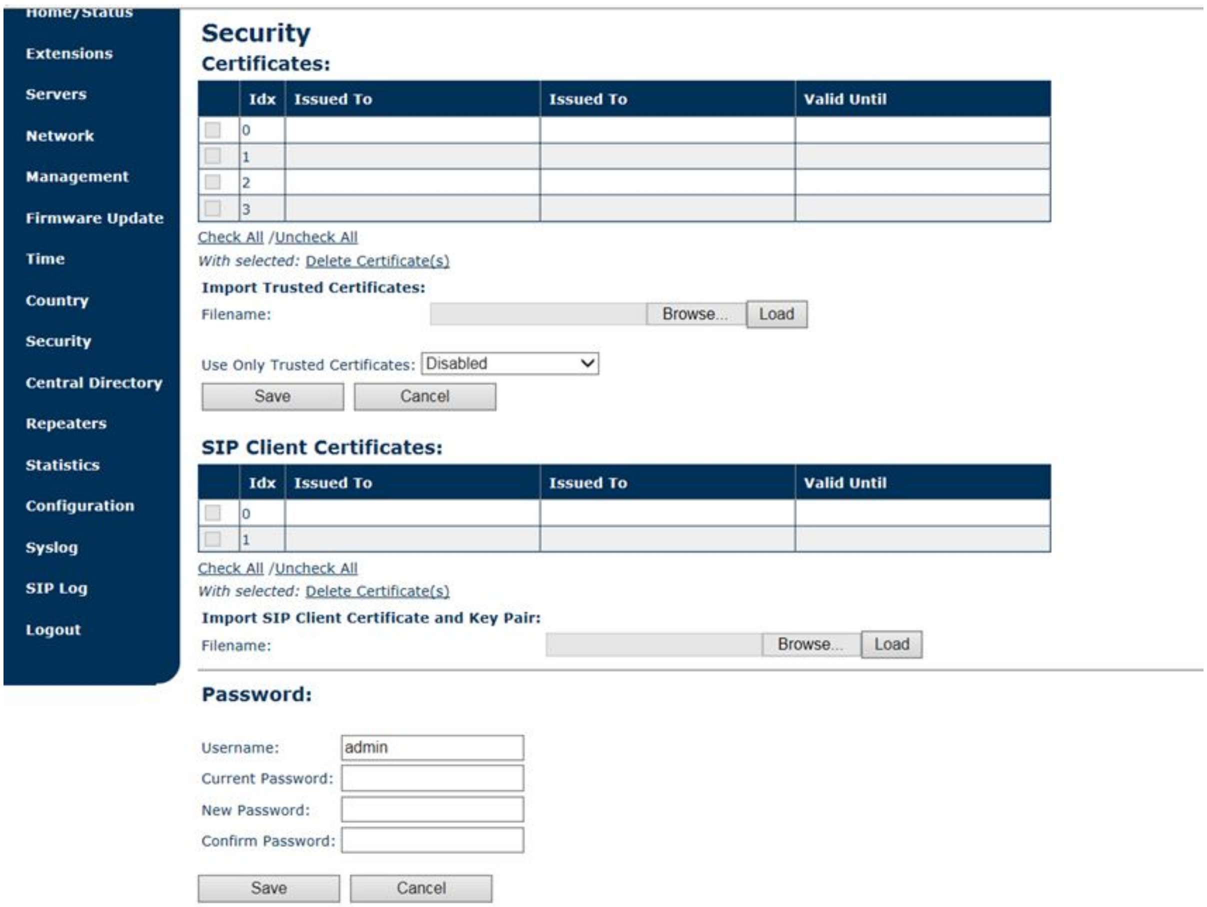
6. Click **Security**:

- Under **Password**, change the administrator password (default **admin**) used to access this interface.

  CAUTION: Ensure that you record the new password. If you forget the administrator password, you must reset the base station to the default configuration values and reconfigure the system.

- Click **Save**.

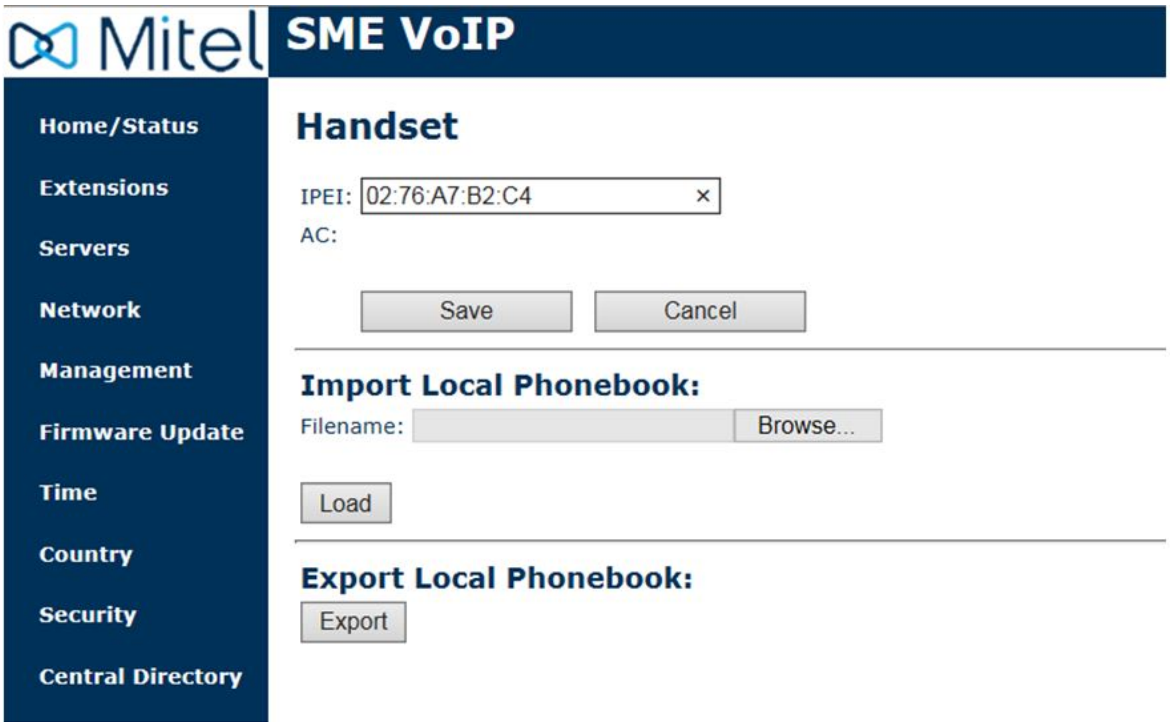
Note: You can reset the stand to the default configuration values (including the username and password) using the RESET button on the base station. Press and hold the RESET button for greater than 10 seconds to reset the base station configuration to the default values.



ADD HANDSETS AND EXTENSIONS

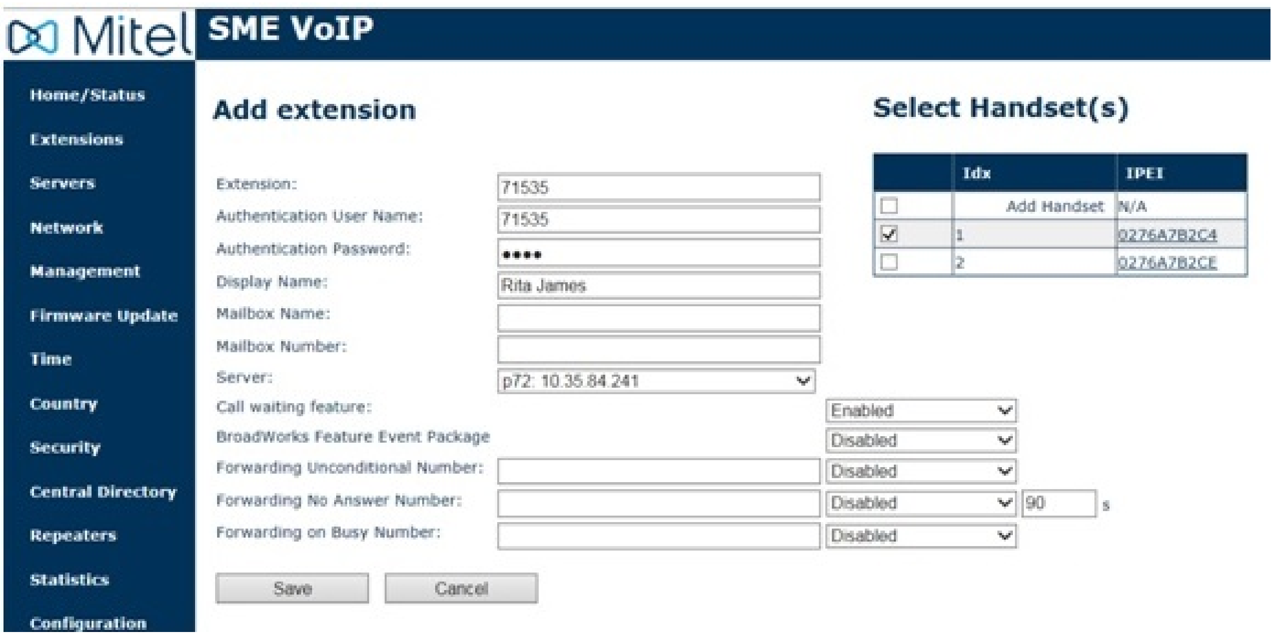
1. Click **Extensions** and add the handsets.

    - Click **Handset**.
    - Click **Add Handset**.
    - Enter the IEPI of the handset. The IEPI is printed on a label located under the handset batteries.
    - Click **Save**.



2. Click **Extensions** and add the extensions.

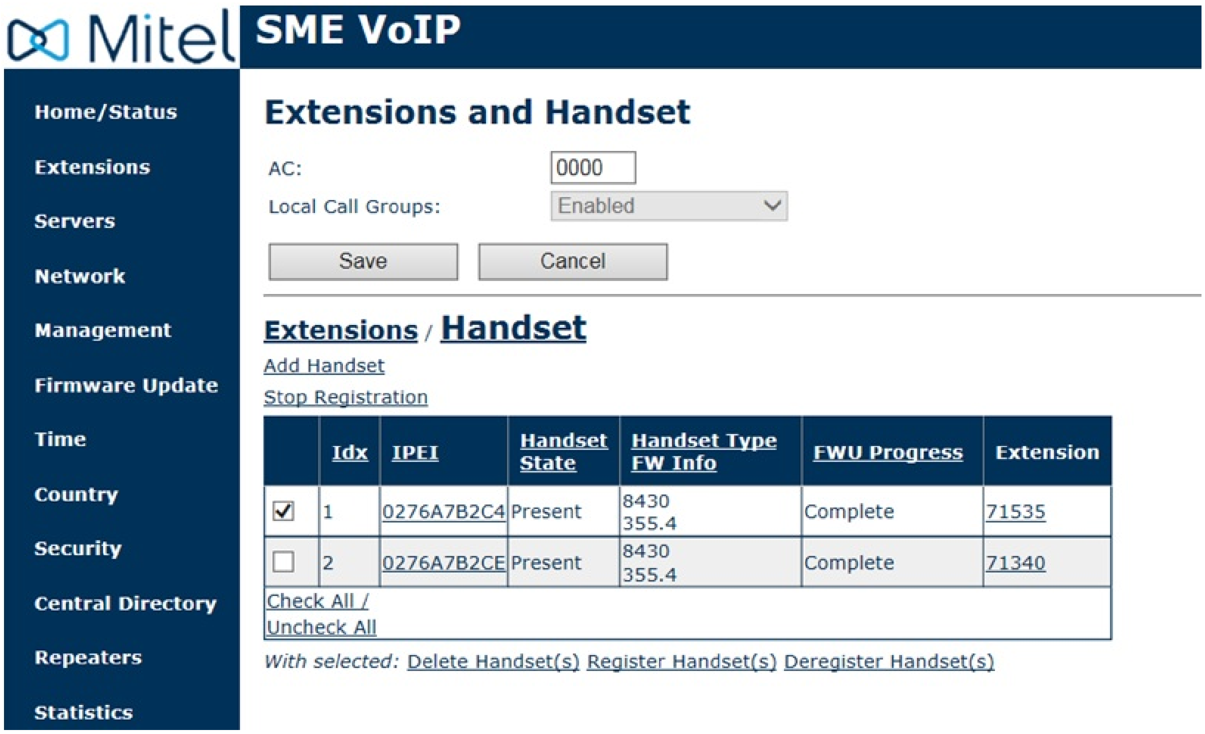
- Click **Add extension**
- Enter the Extension number.
- Enter the user's Display Name.
- Select the Server (MiVoice communications platform).
- Under **Select Handset(s)**, check the box to associate the extension with a handset.
- Click **Save**.



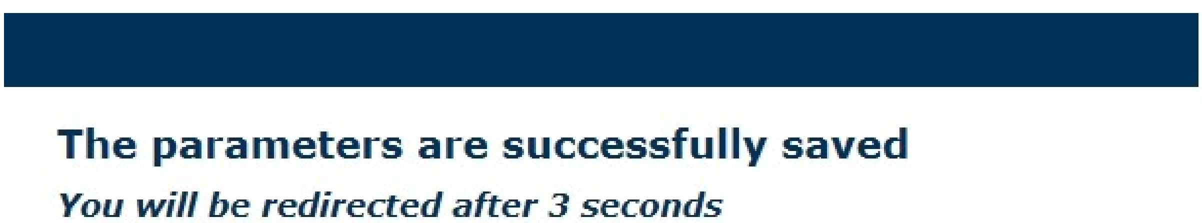
REGISTER THE HANDSETS

1. Open base station to handset registration:

- Click **Extensions**.
- Optionally, change the AC (Access code). You enter the AC on the handset to initiate registration.
- Check the boxes of the handsets that you want to register.
- Click Register Handset(s).



2. The parameters are saved.

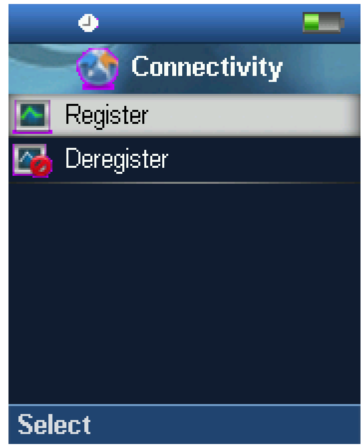


3. The base station is now open (in the ready state) for handset registration for the next 5 minutes. You must register the selected handsets with the base station using the following procedure in the next 5 minutes.

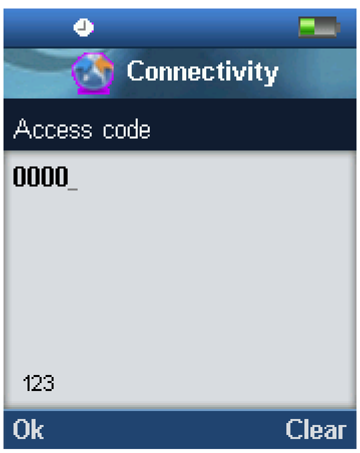
4. Next, register each handset with the base station. Start the registration procedure on the handset by following step “a” to “d” below.

a) Select main menu “Connectivity”

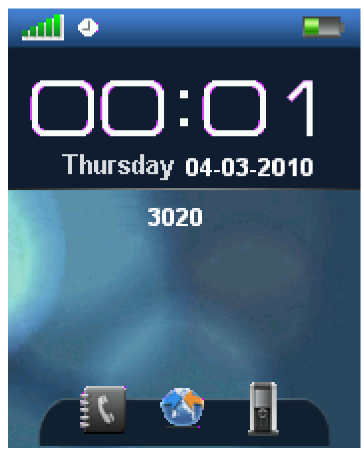
b) Select menu ”Register”



c) Type in the “AC code” and press “OK” to start the registration. The default AC code is “0000”.

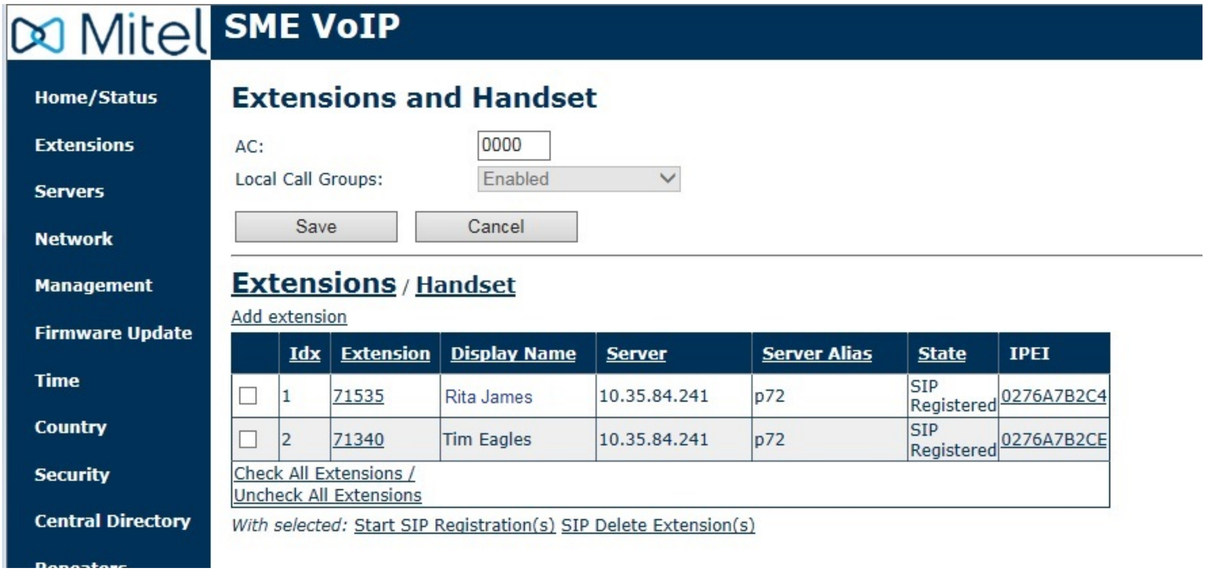


d) After a while the handset is registered, and the idle display is shown.



Note: The unique handset IPEI is displayed on sheet “Extensions” when the handset is successfully registered. The web page must be manually updated by pressing “F5” to see that the handset is registered; otherwise the handset IPEI (International Portable Equipment Identity) isn’t displayed on the web page.

5. The following screen shows an example of the Extensions page after you have registered several handsets.



6. Initial system configuration is now complete.

Note: After you have configured the handsets on a base station, ensure that you have changed the administration interface username and password, and the handset AC codes from the default values to prevent unauthorized access.

VOIP ADMINISTRATION INTERFACE

You manage and troubleshoot the system through the VoIP Administration Interface. The interface is an HTTP Web Server service that resides in each base station.

Note: Enabling secure web is not possible. For secure configuration use secure provisioning.

This section defines the variables and parameters for configuration in the network.

WEB NAVIGATION

This section describes the left menu of the VoIP Administration Interface.

WEB PAGE	DESCRIPTION
Home/Status	This "Welcome" page displays the system information and base station status.
Extensions	Manage the system handsets and extensions
Servers	Define which SIP/NAT server the network should connect to.
Network	Configure the Network settings: **NAT provisionin**g: allows configuration of features for resolving of the NAT – Network Address Translation. These features enable interoperability with most types of routers. **DHCP**: allows changes in protocol for getting a dynamic IP address. Virtual LAN: specifies the Virtual LAN ID and the User priority. **IP Mode**: specify either dynamic (DHCP) or static IP address for your network. Only complete the IP address if you using a static IP address, Otherwise, leave it blank. **Subnet mask**: Leave blank if using DHCP. Complete if assigning a static IP address. **DNS server**: Specify if using DHCP; otherwise, leave it blank. Enter the DNS server address of your Internet service provider. If you are using a static IP address the DNS = Dynamic Name Server. **Default gateway**: if using DHCP, leave it empty. Write in the IP address of your router, when you use static IP address.
Management	Defines the Configuration server address, Management transfer protocol, and the sizes of logs/traces that should be catalogued in the system.
Firmware Update	Remote firmware updates (HTTP(s)/TFTP) settings of base stations and handsets.
Time	Configures a time server for the system. Use a time server that applies to the country of installation. The time server must deliver the time in Network Time Protocol (NTP). The base station and handsets clocks are synchronized to the time server.
Country	Specify the country/territory where the network is located to ensure that your phone functions properly. **Note**: The base language and country setting are independent of each other.
Security	Allows users to administrate certificates and create account credentials with which they can log in or log out of the embedded HTTP web server.
Central Directory	Interface to a common directory. You can import up to 3000 entries using *csv format file or configure a connection to an LDAP directory.

WEB PAGE	DESCRIPTION
	Note: LDAP and central directory cannot operate at the same time.
Repeaters	Administration and configuration of repeaters of the system
Alarm	Administration and configuration of the alarm settings on the system. This controls the settings for alarms that can be sent to the handsets. This feature is only available on certain types of handsets.
Statistics	Overview of system and call statistics for a system.
Configuration	This shows detail and complete network settings for base station(s), HTTP/DNS/DHCP/TFTP server, SIP server, etc.
Syslog	Overall network related events or logs are displayed here (only live feed is shown).
SIP Log	SIP related logs can be retrieved from url link. It is also possible to clear logs from this feature.

HOME/STATUS

This section describes the Home/Status page.

PARAMETER	DESCRIPTION

System information	This base current multi-cell state
Phone Type	Always IPDECT
System Type	This base customer configuration
RF Band	This base RF band setting
Current local time	This base local time
Operation time	Time from last boot of base
RFPI-Address	This base RFPI address
MAC-Address	This base MAC address
IP-Address	This base IP address
Firmware version	This base firmware version
Firmware URL	Firmware update server address and firmware path on server
Base Station Status	"Idle" : When no calls on base "In use" : When active calls on base
SIP Identity Status on this Base Station	List of extensions present at this base station. Format: "extension"@"this base IP address" followed by status to the right. Below is listed possible status: OK: Handset is registered SIP Error: SIP registration error
Reboot	Reboot after all connections is stopped on base. Connections are active call, directory access, firmware update active
Forced Reboot	Reboot immediately even active calls are ongoing.

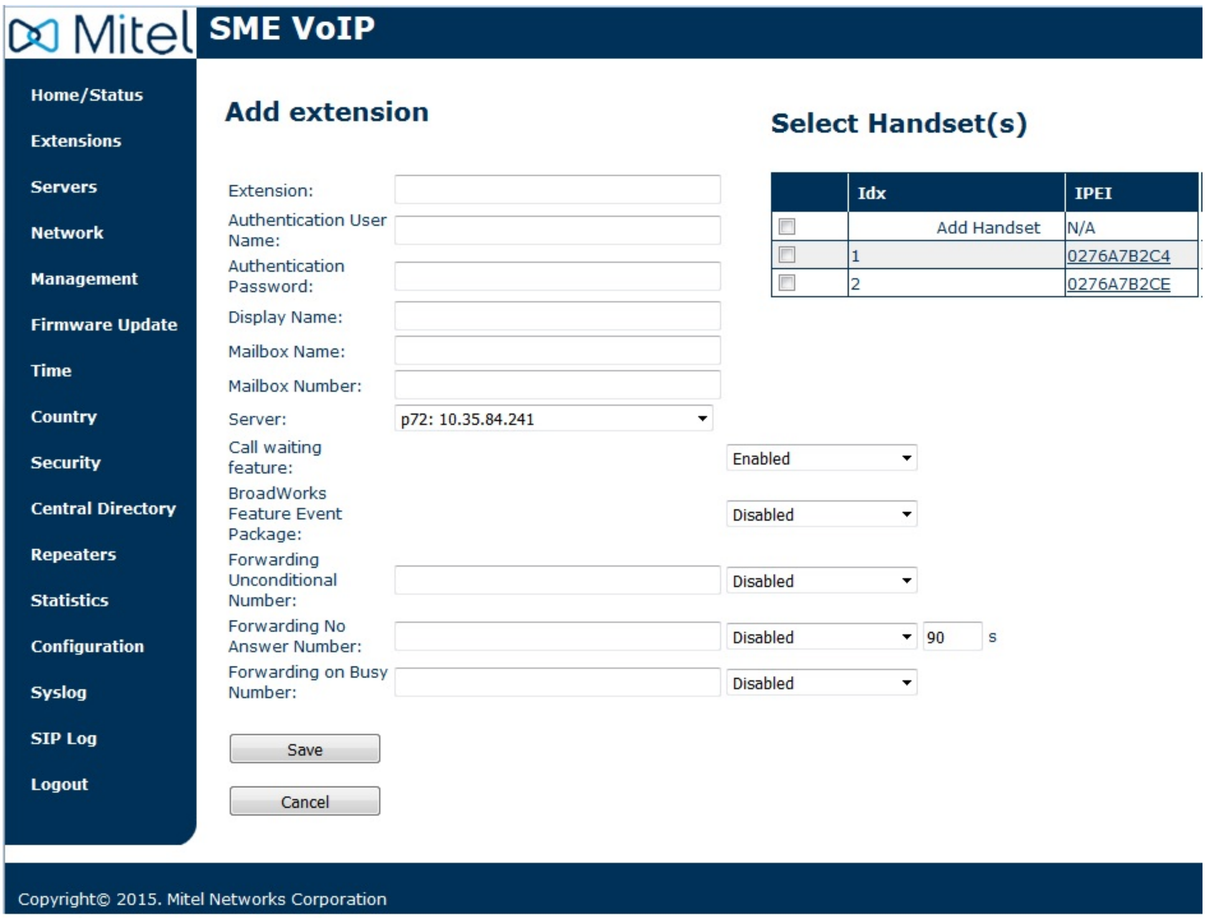
EXTENSIONS

This section describes the different parameters available whenever the administrator is creating extensions for handsets. Note, you cannot add extensions unless servers are defined. This section also describes the group call feature.

The system supports a maximum of 20 extensions with 20 associated handsets which can be divided between servers. Once 20 handsets are registered, it is not possible to add more extensions.

Note: Within servers or even with multi servers, extensions must always be unique. This means same extension number on server 1 cannot be re-used on server 2.

ADD EXTENSION



PARAMETER	DEFAULT VALUE(S)	DESCRIPTION
Extension	Empty	Handset phone number depending on the setup. **Possible value(s):** 8-bit string length **Example: 1024** **Note:** The Extension must also be configured in SIP server in order for this feature to function.
Authentication User Name	Empty	**Username:** SIP authentication username **Permitted value(s):** 8-bit string length
Authentication Password	Empty	**Password:** SIP authentication password. **Permitted value(s):** 8-bit string length
Display Name	Empty	Name displayed on the handset for the extension **Permitted value(s):** 8-bit string length
Mailbox Name	Empty	Name of centralized system that is used to store phone voice messages that can be retrieved by recipient at a later time. **Valid Input(s):** 8-bit string Latin characters for the Name
Mailbox Number	Empty	Dialled mail box number by long key press on key 1. **Valid Input(s)**: 0 – 9, *, # **Note: Mailbox Number parameter** is available only when it's enabled from SIP server.
Server	Server 1 IP	FQDN or IP address of SIP server. Drop down menu to select between the defined Servers of VoIP Service provider.
Call waiting feature	Enabled	Used to enable/disable Call Waiting feature. When disabled a second incoming call will be rejected. If enabled, a second call will be presented as call waiting.
Forwarding Unconditional Number	Empty	Number to which incoming calls must be re-routed, regardless of the current state of the handset.
	Disabled	Forwarding Unconditional must be enabled to function. **Note:** Feature must be enabled in the SIP server before it can function in the network. **Note:** Feature will be automatically disabled in case the handset or extension is part of a group
Forwarding No Answer Number	Empty	Number to which incoming calls must be re-routed to when there is no response from the SIP end node.
	Disabled	Forwarding No Answer Number must be enabled to function. **Note:** Feature must be enabled in the SIP server before it can function in the network.
	90	Specify delay from call to forward in seconds. **Note:** Feature is automatically disabled if the handset or extension is part of a group.
Forwarding On Busy Number	Empty	Number to which incoming calls must be re-routed when SIP node is busy. Forwarding On Busy Number must be enabled to function.

PARAMETER	DEFAULT VALUE(S)	DESCRIPTION
	Disabled	**Note:** Feature must be enabled in the SIP server before it can function in the network **Note:** Feature is automatically disabled if the handset or extension is part of a group.

GROUP CALL

When you add or edit an extension, you can subscribe handsets to the extension by selecting them in the **Selected Handset(s)** table, and make them part of a group.

Group Call is when a SIP extension is associated with multiple handsets. All handsets that are assigned with the extension can receive incoming calls and initiate outgoing calls from that extension. When assigned with Group Call, a handset supports all normal call features such as Hold, Transfer and so forth.

When an incoming call arrives to a group, all of the handsets assigned to the group are alerted. For example, if a group contains 20 handsets, all 20 handset will alert.

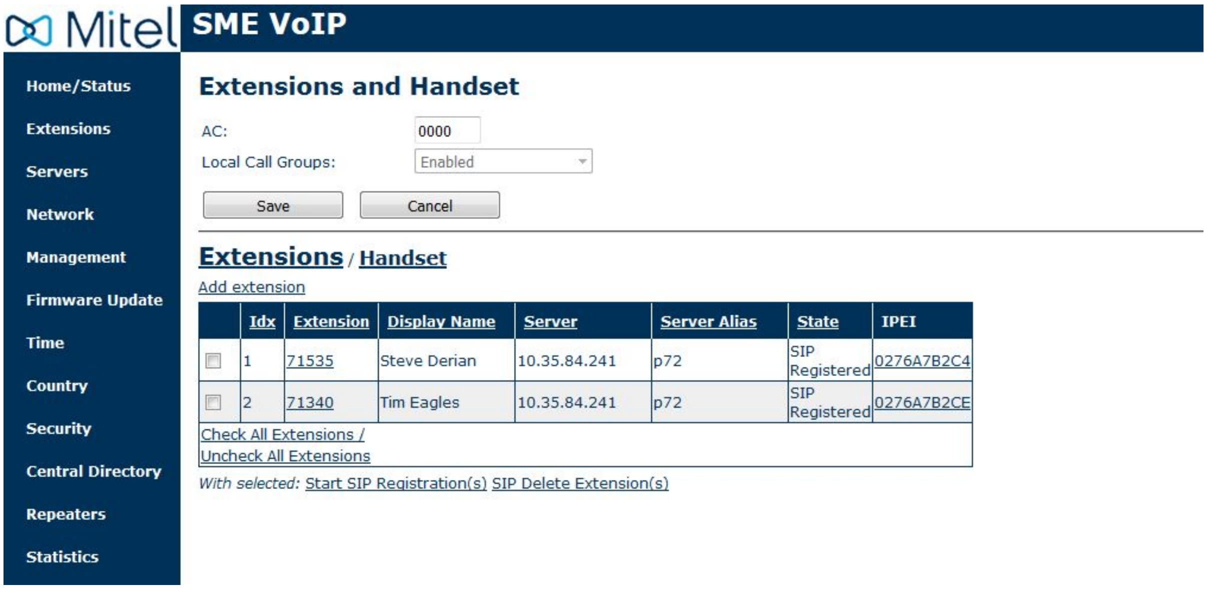
An alerting handset cannot receive another incoming call, and therefore if a handset subscribes for multiple Call Groups, and a call arrives for a 2nd Call Group while the handset is alerting, the handset will not receive this call. If DND is enabled for a given handset, it will not receive the incoming call.

For outgoing calls, it can be selected in the handset which line (i.e. Call Group) to use for the call. The maximum number of lines is 20. For any outgoing actions, the settings for the selected line (SIP extension) will be used.

EXTENSIONS LIST

The added extensions will be shown in the extension lists.

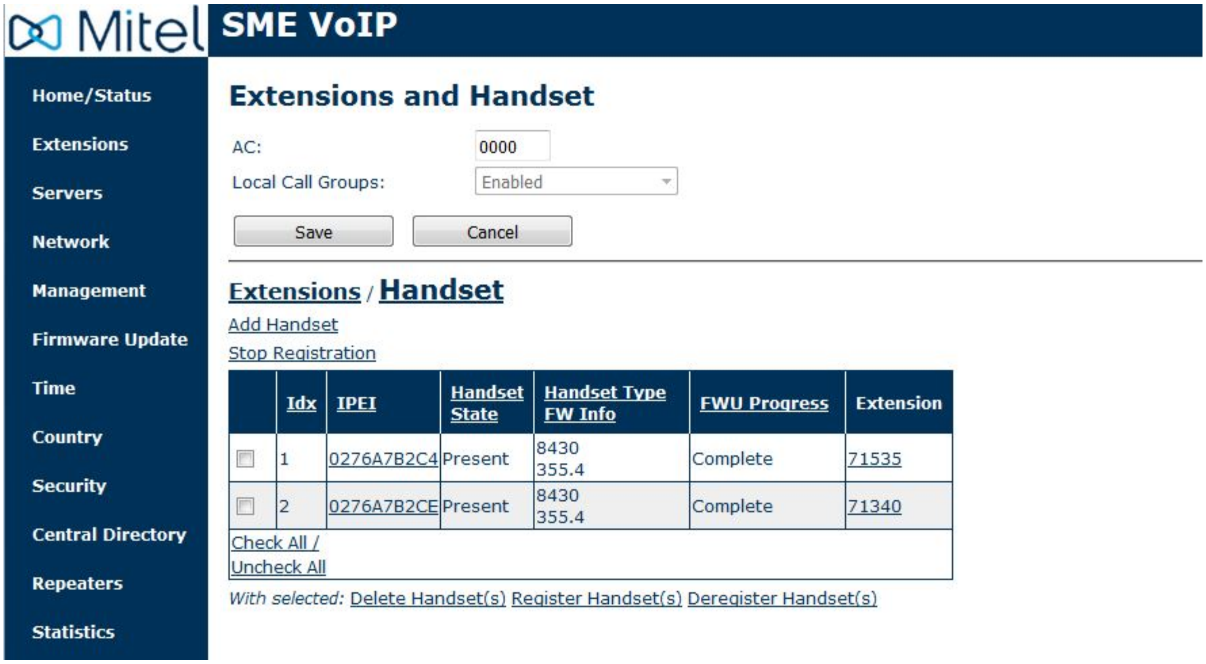
The list can be sorted by any of the top headlines, by mouse click on the headline link.



PARAMETER	DESCRIPTION
Idx	Select / deselect for delete, register and deregister handsets
Extension	Given extension is displayed.
Display Name	Given display name is displayed. If no name given this field will be empty
Server	Server IP or URL
Server Alias	Given server alias is displayed. If no alias given this field will be empty.
State	**SIP** registration state – if empty the handset is not SIP registered.
IPEI	Handset IPEI. IPEI is a unique DECT identification number. Group call: One extension can be associated to up to 20 IPEI's. The IPEI's will be listed in this cell.

HANDSET LIST

The added handsets will be shown in the handset lists.
The list can be sorted by any of the top headlines, by mouse click on the headline link.



PARAMETER	DESCRIPTION
Idx	Select / deselect for delete, register and deregister handsets
IPEI	Handset IPEI. IPEI is unique DECT identification number.
Handset state	The state of the given handset: **Present:** The handset is DECT located at the base **Detached:** The handset is detached from the system (e.g. powered off) **Removed:** The handset has been out of sight for a specified amount of time (~one hour).
Handset Type FW info	Handset type and firmware version of handset
FWU Progress	Possible FWU progress states: **Off:** Means sw version is specified to 0 = fwu is off **Initializing:** Means FWU is starting and progress is 0%. **X% :** FWU ongoing **Verifying X%:** FWU writing is done and now verifying before swap "**Waiting for charger**" (HS) / "**Conn. term. wait**" (Repeater): All FWU is complete and is now waiting for handset/repeater restart. **Complete HS/repeater**: FWU complete **Error:** Not able to fwu e.g. file not found, file not valid etc
Extension	Given extension is displayed. Group call: The cell will show all the extensions associated with this handset and IPEI.

Handset and extension list top/sub-menus

The handset extension list menu is used to control paring or deletion of handset to the system (DECT registration/de-registrations) and to control SIP registration/de-registrations to the system.

Above and below the list are found commands for making operations on handsets/and extensions. The top menu is general operations, and the sub menu is always operating on selected handsets/extensions.

Screenshots

In the below table each command is described.

ACTIONS	DESCRIPTION
Add extension	Access to the “Add extension” sub menu
Stop Registration	Manually stop DECT registration mode of the system. This prevents any handset from registering to the system
Delete Handset(s)	Deregister selected handset(s), but do not delete the extension(s).
Register Handset(s)	Enable registration mode for the system making it possible to register at a specific extension (selected by checkbox)
Deregister Handset(s)	Deregister the selected handset(s) and delete the extension(s).

EDIT EXTENSION

To edit extension use the mouse to click the link of the extension.

Edit extension will open the same configuration possibilities as add extension. Refer to the above add extension section.

SERVERS

In this section, we describe the different parameters available in the Servers configurations menu. A maximum of 10 servers can be configured.

PARAMETER	DEFAULT VALUE	DESCRIPTION
Server Alias	Empty	Parameter for server alias
NAT Adaption	Disabled	To ensure all SIP messages goes directly to the NAT gateway in the SIP aware router.

PARAMETER	DEFAULT VALUE	DESCRIPTION
Registrar	Empty	SIP Server proxy DNS or IP address Permitted value(s): AAA.BBB.CCC.DDD:<Port-Number> or <URL>:<Port-Number> Note: Specifying the Port Number is optional.
Outbound Proxy	Empty	This is a Session Border Controller DNS or IP address (OR SIP server outbound proxy address) Set the Outbound proxy to the address and port of private NAT gateway so that SIP messages sent via the NAT gateway. Permitted value(s): AAA.BBB.CCC.DDD or <URL> or <URL>:<Port-Number> Examples: “192.168.0.1”, “192.168.0.1:5062”, “nat.company.com” and “sip:nat@company.com:5065”.
Conference Server	Empty	Broadsoft conference feature. Set the IP address of the conference server. In case an IP is specified pressing handset conference will establish a connection to the conference server. If the field is empty the original 3-party local conference of 8660 is used.
Call Log Server	Empty	Broadsoft call log feature. Set the IP address of the XSI call log server. In case an IP is specified pressing handset will use the call log server. If the field is empty the local call log is used
Re-registration time	600	The “expires” value 36nalyse36n in SIP REGISTER requests. This value indicates how long the current SIP registration is valid, and hence is specifies the maximum time between SIP registrations for the given SIP account. Permitted value(s): A value below 60 sec is not recommended, Maximum value 65636
SIP Session Timers:	Disabled	RFC 4028. A “keep-alive” mechanism for calls. The session timer value specifies the maximum time between “keep-alive” or more correctly session refresh signals. If no session refresh is received when the timer expires the call will be terminated. Default value is 1800 s according to the RFC. Min: 90 s. Max: 65636. If disabled session timers will not be used.
Session Timer Values (s):	1800	Default value is 1800s according to the RFC. If disabled session timers will not be used. Permitted value(s): Minimum value 90, Maximum 65636
SIP Transport	UDP	Select UDP, TCP, TLS 1.0
Signal TCP Source Port	Disabled	When SIP Transport is set to TCP or TLS, a TCP (or TLS) connection will be established for each SIP

PARAMETER	DEFAULT VALUE	DESCRIPTION
		extension. The source port of the connection will be chosen by the TCP stack, and hence the local SIP port parameter, specified within the SIP/RTP Settings (see 0) will not be used. The "Signal TCP Source Port" parameter specifies if the used source port shall be signaled explicitly in the SIP messages.
Use One TCP/TLS Connection per SIP Extension:	Disabled	When using TCP or TLS as SIP transport, choose if a TCL/TLS connection shall be established for each SIP extension or if the base station shall establish one connection which all SIP extensions use. Please note that if TLS is used and SIP server requires client authentication (and requests a client certificate), this setting must be set to disabled. 0: Disabled. (Use one TCP/TLS connection for all SIP extensions) 1: Enabled. (Use one TCP/TLS connection per SIP extensions).
Keep Alive	Enabled	This directive defines the window period (30 sec.) to keep opening the port of relevant NAT-aware router(s), etc.
Show Extension on Handset Idle Screen	Enabled	If enabled extension will be shown on handset idle screen.
Hold Behaviour	RFC 3264	Specify the hold behaviour by handset hold feature. RFC 3264: Hold is 37nalyse37n according to RFC 3264, i.e. the connection information part of the SDP contains the IP Address of the endpoint, and the direction attribute is sendonly, recvonly or inactive dependant of the context RFC 2543: The "old" way of 37nalyse37ng HOLD. The connection information part of the SDP is set to 0.0.0.0, and the direction attribute is sendonly, recvonly or inactive dependant of the context
Attended Transfer Behaviour	Hold 2nd Call	1. When we have two calls, and one call is on hold, it is possible to perform attended transfer. When the transfer soft key is pressed in this situation, we have traditionally also put the active call on hold before the SIP REFER request is sent. However, we have experienced that some PBXes do not expect that the 2nd call is put on hold, and therefore attended transfer fails on these PBXes. 2. The "Attended Transfer Behaviour" feature defines whether or not the 2nd call shall be put on hold before the REFER is sent. 3. If "Hold 2nd Call" is selected, the 2nd call will be held before REFER is sent. If "Do Not Hold 2nd Call" is selected, the 2nd call will not be held before the REFER is sent
Use Own Codec Priority	Disabled	Default disabled. By enable the system codec priority during incoming

PARAMETER	DEFAULT VALUE	DESCRIPTION
		call is used instead of the calling party priority. E.g. If base has G722 as top codec and the calling party has Alaw on top and G722 further down the list, the G722 will be chosen as codec for the call.
DTMF Signalling	RFC 2833	Conversion of decimal digits (and '*' and '#') into sounds that share similar characteristics with voice to easily traverse networks designed for voice SIP INFO: Carries application level data along SIP signalling path (e.g.: Carries DTMF digits generated during SIP session OR sending of DTMF tones via data packets in the same internet layer as the Voice Stream, etc.). RFC 2833: DTMF handling for gateways, end systems and RTP trunks (e.g.: Sending DTMF tones via data packets in different internet layer as the voice stream) Both: Enables SIP INFO and RFC 2833 modes.
DTMF Payload Type	101	This feature enables the user to specify a value for the DTMF payload type / telephone event (RFC2833).
Codec Priority	G.711U G.711A G.726	Defines the codec priority that base stations uses for audio compression and transmission. Possible Option(s): G.711U,G.711A, G.726, G.729, G.722. Note: Modifications of the codec list must be followed by a "reset codes" and "Reboot chain" on the multipage in order to change and update handsets. Note: With G.722 as first priority the number of simultaneous calls per base station will be reduced from 10 (8) to 4 calls. With G.722 in the list the codec negotiation algorithm is active causing the handset (phone) setup time to be slightly slower than if G.722 is removed from the list. With G.729 add on DSP module for the base is required.
RTP Packet size	20ms	The packet size offered as preferred RTP packet size by 8630 when RTP packet size negotiation. Selections available: 20ms, 40ms, 60ms, 80ms
Secure RTP	Disabled	With enable RTP will be encrypted (AES-128) using the key negotiated via the SDP protocol at call setup.
Secure RTP Auth	Disabled	With enable secure RTP is using authentication of the RTP packages. Note: with enabled SRTP authentication maximum 4 concurrent calls is possible per base in a single or multicell system.
SRTP Crypto Suites	AES_CM_128_HMAX_SHA1_32 AES_CM_128_HMAX	Field list of supported SRTP Crypto Suites. The device is born with two suites.

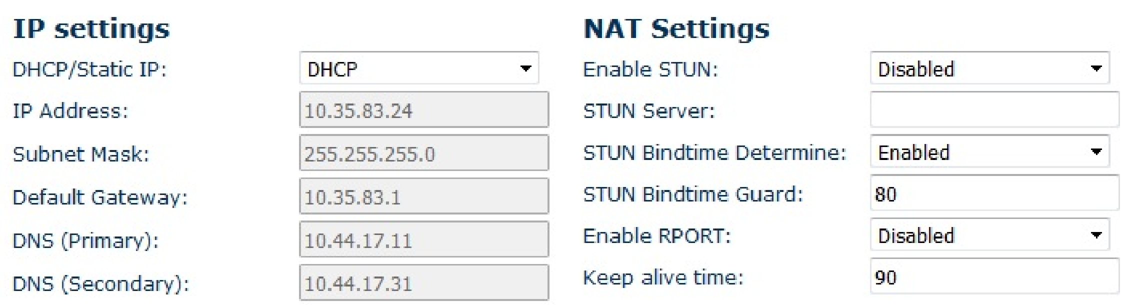
PARAMETER	DEFAULT VALUE	DESCRIPTION
	_SHA1_80	

Note: Within servers or even with multi servers, extensions must always be unique. This means same extension number on server 1 cannot be re-used on server 2.

NETWORK

In this section, we describe the different parameters available in the network configurations menu.

IP SETTINGS



PARAMETER	DEFAULT VALUES	DESCRIPTION
DHCP/Static IP	DHCP	If DHCP is enabled, the device automatically obtains TCP/IP parameters. **Possible value(s):** Static, DHCP **DHCP:** IP addresses are allocated automatically from a pool of leased address. **Static IP:** IP addresses are manually assigned by the network administrator. If the user chooses DHCP option, the other IP settings or options are not available.
IP Address	NA	32-bit IP address of device (e.g. base station). 64-bit IP address will be supported in the future. **Permitted value(s): AAA.BBB.CCC.DDD**
Subnet Mask	NA	Is device subnet mask. **Permitted value(s): AAA.BBB.CCC.DDD** This is a 32-bit combination used to describe which portion an IP address refers to the subnet and which part refers to the host. A network mask helps users know which portion of the address identifies the network and which portion of the address identifies the node.
Default Gateway	NA	Device’s default network router/gateway (32-bit).

PARAMETER	DEFAULT VALUES	DESCRIPTION
		Permitted value(s): AAA.BBB.CCC.DDD e.g. **192.168.50.0** IP address of network router that acts as entrance to other network. This device provides a default route for TCP/IP hosts to use when communicating with other hosts on hosts networks.
DNS (Primary)	NA	Main server to which a device directs Domain Name System (DNS) queries. **Permitted value(s): AAA.BBB.CCC.DDD or <URL>** This is the IP address of server that contains mappings of DNS domain names to various data, e.g. IP address, etc. The user needs to specify this option when static IP address option is chosen.
DNS (Secondary)	NA	This is an alternate DNS server.

VLAN SETTINGS

Enable users to define devices (e.g. Base station, etc.) with different physical connection to communicate as if they are connected on a single network segment.

The VLAN settings can be used on a managed network with separate Virtual LANs (VLANs) for sending voice and data traffic. To work on these networks, the base stations can tag voice traffic it generates on a specific “voice VLAN” using the IEEE 802.1q specification.

PARAMETER	DEFAULT VALUES	DESCRIPTION
VLAN id	0	Is a 12 bit identification of the 802.1Q VLAN. **Permitted value(s):** 0 to 4094 (only decimal values are accepted) A VLAN ID of 0 is used to identify priority frames and ID of 4095 (i.e. FFF) is reserved. Null means no VLAN tagging or No VLAN discovery through DHCP.
VLAN User Priority	0	This is a 3 bit value that defines the user priority. Values are from 0 (best effort) to 7 (highest); 1 represents the lowest priority. These values can be used to prioritize different classes of traffic (voice, video, data, etc). **Permitted value(s):** 8 priority levels (i.e. 0 to 7)

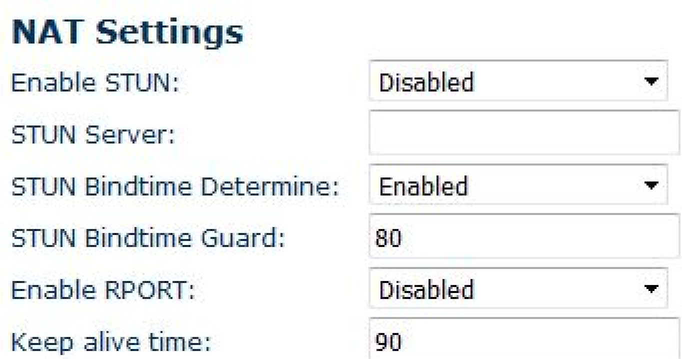
For further help on VLAN configuration refer to Appendix.

DHCP OPTIONS

PARAMETER	DEFAULT VALUES	DESCRIPTION
Plug-n-Play	Disabled	Enabled: DHCP option 43 to automatically provide PBX IP address to base.

NAT SETTINGS

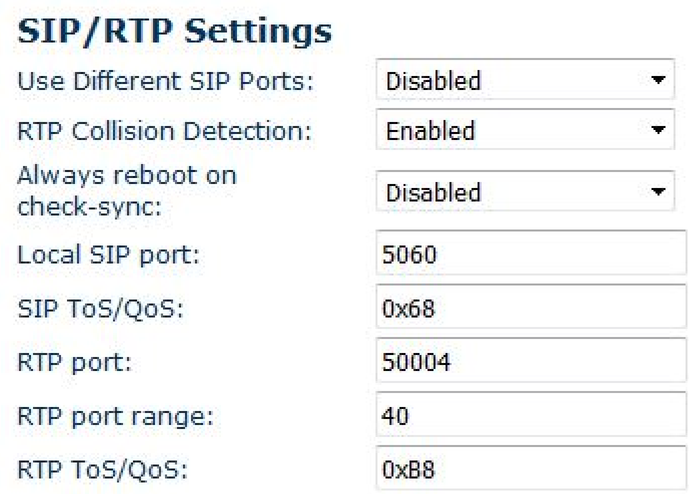
We define some options available when NAT aware routers are enabled in the network.



PARAMETER	DEFAULT VALUES	DESCRIPTION
Enable STUN	Disabled	Enable to use STUN
STUN Server	NA	**Permitted value(s): AAA.BBB.CCC.DDD** (Currently only Ipv4 are supported) or **url** (e.g.: firmware.rtx.net).
STUN Bindtime Determine	Enabled	
STUN Bindtime Guard	80	**Permitted values:** Positive integer default is 90, unit is in seconds
Enable RPORT	Disabled	Enable to use RPORT in SIP messages.
Keep alive time	90	This defines the frequency of how keep-alive are sent to maintain NAT bindings. **Permitted values:** Positive integer default is 90, unit is in seconds

SIP/RTP SETTINGS

These are some definitions of SIP/RTP settings:



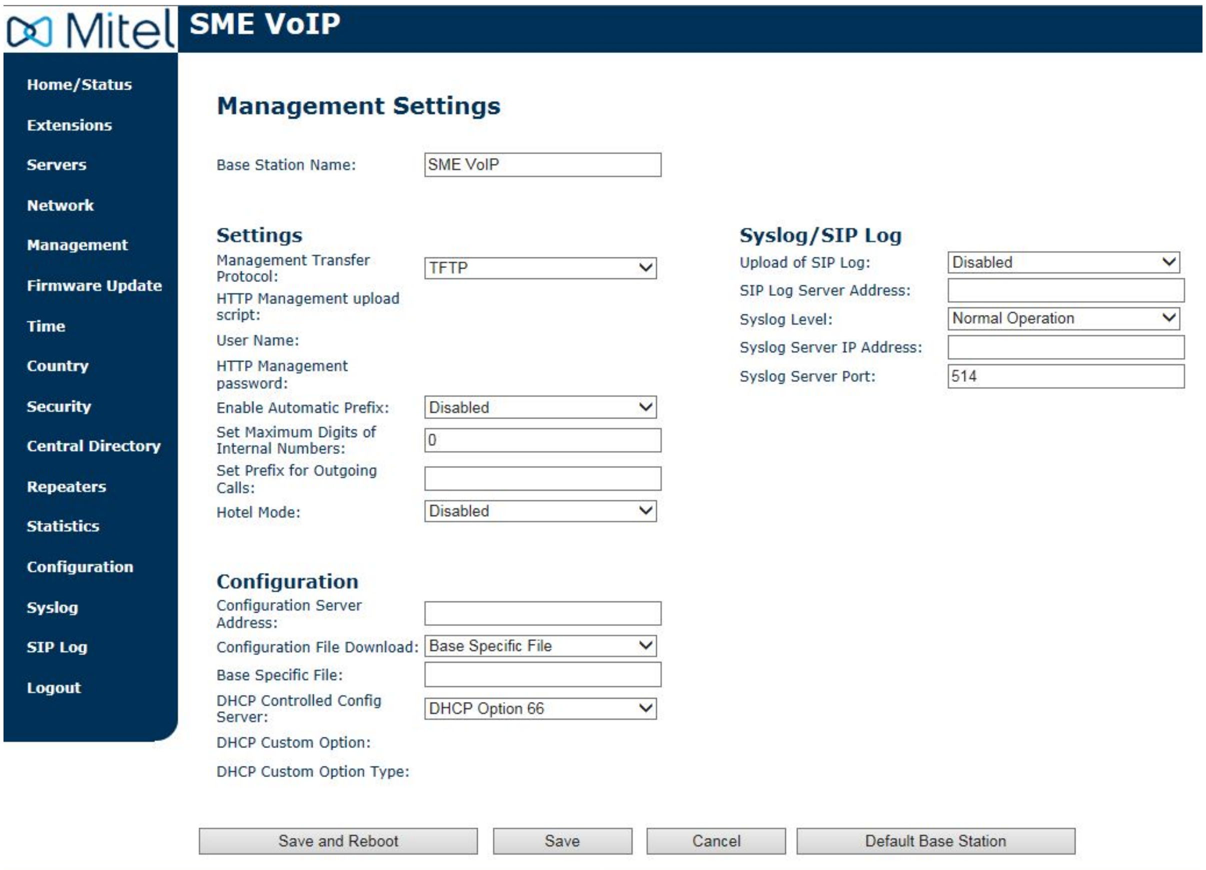
PARAMETER	DEFAULT VALUES	DESCRIPTION
Use Different SIP Ports	Disabled	If disabled, the Local SIP port parameter specifies the source port used for SIP signalling in the system. If enabled, the Local SIP Port parameter specifies the source port used for first user agent (UA) instance. Succeeding UA's will get succeeding ports.
RTP Collision Detection	Enabled	
Local SIP port	5060	The source port used for SIP signalling **Permitted values:** Port number default 5060.
SIP ToS/QoS	0x68	Priority of call control signalling traffic based on both IP Layers of Type of Service (ToS) byte. ToS is referred to as Quality of Service (QoS) in packet based networks. **Permitted values:** Positive integer, default is 0x68
RTP port	50004	The first RTP port to use for RTP audio streaming. **Permitted values:** Port number default 50004 (depending on the setup).
RTP port range	40	The number of ports that can be used for RTP audio streaming. **Permitted values:** Positive integers, default is 40
RTP TOS/QoS	0xB8	Priority of RTP traffic based on the IP layer ToS (Type of Service) byte. ToS is referred to as Quality of Service (QoS) in packet based networks. See RFC 1349 for details. "cost bit" is not supported. o Bit 7..5 defines precedence. o Bit 4..2 defines Type of Service.

PARAMETER	DEFAULT VALUES	DESCRIPTION
		o Bit 1..0 are ignored. Setting all three of bit 4..2 will be ignored. **Permitted values:** Positive integer, default is 0xB8

MANAGEMENT SETTINGS DEFINITIONS

The administrator can configure base stations to perform some specific functions such as configuration of file transfers, firmware up/downgrades, password management, and SIP/debug logs.

Screenshot



PARAMETER	DEFAULT VALUE	DESCRIPTION
Base Station Name:	VoIP	It indicates the title that appears at the top window of the browser and is used in the multicell page.
Management Transfer Protocol	TFTP	The protocol assigned for configuration file and central directory **Valid Input(s):** TFTP, HTTP, HTTPs
HTTP Management upload script	Empty	The folder location or directory path that contains the configuration files of the Configuration server. The configuration upload script is a file located in e.g. TFTP server or Apache Server which is also the configuration server. **Permitted value(s): /<configuration-file-directory>** **Example:** /CfgUpload **Note:** Must begin with (/) slash character. Either / or \ can

PARAMETER	DEFAULT VALUE	DESCRIPTION
		be used.
HTTP Management password	Empty	Password that should be entered in order to have access to the configuration server. **Permitted value(s):** 8-bit string length
Enable Automatic Prefix	Disabled	
Set Maximum Digits of Internal Numbers	0	
Set Prefix for Outgoing Calls	Blank	
Hotel Mode	Disabled	For hospitality (Hotel/Motel) environments, enable the **Hotel Mode** setting to • Black out the handset display when placed in cradle (after 65 seconds) • Protect the handset **Settings** menu (changes default handset PIN from 0000 to 9351; PIN is required to access the **Settings** menu) • Enable silent upgrades and resets • Disable call logging • Prevent phonebook modification.
Configuration server address	Empty	Server/device that provides configuration file to base station. **Type:** DNS or IP address **Permitted value(s): AAA.BBB.CCC.DDD or <URL>**
Base Specific File	Empty	Base configuration file
Configuration File Download	Disabled	Base Specific file: Used when configuring a single cell base Multicell Specific File: Used when configuring a multicell based system Base and Multicell Specific File: Used on out of factory bases to specify VLAN and Multicell ID and settings.
DHCP Controlled Config Server	Disabled	Provisioning server options. DHCP Option 66: Look for provision file by TFTP boot up server. DHCP Custom Option: Look for provision file by custom option DHCP Custom Option & Option 66: Look for provision file by first custom option and then option 66.
DHCP Custom Option	Empty	By default option 160, but custom option can be defined. An option 160 URL defines the protocol and path information by using a fully qualified domain name for clients that can use DNS.

PARAMETER	DEFAULT VALUE	DESCRIPTION
DHCP Custom Option Typr	Empty	URL: URL of server with path. Example of URL: http://myconfigs.com:5060/configs Default configuration file on server must follow the name: MAC.cfg IP Address: IP of server with path.
Text Messaging	Disabled	Disable/enable messaging with Mobicall server The third option is to "Enable Without Server". With this setting handset can send messages to other handsets, which support messaging. **Note**: Contact Mobicall to get the proper version and setup for Mobicall server
Text Messaging & Alarm server	Empty	**Permitted value(s): AAA.BBB.CCC.DDD or <URL>**
Text Messaging Port	1300	Port number of message server.
Text Messaging Keep Alive (m)	30	This defines the frequency of how keep-alive are sent **Permitted values:** Positive integer, unit is in minutes
Text Messaging Response (s)	30	This defines the frequency of how response timeout **Permitted values:** Positive integer, unit is in seconds
Text Messaging TTL	0	This defines the text messaging time to live **Permitted values:** Positive integer, unit is in seconds
SIP Log Server Address	Empty	**Permitted value(s): AAA.BBB.CCC.DDD or <URL>** Requires a predefined folder named: \SIP
Upload of SIP Log	Disabled	Enable this option to save low level SIP debug messages to the server. The SIP logs are saved in the file format: **<MAC_Address><Time_Stamp>SIP.log**
Syslog Server IP-Address	NA	**Permitted value(s): AAA.BBB.CCC.DDD or <URL>**
Syslog Server Port	NA	Port number of syslog server.
Syslog Level	Off	Off: No data is saved on syslog server Normal Operation: Normal operation events are logged, incoming call, outgoing calls, handset registration, DECT location, and call lost due to busy, critical system errors, general system information. System Analyze: Handset roaming, handset firmware updates status. The system 46nalyse level also contains the messages from normal operation. Debug: Used by Design for debug. Should not be enabled during normal operation.
Enable Automatic Prefix	Disabled	**Disabled**: Feature off. **Enabled**: The base will add the leading digit defined in "Set

PARAMETER	DEFAULT VALUE	DESCRIPTION
		Prefix for Outgoing Calls”. **Enabled + fall through on * and #:** Will enable detection of * or # at the first digit of a dialled number. In case of detection the base will not complete the dialled number with a leading 0. Examples: 1. dialed number on handset * 1234 - > dialed number to the pabx *1234 2. dialed number on handset #1234 - > dialed number to the pabx #1234 3. dialed number on handset 1234 - > dialed number to the pabx 01234
Set Maximum Digits of Internal Numbers	0	Used to detect internal numbers. In case of internal numbers no prefix number will be added to the dialled number.
Set Prefix for Outgoing Calls	Empty	Prefix number for the enabled automatic prefix feature. **Permitted value(s): 1 to 9999**

There are three ways of configuring the system.

1. Manual configuration by use of the Web server in the base station(s)

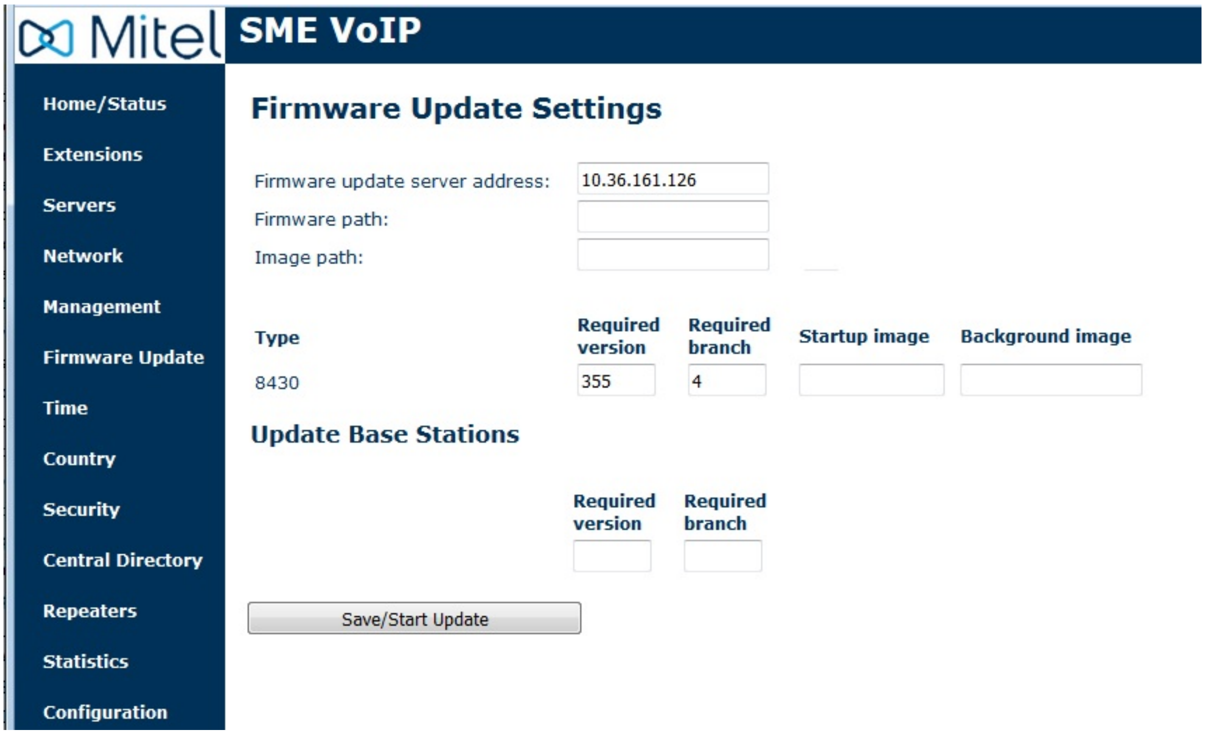
2. By use of configuration files that are uploaded from a disk via the “Configuration” page on the Web server.

3. By use of configuration files which the base station(s) download(s) from a configuration server.

For further details refer to doc reference [3].

FIRMWARE UPDATE DEFINITIONS

In this page, the system administrator can configure how base stations and SIP nodes upgrade/downgrade to the relevant firmware. Handset firmware update status can be found in the extensions page and repeater firmware update status in the repeater page. Base firmware update status is found in the multicell page.



PARAMETER	DEFAULT VALUE(S)	DESCRIPTION
Firmware update server address	Empty	IP address or DNS of firmware update files source **Valid Inputs:** AAA.BBB.CCC.DDD or <URL> **Example:** firmware.rtx.net or 10.10.104.41
Firmware path	Empty	Location of firmware on server (or firmware update server path where firmware update files are located). **Example:** /East_Fwu **Note:** Must begin with (/) slash character
Required Version Type	Empty	Version of firmware to be upgraded (or downgraded) on handset type or repeater. **Valid Input(s):** 8-bit string length. E.g. 280 **Note: Value version 0** will disable firmware upgrade for handsets and/or repeater **Note:** Two handset types will be serial firmware upgraded. First type 8630 then type 8430.
Required Version Base	Empty	Version of firmware to be upgraded (or downgraded) on Base station. Base units are referred to as gateways over here. **Valid Input(s):** 8-bit string length. E.g. 280

TIME SERVER

In this section, we describe the different parameters available in the Time Server menu.

The Time server supplies the time used for data synchronisation in a multi-cell configuration. As such it is mandatory for a multi-cell configuration. The system will not work without a time server configured.

As well the time server is used in the debug logs and for SIP traces information pages, and used to determine when to check for new configuration and firmware files.

Note: It is not necessary to set the time server for standalone base stations (optional).

Press the "Time PC" button to grab the current PC time and use in the time server fields.

Note: When time server parameters are modified/changed synchronisation between base stations can take up to 15 minutes before all base stations are synchronised, depending on the number of base stations in the system.

PARAMETER	DEFAULT VALUES	DESCRIPTION
Time Server	Empty	DNS name or IP address of NTP server. Enter the IP/DNS address of the server that distributes reference clock information to its clients including Base stations, Handsets, etc. **Valid Input(s):** AAA.BBB.CCC.DDD or URL (e.g. time.server.com) Currently only Ipv4 address (32-bit) nomenclature is supported.
Allow broadcast NTP	Checked	
Refresh time (h)	Empty	The window time in hours within which time server refreshes. **Valid Inputs:** positive integer

PARAMETER	DEFAULT VALUES	DESCRIPTION
Set timezone by country/region	Checked	By checked country setting is used (refer to country web page).
Time Zone	0	Refers to local time in GMT or UTC format. **Min:** -12:00 **Max:** +13:00
Set DST by country/region	Checked	By checked country setting is used (refer to country web page).
Daylight Saving Time (DST)	Disabled	The system administrator can Enable or Disable DST manually. Automatic: Enter the start and stop dates if you select Automatic.
DST Fixed By Day	Use Month and Date	You determine when DST actually changes. Choose the relevant date or day of the week, etc. from the drop down menu.
DST Start Month	March	Month that DST begins **Valid Input(s):** Gregorian months (e.g. January, February, etc.)
DST Start Date	25	Numerical day of month DST comes to effect when DST is fixed to a specific date **Valid Inputs:** positive integer
DST Start Time	3	DST start time in the day **Valid Inputs:** positive integer
DST Start Day of Week	Monday	Day within the week DST begins
DST Start Day of Week, Last in Month	Last in Month	Specify the week that DST will actually start.
DST Stop Month	October	The month that DST actually stops.
DST Stop Date	1	The numerical day of month that DST turns off. **Valid Inputs:** positive integer (1 to 12)
DST Stop Time	2	The time of day DST stops **Valid Inputs:** positive integer (1 to 12)
DST Stop Day of Week	Sunday	The day of week DST stops
DST Stop Day of Week Last in Month	First in Month	The week within the month that DST will turn off.

COUNTRY

The country setting controls the in-band tones used by the system. To select web interface language go to the management page.

PARAMETER	DEFAULT VALUES	DESCRIPTION
Select Country	Germany	Supported countries: Australia, Belgium, Brasil, Denmark, Germany, Spain, France, Ireland, Italia, Luxembourg, Nederland, New Zealand, Norway, Portugal, Swiss, Finland, Sweden, Tyrkey, United Kingdom, US/Canade, Austria
State / Region	NA	Only shown by country selection US/Canada, Autralia, Brasil
Select Language	English	Web interface language. Number of available languages: English, Dansk, Italiano, Tyrkie, Deutsch, Portuguese, Hrvatski, Srpski, Slovenian, Nederlands, Francaise, Espanol, Russian, Polski.
Set timezone by country/region	checked	When checked timezone will follow country/region
Set DST by country/region	checked	When checked DST will follow country/region
Notes	Empty	Only showing notes to time setting for countries: US/Canada, Brasil

Note: By checked timezone and DST the parameters in web page Time will be discarded.

The following types of in-band tones are supported:

1. Dial tone
2. Busy tone
3. Ring Back tone
4. Call Waiting tone
5. Re-order tone

SECURITY

The security section is used for loading of certificates and for selecting if only trusted certificates are used. Furthermore, web password can be configured.

The Security web is divided into three sections: Certificates (trusted), SIP Client Certificates (and keys) and Password administration.

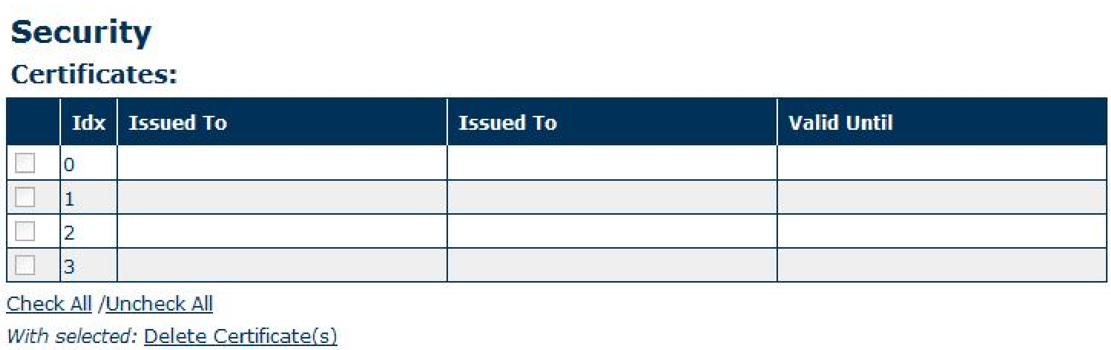
To setup secure fwu and configuration file download select HTTPs for the Management Transfer Protocol (refer to management web).

SIP and RTP security is server dependent and in order to configure user must use the web option Servers (refer to servers web).

CERTIFICATES

The certificates list contains the list of loaded certificates for the system. Using the left column check mark it is possible to check and delete certificates. To import a new certificate use the mouse “select file” and browse to the selected file. When file is selected, use the “Load” bottom to load the certificate.

The certificate format supported is DER encoded binary X.509 (.cer).


Security

Certificates:

	Idx	Issued To	Issued To	Valid Until
	0			
	1			
	2			
	3			

Check All /Uncheck All

With selected: Delete Certificate(s)

Certificates list

PARAMETER	DEFAULT VALUES	DESCRIPTION
Idx	Fixed indexes	Index number
Issued To	Empty	IP address – which is part of the certificate file
Issued To	Empty	Organization, Company – which is part of the certificate file

PARAMETER	DEFAULT VALUES	DESCRIPTION
Valid Until	Empty	Date Time Year – which is part of the certificate file

By enabling Use Only Trusted Certificates, the certificates the base will receive from the server must be valid and loaded into the system. If no valid matching certificate is found during the TLS connection establishment, the connection will fail. When Use Only Trusted Certificates is disabled, all certificates received from the server will be accepted.

Note: It is important to use correct date and time of the system when using trusted certificates. In case of time/date not defined the certificate validation can fail.

SIP CLIENT CERTIFICATES

To be able to establish a TLS connection in scenarios, where the server requests a client certificate, a certificate/key pair must be loaded into the base. This is currently supported only for SIP.

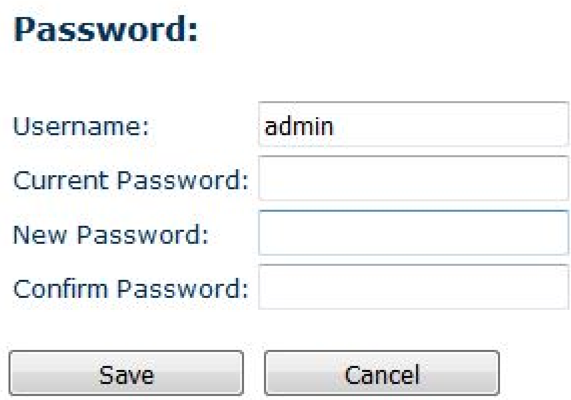
To load a client certificate/key pair, both files must be selected at the same time, and it is done by pressing “select files” under “Import SIP Client Certificate and Key Pair” and then select the certificate file as well as the key file at the same time. Afterwards, press load.

The certificate must be provided as a DER encoded binary X.509 (.cer) file, and the key must be provided as a binary PKCS#8 file.

Note: Use Chrome for loading SIP Client Certificates.

PASSWORD

In the below the password parameters are defined.



PARAMETER	DEFAULT VALUES	DESCRIPTION
Username	Admin	Can be modified to any supported character and number
Current Password	Admin	Can be modified to any supported character and number
New Password	Empty	Change to new password
Confirm Password	Empty	Confirm password to reduce accidently wrong changes of passwords

Password valid special signs:	@/|<>-_:.!?*+#
Password valid numbers:	0-9
Password valid letters:	a-z and A-Z

CENTRAL DIRECTORY AND LDAP

The system supports two types of central directories, a local central directory or LDAP directory.

For both directories caller id look up is made with match for 6 digits of the phone number.

LOCAL CENTRAL DIRECTORY

Select local and save for local central directory.

Screenshot

PARAMETER	DEFAULT VALUES	DESCRIPTION
Local	Local	Drop down menu to select between local central directory and LDAP based central directory

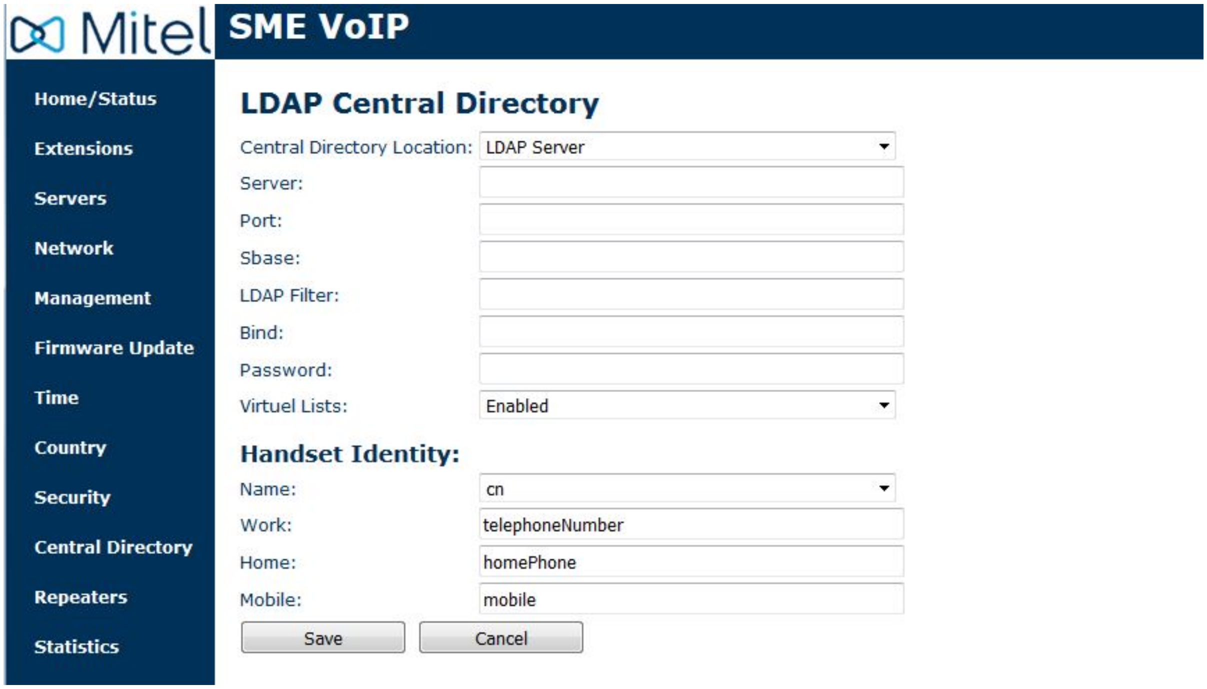
Server	Empty	The parameter is used if directory file is located on server. Valid Inputs: AAA.BBB.CCC.DDD or <URL> Refer to appendix for further details.
Filename	Empty	The parameter is used if directory file is located on server. Refer to appendix for further details
Phonebook reload interval (s)	0	The parameter is controlling the reload interface of phonebook in seconds. The feature is for automatic reload the base phonebook file from the server with intervals. It is recommended to specify a conservative value to avoid overload of the base station. With default value setting 0 the reload feature is disabled.

Import Central Directory

The import central directory feature is using a browse file approach. After file selection press the load button to load the file. The system support only the original *.csv format. Please note that some excel csv formats are not the original csv format. The central directory feature can handle up to 3000 contacts. For further details of the central directory feature refer to appendix.

LDAP

In the Location field, select LDAP Server and click Save.



PARAMETER	DEFAULT VALUES	DESCRIPTION
LDAP Server	LDAP Server	Drop down menu to select between local central directory and LDAP based central directory. LDAP Server is displayed when LDAP server is selected.
Server	Empty	IP address of the LDAP server. **Valid Inputs:** AAA.BBB.CCC.DDD or <URL>
Port	Empty	The server port number that is open for LDAP connections.
Sbase	Empty	Search Base. The criteria depends on the configuration of the LDAP server. Example of the setting is CN=Users, DC=umber, DC=loc
LDAP filter	Empty	LDAP Filter is used to as a search filter, e.g. setting LDAP filter to (|(givenName=%*)(sn=%*)) the IP-DECT will use this filter when requesting entries from the LDAP server. % will be replaced with the entered prefix e.g searching on J will give the filter (|(givenName=J*)(sn=J*)) resulting in a search for given name starting with a J or surname starting with J.
Bind	Empty	Bind is the username that will be used when the IP-DECT phone connects to the server
Password	Empty	Password is the password for the LDAP Server
Name	Empty	The name can be used to specify if sn+givenName or cn (common name) is return in the LDAP search results
Work Number	Empty	Work number is used to specify that LDAP attribute that will be mapped to the handset work number

PARAMETER	DEFAULT VALUES	DESCRIPTION
Home Number	Empty	Home number is used to specify that LDAP attribute that will be mapped to the handset home number
Mobile Number	Empty	Mobile number is used to specify that LDAP attribute that will be mapped to the handset mobile number

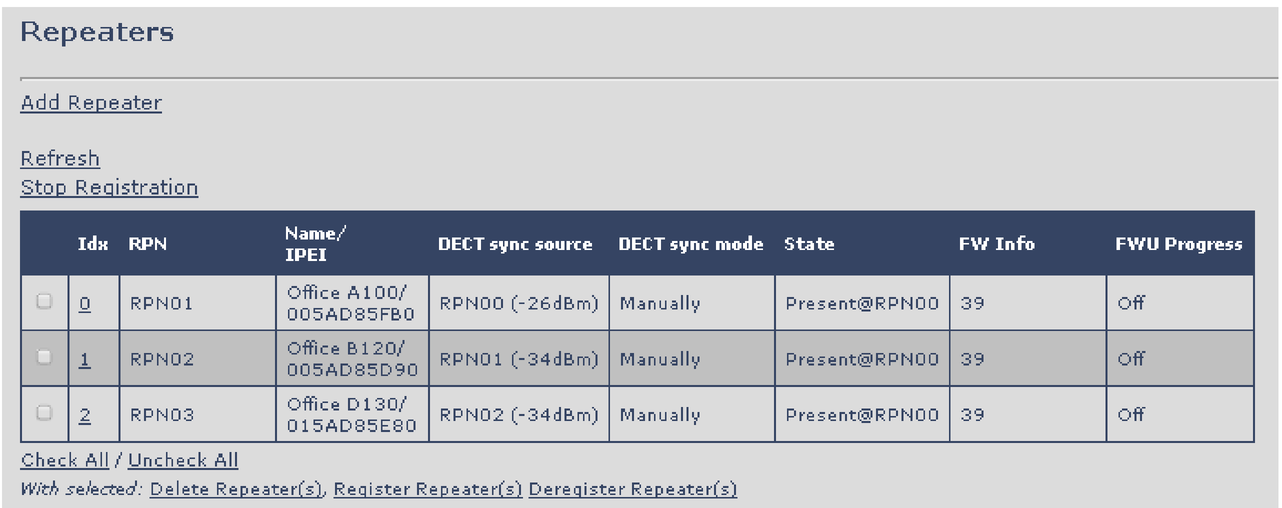
REPEATERS

Within this section we describe the repeater parameter, and how to operate the repeater.

ADD REPEATER

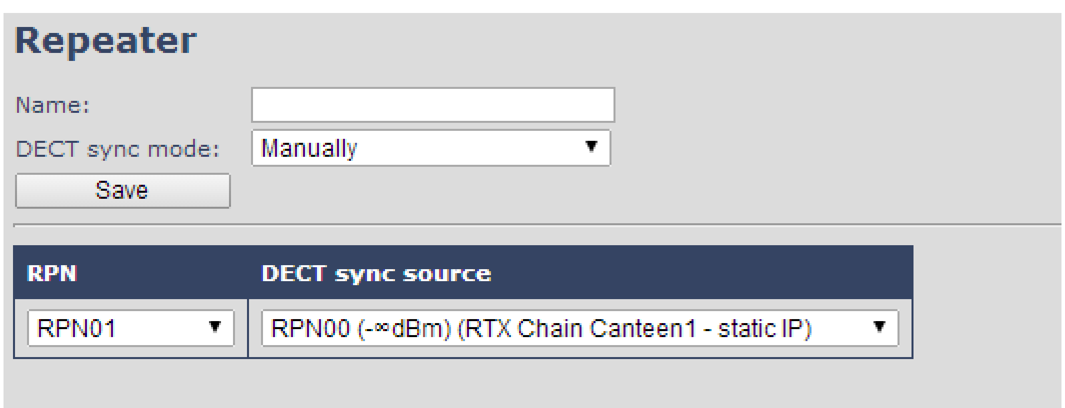
From repeaters web select "Add Repeater"

Screenshot



Then select "DECT Sync mode"

Screenshot



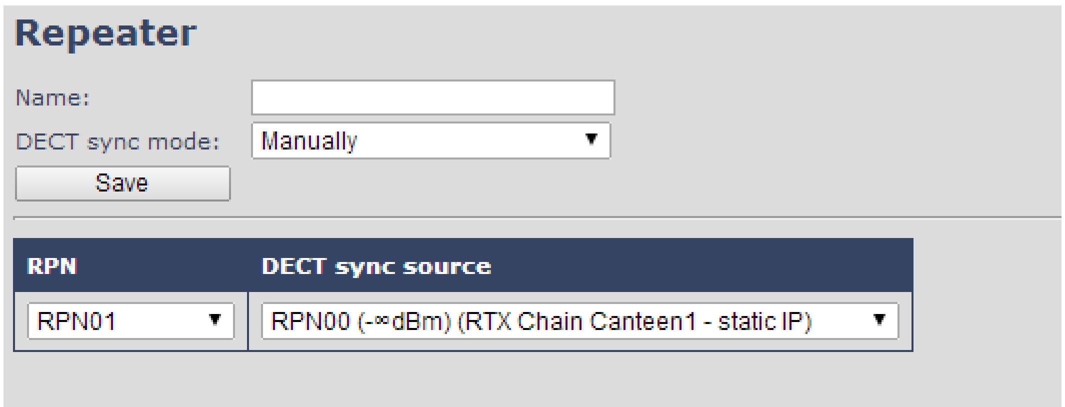
PARAMETERS **DESCRIPTION**

Name	Repeater name. If no name specified the field will be empty
DECT sync mode	**Manually:** User controlled by manually assign "Repeater RPN" and "DECT sync source RPN" **Local Automatical:** Repeater controlled by auto detects best base signal and auto assign RPN.

Manually

User controlled by manually assign "Repeater RPN" and "DECT sync source RPN". The parameters are selected from the drop down menu.

Screenshot



PARAMETERS	DESCRIPTION
Idx	System counter
RPN	SINGLE CELL SYSTEM: The base has always RPN00, first repeater will then be RPN01, second repeater RPN02 and third RPN03 (3 repeaters maximum per base) MULTI CELL SYSTEM: Bases are increment by 2^2 in hex, means first base RPN00 second base RPN04 etc., in between RPN01, 02, 03 addressed for repeaters at Primary base and 05, 06, 07 addressed for Secondary base (3 repeaters maximum per base)
DECT sync source	Select the base or repeater the repeater has to be synchronized to.

Local Automatical

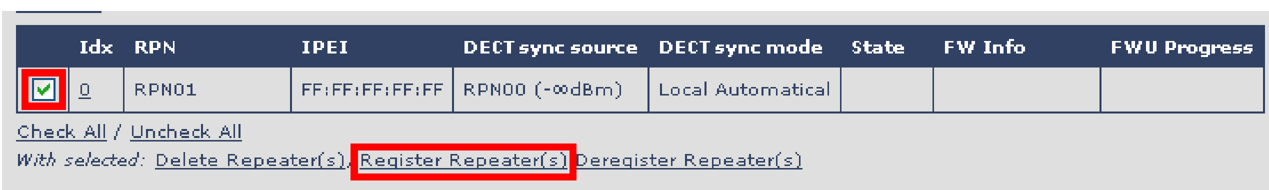
Repeater controlled by auto detects best base signal and auto assign RPN. The RPN and DECT sync source are greyed out.

The repeater RPN is dynamic assigned in base RPN range.

With local automatical mode, repeater on repeater (chain) is not supported.

REGISTER REPEATER

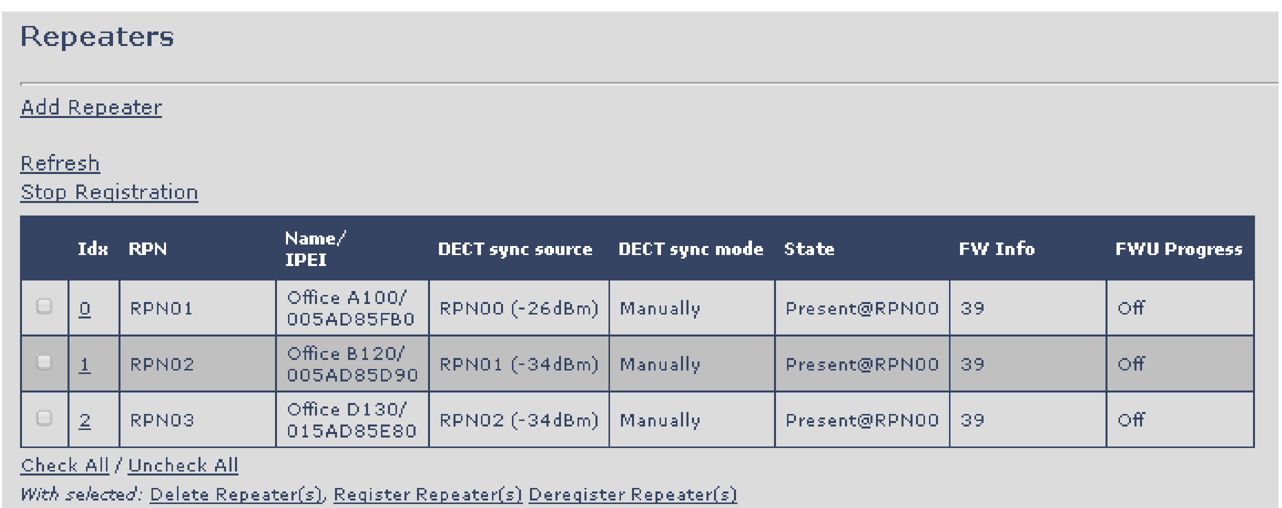
Adding a repeater makes it possible to register the repeater. Registration is made by select the repeater and pressing register repeater. The base window for repeater registration will be open until the registration is stopped. By stopping the registration all registration on the system will be stopped inclusive handset registration.



	Idx	RPN	IPEI	DECT sync source	DECT sync mode	State	FW Info	FWU Progress
☑	0	RPN01	FF:FF:FF:FF:FF	RPN00 (-∞dBm)	Local Automatical			

Check All / Uncheck All
With selected: Delete Repeater(s), Register Repeater(s) Deregister Repeater(s)

REPEATERS LIST



Repeaters

Add Repeater

Refresh
Stop Registration

	Idx	RPN	Name/ IPEI	DECT sync source	DECT sync mode	State	FW Info	FWU Progress
☐	0	RPN01	Office A100/ 005AD85FB0	RPN00 (-26dBm)	Manually	Present@RPN00	39	Off
☐	1	RPN02	Office B120/ 005AD85D90	RPN01 (-34dBm)	Manually	Present@RPN00	39	Off
☐	2	RPN03	Office D130/ 015AD85E80	RPN02 (-34dBm)	Manually	Present@RPN00	39	Off

Check All / Uncheck All
With selected: Delete Repeater(s), Register Repeater(s) Deregister Repeater(s)

PARAMETERS	DESCRIPTION
IDx	Repeater unit identity in the chained network. **Permitted Output:** Positive Integers
RPN	The Radio Fixed Part Number is an 8-bit DECT cell identity allocated by the installer. The allocated RPN within the must be geographically unique. **Permitted Output:** 0 to 255 (DEC) **OR** 0x00 to 0xFF (HEX)
Name/IPEI	Contains the name and the unique DECT serial number of the repeater. If name is given the field will be empty.
DECT sync Source	The “multi cell chain” connection to the specific Base/repeater unit. Maximum number of chain levels is 12. Sync. source format: “RPNyy (-zz dBm)” yy: RPN of source zz: RSSI level seen from the actual repeater
DECT sync Mode	**Manually:** User controlled by manually assign “Repeater RPN” and “DECT sync source RPN” **Local Automatical:** Repeater controlled by auto detects best base signal and auto assign RPN. **Chaining Automatical:** Base controlled by auto detects best base or repeater signal and auto assign RPN. This feature will be supported in a future version
State	Present@unit means connected to unit with RPN yy
FW info	Firmware version
FWU Progress	Possible FWU progress states: **Off:** Means sw version is specified to 0 = fwu is off **Initializing:** Means FWU is starting and progress is 0%. **X% :** FWU ongoing **Verifying X%:** FWU writing is done and now verifying before swap ”**Conn. term. wait**” (Repeater): All FWU is complete and is now waiting for connections to stop before repeater restart. **Complete HS/repeater**: FWU complete **Error:** Not able to fwu e.g. file not found, file not valid etc

STATISTICS

The statistic feature is divided into four administrative web pages, which can be access from any base.

1. System
2. Calls
3. Repeater
4. DECT data

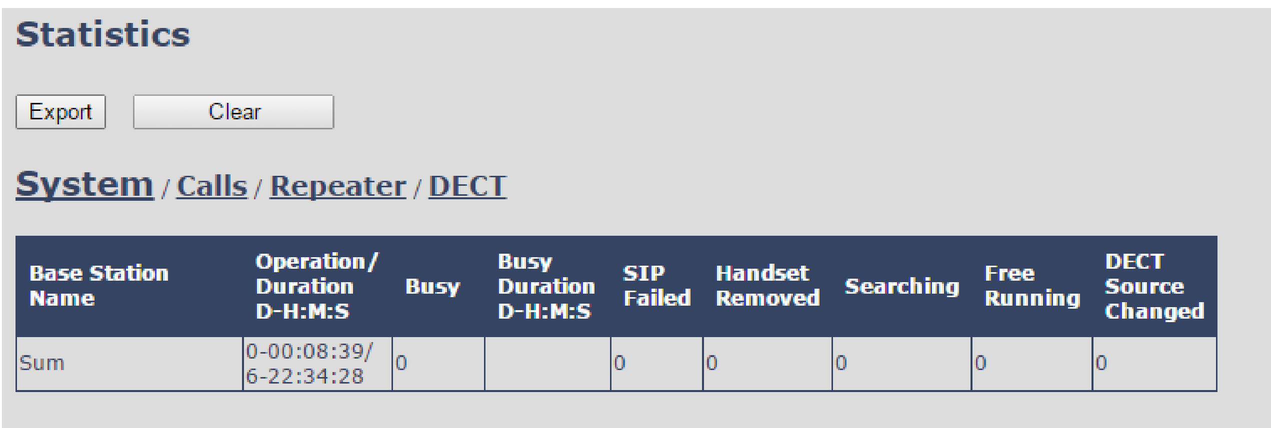
All four views have an embedded export function, which export all data to comma separated file.

By pressing the clear button all data in the full system is cleared.

SYSTEM DATA

The system data web is access by http://ip/SystemStatistics.html and data is organized in a table as shown in below example.

Screenshot



Base Station Name	Operation/ Duration D-H:M:S	Busy	Busy Duration D-H:M:S	SIP Failed	Handset Removed	Searching	Free Running	DECT Source Changed
Sum	0-00:08:39/ 6-22:34:28	0		0	0	0	0	0

The table is organized with headline row, data pr. base rows and with last row containing the sum of all base parameters.

PARAMETERS	DESCRIPTION
Base Station Name	Base IP address and base station name from management settings
Operation time	Total operation time for the base
Busy Count	Busy Count is the number of times the base has been busy.
Busy Duration	Busy duration is the total time a base has been busy for speech (8 or more calls active).
SIP Failed	Failed SIP registrations count the number of times a SIP registration has failed

Handset Removed	Handset removed count is the number of times a handset has been marked as removed
Searching	Base searching is the number of times a base has been searching for it's sync source
Free Running	Base free running is the number of times a base has been free running
DECT Source Changed	Number of time a base has changed sync source

CALL DATA

The call data web is access by http://ip/CallStatistics.html and data are organized in a table as shown in below example.

Screenshot

System / **Calls** / Repeater / DECT

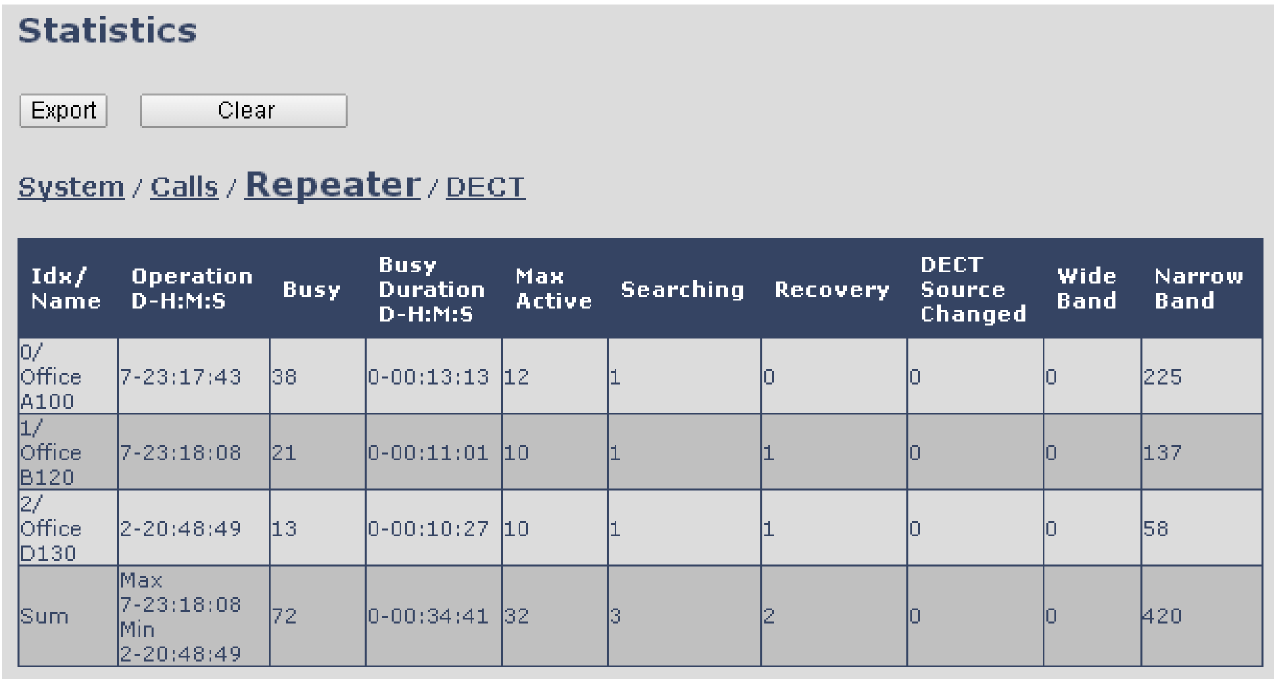
Base Station Name	Operation/ Duration D-H:M:S	Count	Dropped	No Response	Duration D-H:M:S	Active	Max Active	Codec G711U: G711A: G729: G722: G726:	Handover Success	Handover Failed
Sum	0-00:14:12/ 6-22:40:01	7	0	0	0-00:00:31	0	2	0:0:0:3:0	0	0

The table is organized with headline row, data pr. base rows and with last row containing the sum of all base parameters.

PARAMETERS	DESCRIPTION
Base Station Name	Base IP address and base station name from management settings
Operation time/Duration	Total operation time for the base since last reboot or reset Duration is the time from data was cleared or system has been firmware upgraded.
Count	Counts number of calls on a base.
Dropped	Dropped calls are the number of active calls that was dropped. E.g. if a user has an active call and walks out of range, the calls will be counted as a dropped call. An entry is stored in the syslog when a call is dropped.
No response	No response calls is the number of calls that have no response, e.g. if a external user tries to make a call to a handset that is out of range the call is counted as no response. An entry is stored in the syslog when a call is no response.
Duration	Call duration is total time that calls are active on the base.
Active	Active call shows how many active calls that are active on the base (Not active DECT calls, but active calls). On one base there can be up to 30 active calls.
Max Active	Maximum active calls are the maximum number of calls that has been active at the same time.

PARAMETERS	DESCRIPTION
Codecs	Logging and count of used codec types on each call.
Handover Success	Counts the number of successful handovers.
Handover Failed	Counts the number of failed handovers.

REPEATER DATA



Idx/ Name	Operation D-H:M:S	Busy	Busy Duration D-H:M:S	Max Active	Searching	Recovery	DECT Source Changed	Wide Band	Narrow Band
0/ Office A100	7-23:17:43	38	0-00:13:13	12	1	0	0	0	225
1/ Office B120	7-23:18:08	21	0-00:11:01	10	1	1	0	0	137
2/ Office D130	2-20:48:49	13	0-00:10:27	10	1	1	0	0	58
Sum	Max 7-23:18:08 Min 2-20:48:49	72	0-00:34:41	32	3	2	0	0	420

The table is organized with headline row, data pr. base rows and with last row containing the sum of all base parameters.

PARAMETERS	DESCRIPTION
Idx	Base IP address and base station name from management settings
Operation time/Duration	Total operation time for the repeater since last reboot or reset Duration is the time from data was cleared or system has been firmware upgraded.
Busy	Busy Count is the number of times the repeater has been busy.
Busy Duration	Busy duration is the total time a repeater has been busy for speech (5 or more calls active).
Max Active	Maximum active calls are the maximum number of calls that has been active at the same time.
Searching	Repeater searching is the number of times a repeater has been searching for it's sync source
Recovery	In case the sync source is not present anymore the repeater will go into lock on another base or repeater and show recovery mode

DECT Source Changed	Number of time a repeater has changed sync source
Wide Band	Number of wideband calls on repeaters
Narrow Band	Number of narrow band calls on repeaters

DECT DATA

The DECT data web is access by http://ip/DectStatistics.html and data is organized in a table as shown in below example.

Screenshot

Statistics

Export Clear

System / Calls / DECT

	Slot0	Slot1	Slot2	Slot3	Slot4	Slot5	Slot6	Slot7	Slot8	Slot9	Slot10	Slot11
Frequency0	0	0	0	0	0	0	0	0	0	0	0	0
Frequency1	0	0	0	0	0	0	0	0	0	0	0	0
Frequency2	0	0	0	0	0	0	0	0	0	0	0	0
Frequency3	2	3	2	9	4	3	2	3	9	5	3	4
Frequency4	4	7	5	1	5	3	3	6	4	3	4	4
Frequency5	6	0	2	2	1	5	5	2	4	3	5	6
Frequency6	3	3	7	3	4	3	4	5	4	4	3	2
Frequency7	5	2	4	3	4	4	2	4	1	5	3	3
Frequency8	3	1	3	2	2	1	4	2	3	2	2	1
Frequency9	3	3	4	7	8	7	7	2	5	3	2	6

Please note that frequencies 0, 1 and 2 were manually removed in the example above.

SETTINGS – CONFIGURATION FILE SETUP

This page provides non editable information showing the native format of entire VoIP Configuration parameter settings. The **settings** format is exactly what is used in the configuration file. The configuration file is found in the TFTP server.

The filename for the configuration server is **<MAC_Address>.cfg**. The configuration file is saved in the folder **/Config** in the TFTP sever.

There are three ways to edit the configuration file or make changes to the **settings** page:

1. Using the VoIP Configuration interface to make changes. Each page of the HTTP web interface is a template for which the user can customise settings in the configuration file.
2. Retrieving the relevant configuration file from the TFTP and modify and enter new changes. This should be done with an expert network administrator.
3. Navigate to the settings page of the VoIP Configuration interface > copy the contents of settings > save them to any standard text editor e.g. notepad > modify the relevant contents, make sure you keep the formatting intact > Save the file as **<Enter_MAC_Address_of_RFP>.cfg** > upload it into the relevant TFTP server.

An example of contents of settings is as follows:

```
~RELEASE=UMBER_FP_V0054
%GMT_TIME_ZONE%:16
%COUNTRY_VARIANT_ID%:18
%FWU_POLLING_ENABLE%:0
%FWU_POLLING_MODE%:0
%FWU_POLLING_PERIOD%:86400
%FWU_POLLING_TIME_HH%:3
%FWU_POLLING_TIME_MM%:0
%DST_ENABLE%:2
%DST_FIXED_DAY_ENABLE%:0
%DST_START_MONTH%:3
%DST_START_DATE%:1
....
....
```

SYS LOG

This page shows live feed of system level messages of the current base station. The messages the administrator see here depends on what is configured at the Management settings. The Debug logs can show only **Boot Log** or **Everything** that is all system logs including boot logs.

The Debug log is saved in the file format **<Time_Stamp>b.log** in a relevant location in the TFTP server as specified in the upload script.

A sample of debug logs follows:

```
0101000013 [N](01):DHCP Enabled
0101000013 [N](01):IP Address: 192.168.10.101
0101000013 [N](01):Gateway Address: 192.168.10.254
0101000013 [N](01):Subnet Mask: 255.255.255.0
0101000013 [N](01):TFTP boot server not set by DHCP. Using Static.
0101000013 [N](01):DHCP Discover completed
0101000013 [N](01):Time Server: 192.168.10.11
0101000013 [N](01):Boot server: 10.10.104.63 path: Config/ Type:
TFTP
0101000013 [N](01):RemCfg: Download request of
Config/00087b077cd9.cfg from 10.10.104.63 using TFTP
0101000014 [N](01):accept called from task 7
0101000014 [N](01):TrelAccept success [4]. Listening on port 10010
0101000019 [N](01):RemCfg: Download request of
Config/00087b077cd9.cfg from 10.10.104.63 using TFTP
0101000019 [W](01):Load of Config/00087b077cd9.cfg from 10.10.104.63
failed
```

To dump the logs, simply copy and paste the full contents.

SIP LOGS

This page shows SIP server related messages that are logged during the operation of the system. The full native format of SIP logs is saved in the TFTP server as **<MAC_Address><Time_Stamp>SIP.log**

These logs are saved in 2 blocks of 17Kbytes. When a specific SIP log is fully dumped to one block, the next SIP logs are dumped to the other blocks. An example of SIP logs is shown below:

```
.....
Sent to udp:192.168.10.10:5080 at 12/11/2010 11:56:42  (791 bytes)
REGISTER sip:192.168.10.10:5080 SIP/2.0
Via: SIP/2.0/UDP
192.168.10.101:5063;branch=z9hG4bKrlga4nkuhimpnj4.qx
Max-Forwards: 70
From: <sip:Ext003@192.168.10.10:5080>;tag=3o5l314
To: <sip:Ext003@192.168.10.10:5080>
Call-ID: p9st.zzrfff66.ah8
CSeq: 6562 REGISTER
Contact: <sip:Ext003@192.168.10.101:5063>
Allow: INVITE, CANCEL, BYE, ACK, REGISTER, OPTIONS, REFER,
SUBSCRIBE, NOTIFY, MESSAGE, INFO, PRACK
Expires: 120
User-Agent: Generic-DPV-001-A-XX(Generic_SIPEXT2MLUA_v1)
Content-Type: application/X-Generic_SIPEXT2MLv1
Content-Length: 251
.....
```

To dump the log simply copy and page the full contents.

FIRMWARE UPGRADES

DOWNLOAD FIRMWARE FILES

STEP 1 Log into Mitel Connect (https://connect.mitel.com/connect/).

STEP 2 Access Mitel Online.

STEP 3 Under **Support**, click **Software Downloads**, and then click **IP DECT**.

STEP 4 Download the ZIP file of the firmware files.

UPGRADE THE FIRMWARE

This procedure describes how to upgrade the base station and handset firmware. You can also use this procedure to upgrade the repeater firmware.

Note: In the following example, the TFTP server is running on a PC.

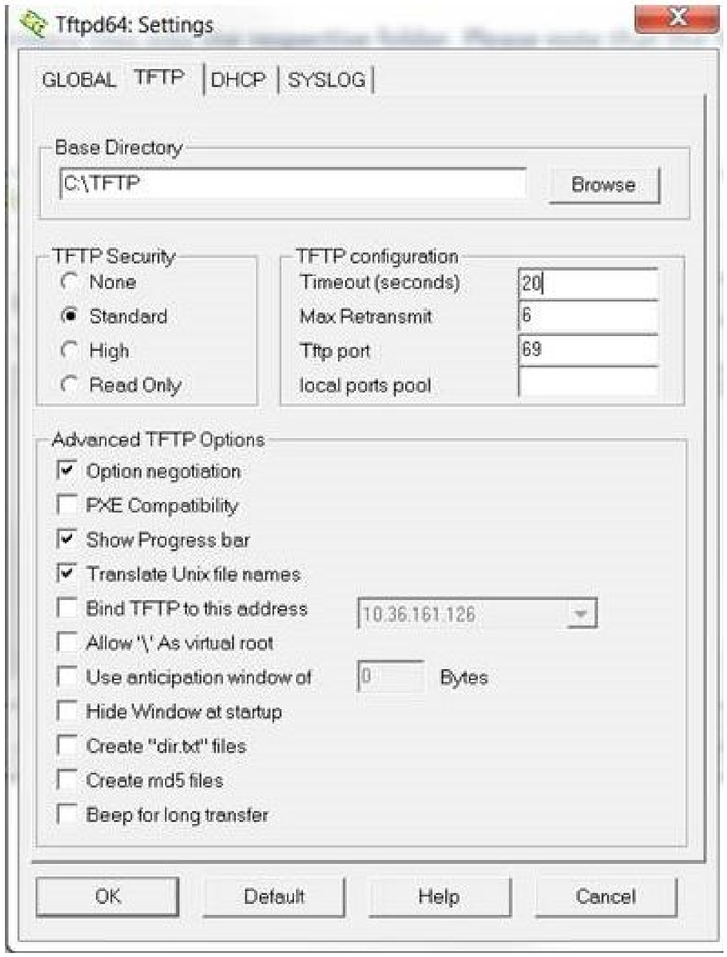
STEP 1 Create a folder on the tftp server for the firmware files. For example:

- C:\TFTP\9430\
- C:\TFTP\8430\

STEP 2 Copy the firmware files into their respective folders. The 9430 folder is for the base station and the 8430 folder is for the handset:

- C:\TFTP\9430\9430_v0355_b0004.fwu
- C:\TFTP\8430\8430_v0355_b0004.fwu

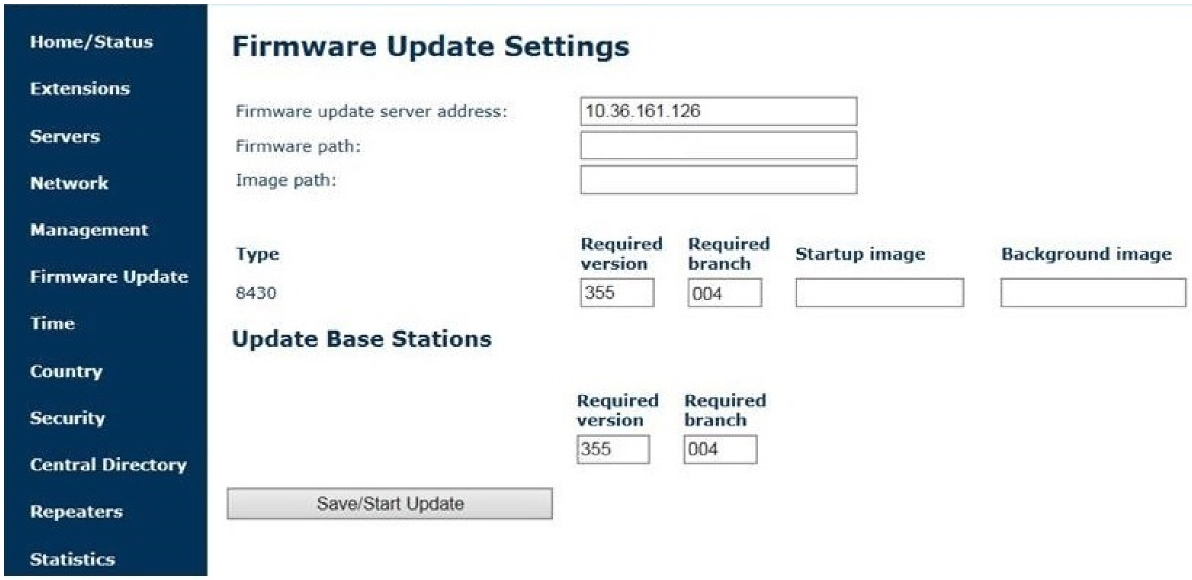
STEP 3 In the TFTP server settings, enter C:\TFTP in the Base Directory field and change the Timeout to 20 seconds.



STEP 3 Login to the Mitel 112 DECT base station management interface.

STEP 4 Click **Firmware Update**.

- In the Firmware update server address field, enter the IP address of the TFTP server.
- Leave the Firmware path blank.
- Leave the Image path field blank.
- Set the Required version field to the last three digits of the file version. For example, for firmware file 9430_v0355_b0004.fwu, enter 355.
- Set the Required branch field. For example, for firmware file 9430_v0355_b0004.fwu, enter 004.



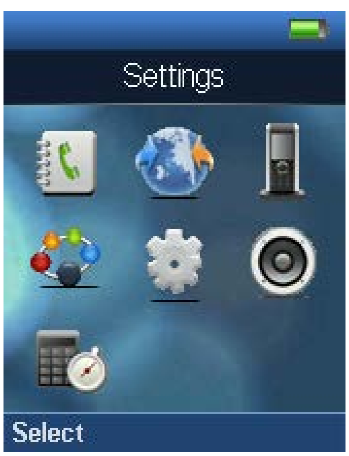
STEP 5 Click **Save/Start Update**.

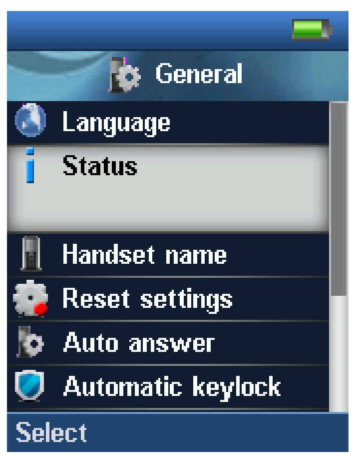
STEP 6 Monitor the log on the TFTP server to confirm that the file transfer is taking place. The Base LED starts flashing (orange, then red, then solid green). The Base station performs its upgrade first. Then, the phone firmware is transferred and the handset is upgraded.

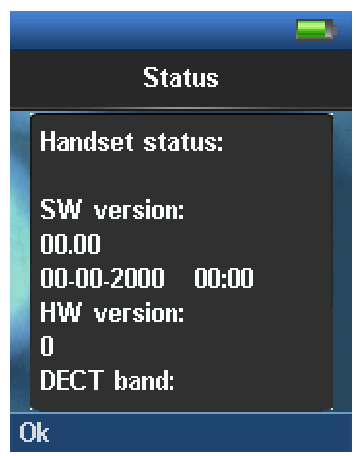
VERIFICATION OF FIRMWARE UPGRADE

The firmware upgrade is confirmed by the FWU Progress status in the second and first right column on the handset extension list or repeater list. The “FWU info” column contains the software version and the “FWU Progress” column contains the status. In case status is “Complete”, the unit is firmware upgraded.

Alternatively the handset firmware can be verified from the Handset **Menu** by navigate to **Settings** > Scroll down to **Status** this will list information regarding Base station and Handset firmware versions.







FUNCTIONALITY OVERVIEW

So far we have set up our system. Next, in this chapter we list what features and functionalities are available in the system. The System supports all traditional and advanced features of most telephony networks. In addition, 3rd party components handle features like voice mail, call forward, conference calls, etc. A brief description of VOIP network functionalities are:

- **Outgoing/incoming voice call management:** The System can provide multiple priority user classes. Further, up to 3 repeaters can be linked to a Base-station.
- **Internal handover**: User locations are reported to SIP Server in order to provide differentiated services and tariff management. Within a DECT traffic area, established calls can seamlessly be handover between Base-station and repeaters using connection handover procedures.
- **Security:** The RTX System also supports robust security functionalities for Base-station. Most security[1] functionality is intrinsically woven into the VOIP network structure so that network connections can be encrypted and terminal authentication can be performed.
- **Hospitality**: For Hotel/Motel environments you can apply the following system behaviors by enabling the **Hotel Mode** setting in **Management Settings** page of the of the IP DECT web configuration interface:
    - Black out the handset display when placed in cradle (after 65 seconds)
    - Protect the handset **Settings** menu (changes default handset PIN from 0000 to 9351 and the PIN is required to access the **Settings** menu)
    - Enable silent upgrades and resets
    - Disable call logging
    - Prevent phonebook modification.

BASE STATION INTERFACES

Interfaces	
Power	Input: 100-240 VAC 50-60Hz (90 – 265 VAC) Output Nom: 5VDC 1000mA Type: Switch mode single or multi-plug solution Plugs: UK, EU, US and AUS
LAN Interface	Standard : 10BASE-T(IEEE 802.3 100Mbps) Connector: RJ45 8/8
Keys	
	1: Reset key, Page and Default
LED indicator	
	One Status LED (multicolour, red, green, orange)

[1] With active security 4 channels is supported

RF	
Frequency Bands	1880 – 1900 MHz (EMEA) 1910 – 1930 MHz (Latam) 1920 – 1930 MHz (USA) Factory setting which can't be modified after production
Output Power	250 mW or 140mW depending on country version
Antenna	Two antennas for diversity
Software upgrade	
Downloadable	Remote firmware update using HTTP, HTTPS or TFTP
Temperatures	
Operation	0˚C to 40˚C

SOFTWARE FEATURES

CODEC's	
G.711 PCM A-law & U-law	Yes
G.722	Yes
G.726	Yes
G.729	A/AB (including VAD), max 4 coders G729 licence not included
SIP	
RFC2327	SDP: Session Description Protocol
RFC2396	Uniform Resource Identifiers (URI): Generic Syntax
RFC2833	In-Band DTMF/Out of band DTMF support
RFC2976	The SIP INFO method
RFC3261	SIP 2.0
RFC3262	Reliability of Provisional Responses in the Session Initiation Protocol (PRACK)
RFC3263	Locating SIP Servers (DNS SRV, redundant server support)
RFC3264	Offer/Answer Model with SDP
RFC3265	Specific Event Notification
RFC3326	The Reason Header Field for the Session Initiation Protocol
RFC3311	The Session Initiation Protocol UPDATE Method
RFC3325	P-Asserted Identity

RFC3326	The Reason Header Field for the Session Initiation Protocol (SIP)
RFC3489	STUN
RFC3515	REFER: Call Transfer
RFC3550	RTP: A Transport Protocol for Real-Time Application
RFC3581	Rport
RFC3842	Message Waiting Indication
RFC3891	Replace header support
RFC3892	The Session Initiation Protocol (SIP) Referred-By Mechanism
RFC3960	Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
RFC4475	Session Initiation Protocol (SIP) Torture Test Messages
SIPS	Secure SIP
In-band DTMF	No
SRTP	Yes, packet authentication will limit the number of calls to 4
SIP registrations	max 20
RTP streams	max 10
SIP transport	UDP, TCP or TLS
Web server	
	Embedded web server, accessed using HTTP
Other features	
IP quality	Warning – Network outage, VoIP service outage
Jitter buffer	Yes, adaptive
Automatic DST	Yes
Tone Scheme	Country Depend Tone Scheme
Provisioning	Yes
Re-direct server	Yes
SIP configuration	Yes, from web page or configuration file
Call groups	Yes
IP features	
IPv4	Yes
IPv6	Hardware ready, software not included
TCP/IP/UDP	Yes
DHCP Support	Yes

DHCP option	66, 120
Static IP	Yes
DNS srv	Yes
VLAN	Yes, 802.1p/q
Quality of service	Type of Service (ToS) including DiffServ Tagging, and QoS per IEEE 802.1p/q
TLS	Yes, 1.0
Certificates	Yes, X.509 (certificate not included)
TFTP	Yes, for firmware and configuration file download
HTTP server	Yes
HTTP client	Yes, for firmware and configuration file download
HTTPS	Yes, for firmware and configuration file download
SNTP	Yes, For internet clock synchronization
DECT	
DECT handover	Yes, inter-cell handover for repeater support
CAT-IQ v1.0	HD audio or NB audio support
Repeater support	Yes
Intercom	No
DECT encryption	Yes
DECT Authentication	Yes
Group TPUI support	Yes, for call groups
GAP compliant	No
CAT-IQ compliant	No
Handset registrations	20

CALL FEATURES

Call supported	5 simultaneous call supported
Simultaneous calls/base	5 Wideband calls (g.722). 5 narrowband calls (PCMA, PCMU, G.726) or 4 when using G729
Simultaneous calls/handset	2
Call features	Codec Negotiation
	Codec Switching
	Missed call notification

	Voice mssage waiting notification
	Date and Time synchronization
	Parallel calls
	Call Hold
	Call Retrieve
	Call transfer unannounced
	Call transfer announced
	Conference (3PTY)
	Conference, Network
	Call Waiting Indication
	Calling line identity
	Outgoing call
	Call Toggle/Swap
	Incoming call
	Line identification
	Multiple Lines
	Multiple calls
	Call identification
	Calling Name Identification Presentation (CNIP)
	Calling Line Identification Presentation (CLIP)
	Call Completed Elsewhere
	Distinctive Ringing
Central Phone Book:	
- LDAP	Yes
- XML	Yes, remote or file load from web interface
- CSV	Yes, file load through web interface
DND:	Yes
Call Forward:	Configurable from base or handset (Not with Call Group active))
- CFU	Yes
- CFNA	Yes
- CFB	Yes

Call groups:	Yes, 1-20 handsets/SIP account

APPENDIX A: BASIC NETWORK SERVER(S) CONFIGURATION

In this chapter we describe how to setup the various server elements in the system.

SERVER SETUP

In the network, the server environment is installed as a centralized system.

The main server types hosted on the network include SIP, DNS/DHCP and HTTP/TFTP Servers. These servers can be hosted both in one or multiple windows and/or Linux Server environment.

Management servers are normally installed to monitor and manage the network in detail. Each Base-station status can be checked. Each Repeater and each Subscriber Terminal can be monitored over the air from a centralized location.

Further, new software can be uploaded to all system elements from the centralized location (typically a TFTP server) on an individual basis. This includes Subscriber Handsets where the latest software is downloaded over the air.

REQUIREMENTS

Regardless of whether or not you will be installing a centrally provisioned system, you must perform basic TCP/IP network setup, such as IP address and subnet mask configuration, to get your organization’s phones up and running.

DNS SERVER INSTALLATION/SETUP

Name server is a name server service installed in a server for mapping or resolution of humanly memorable domain names and hostnames into the corresponding numeric Internet Protocol (IP) addresses.

The customer should refer to the platform vendor either windows or Linux vendor for detail step-by-step guide on how to install and configure Domain Name System for internet access. In this section, we briefly describe hints on how to setup DNS behind NAT or Firewall.

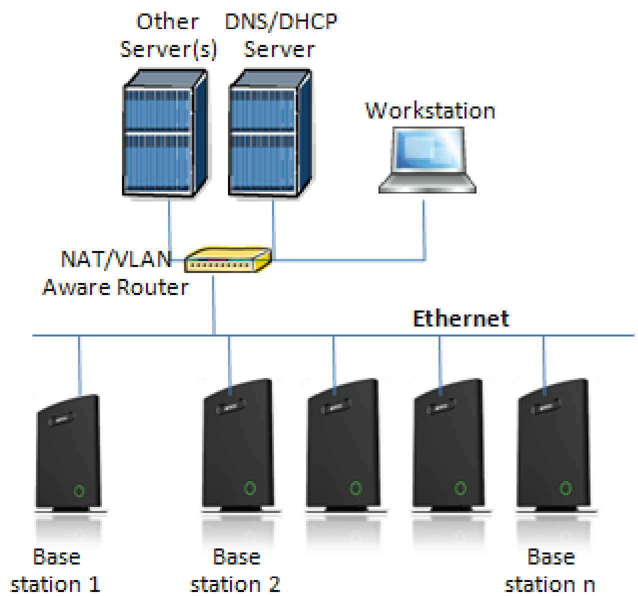
Hints on how to Configure DNS behind a Firewall/NAT

Proxy and Network Address Translation (NAT) devices can restrict access to ports. Set the DNS to use UDP port 53 and TCP port 53. For windows Servers, set the RCP option on the DNS Service Management console and configure the RCP to use port 135.

These settings should be enough to resolve some of potential issues that may occur when you configure DNS and firewalls/NAT.

DHCP SERVER SETUP

A DHCP Server allows diskless clients to connect to a network and automatically obtain an IP address. This server is capable of supplying each network client with an IP address, subnet mask, default gateway, an IP address for a WINS server, and an IP address for a DNS server. This is very often used in enterprise networks to reduce configuration efforts. All IP addresses of all computers/routers/bases are stored in a database that resides on a server machine.



The network administrator should contact the relevant vendors for detail information or step-by-step procedure on how to install and setup DHCP process or service on windows/Linux servers. In this section, we will provide some hints of how to resolve potential problems to be encountered you setup DHCP Servers.

DHCP SERVER TROUBLESHOOTING

Windows Server:

1. **Clients are unable to obtain an IP address**
   If a DHCP client does not have a configured IP address; it generally means that the client has not been able to contact a DHCP server. This is either because of a network problem or because the DHCP server is unavailable. If the DHCP server has started and other clients have been able to obtain a valid address, verify that the client has a valid network connection and that all related client hardware devices (including cables and network adapters) are working properly.

2. **The DHCP server is unavailable**
   When a DHCP server does not provide leased addresses to clients, it is often because the DHCP service has failed to start. If this is the case, the server may not have been authorized to operate on the network. If you were previously able to start the DHCP service, but it has since stopped, use Event Viewer to check the system log for any entries that may explain the cause.

Next, restart the DHCP service, click **Start**, click **Run**, type **cmd**, and then press ENTER. Type **net start dhcpserver**, and then press ENTER.

Linux Platform:

Troubleshooting DHCP, check the following:

1. Incorrect settings in the **/etc/dhcpd.conf** file such as not defining the networks for which the DHCP server is responsible;
2. NAT/Firewall rules that block the DHCP **bootp** protocol on UDP ports 67 and 68;
3. Routers failing to forward the **bootp** packets to the DHCP server when the clients reside on a separate network. Always check your /var/logs/messages file for dhcpd errors.
4. Finally restart the **dhcpd** service daemon

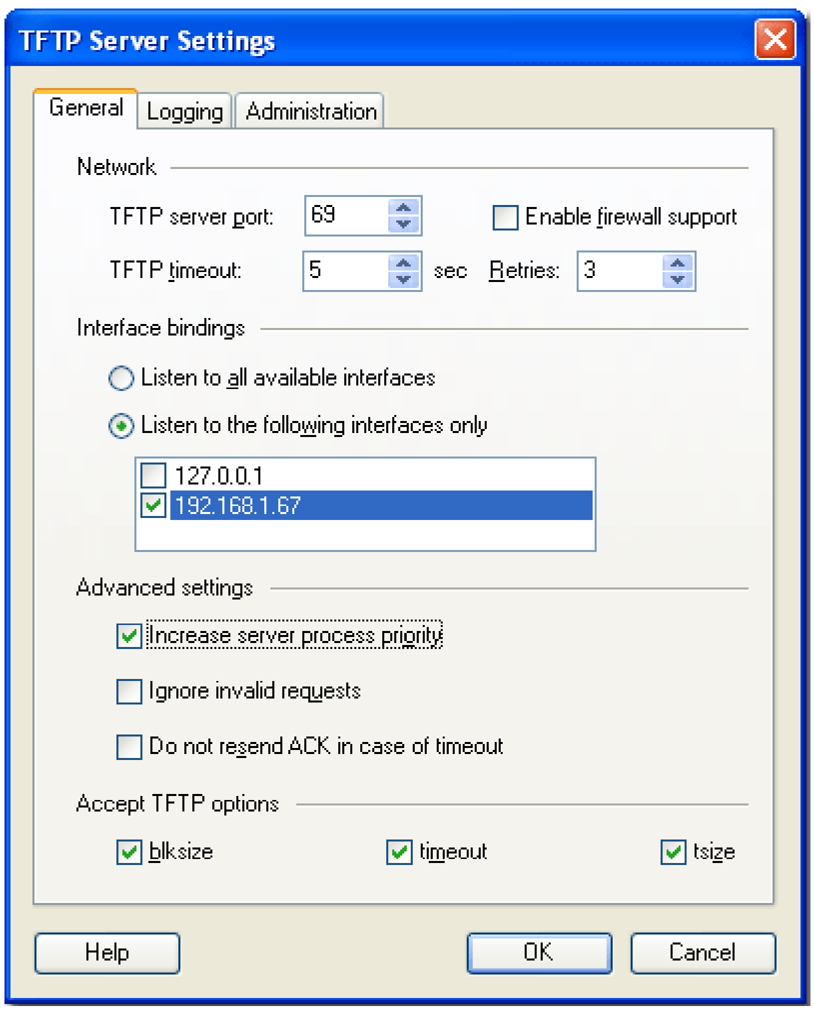
TFTP SERVER SETUP

There are several TFTP servers in the market place; in this section we describe how to setup a commonly used TFTP Server.

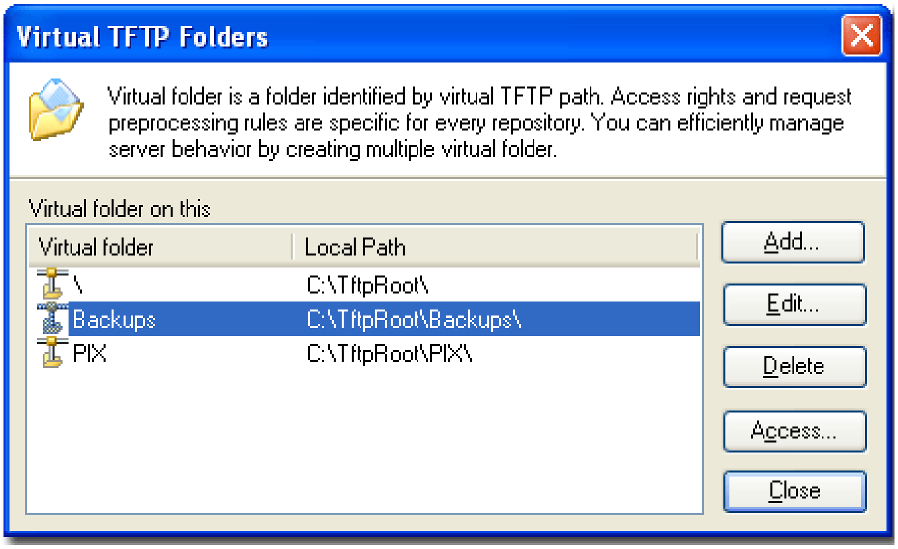
TFTP SERVER SETTINGS

The administrator must configure basic parameters of the TFTP application:

- Specify UDP 69 port – for TFTP incoming requests and TCP 12000 – for remote management of the server. For file transmission the server opens UDP ports with random numbers. In case the option **Enable NAT or firewall support** is activated on the server, the server uses the same port for files transmission and listening to the TFTP incoming requests (UDP 69 port on default).
- Specify the interface bindings, TFTP root directory, port which the TFTP Server will listen, timeout and number of retries, and TFTP options supported by the server.



- Configure the relevant TFTP virtual folder in the server. The TFTP virtual folder is the file folder, visible for TFTP clients under a certain name. You can set security settings separately for every virtual TFTP folder. Next, set rights to access TFTP folders according to the relevant clients.


Virtual TFTP Folders
Virtual folder is a folder identified by virtual TFTP path. Access rights and request preprocessing rules are specific for every repository. You can efficiently manage server behavior by creating multiple virtual folder.
Virtual folder on this
Virtual folder
Local Path
\
C:\TftpRoot\
Backups
C:\TftpRoot\Backups\
PIX
C:\TftpRoot\PIX\
Add...
Edit...
Delete
Access...
Close

APPENDIX B: USING BASE WITH VLAN NETWORK

In this chapter we describe how to setup a typical VLAN in the network.

INTRODUCTION

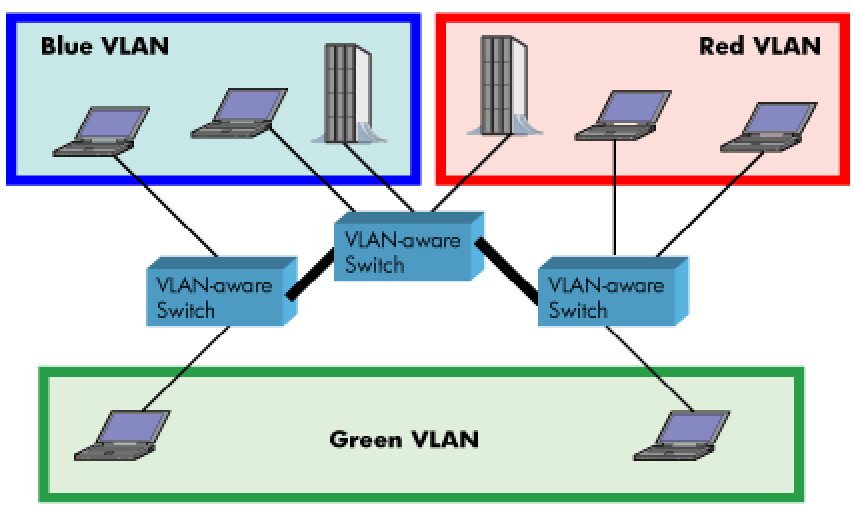
In this chapter, we describe how to setup VLAN to typical network. There are three main stages involved in this procedure:

1. Configure a VLAN Aware Switch to a specific (un)tagged VLAN ID, so the system can process untagged frames forwarded to it.
2. Setup the Time Server (NTP Server) and other relevant network servers.
3. Configure the HTTP server in the Base station to access the features in the PBX or system.

VLAN allows administrators to separate logical network connectivity from physical connectivity analogous to traditional LAN which is limited by its physical connectivity. Normally, users in a LAN belong to a single broadcast domain and communicate with each other at the Data Link Layer or “Layer 2”. LANs are segmented into smaller units for each IP subnets and here communication between subnets is possible at the Network Layer or “Layer 3”, using IP routers.

A VLAN can be described as a single physical network that can be logically divided into discrete LANs that can operate independently of each other.

An Illustration of using VLANs to create independent broadcast domains across switches is shown below:



The figure above highlights several key differences between traditional LANs and VLANs.

- All switches are interconnected to each other. However, there are three different VLANs or broadcast domains on the network. Physical isolation is not required to define broadcast domains. If the figure was a traditional LAN without VLAN-aware switches, all stations would belong to one broadcast domain.

- All switch ports can communicate with one another at the Data Link Layer, if they become members of the same VLAN.
- The physical location of an end station does not define its LAN boundary.
  1. An end station can be physically moved from one switch port to another without losing its "view of the network". That is, the set of stations it can communicate with at the Data Link Layer remains the same, provided that its VLAN membership is also migrated from port to port.
  2. By reconfiguring the VLAN membership of the switch port an end station is attached to, you can change the network view of the end station easily, without requiring a physical move from port to port.

BACKBONE/ VLAN AWARE SWITCHES

To implement a VLAN in your network, you must use VLAN-aware switches.

Before we continue, let consider two rules to remember regarding the functioning of a regular LAN switch:

1. When the switch receives a broadcast or multicast frame from a port, it floods (or broadcasts) the frame to all other ports on the switch.

2. When the switch receives a unicast frame, it forwards it only to the port to which it is addressed.

A VLAN-aware switch changes the above two rules as follows:

1. When the switch receives a broadcast or multicast frame from a port, it floods the frame to only those ports that belong to the same VLAN as the frame.

2. When a switch receives a unicast frame, it forwards it to the port to which it is addressed, only if the port belongs to the same VLAN as the frame.

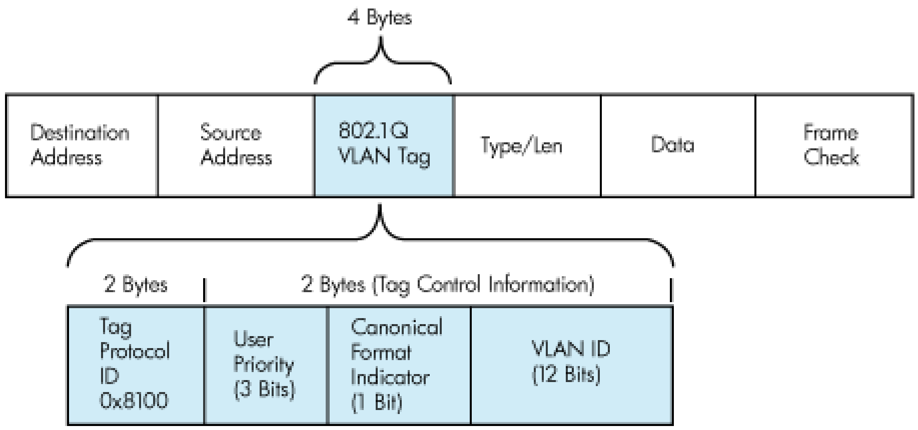
3. A unique number called the VLAN ID identifies each VLAN.

Which VLAN Does a Frame Belong To?

The previous section notes that a frame can belong to a VLAN. The next question is—how is this association made?

- A VLAN-aware switch can make the association based on various attributes of the type of frame, destination of MAC address, IP address, TCP port, Network Layer protocol, and so on.

An illustration of IEEE 802.1Q VLAN tag in Ethernet frame is as follows:



HOW VLAN SWITCH WORK: VLAN TAGGING

VLAN functionality can be implemented via explicit frame tagging by switches and end stations. Network switches and end stations that know about VLANs are said to be VLAN aware. Network switches and end stations that can interpret VLAN tags are said to be VLAN tag aware. VLAN-tag-aware switches and end stations add VLAN tags to standard Ethernet frames–a process called explicit tagging. In explicit tagging, the end station or switch determines the VLAN membership of a frame and inserts a VLAN tag in the frame header (see figure above for VLAN tagging), so that downstream link partners can examine just the tag to determine the VLAN membership.

IMPLEMENTATION CASES

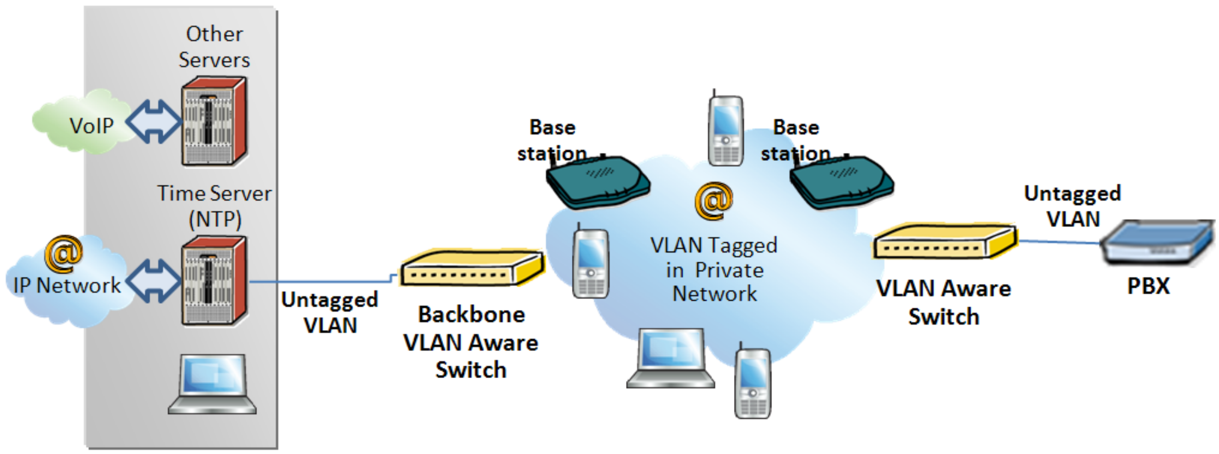
Common types of usage scenarios for VLANs on typical VLAN switches: port-based VLANs, protocol-based VLANs, and IP subnet-based VLANs. Before figuring out which usage scenario suits your needs, you must understand what each type of usage scenario implies.

- **Port-based VLAN:** All frames transmitted by a NIC are tagged using only one VLAN ID. The NIC does not transmit or receive any untagged frames.

  All protocols and applications use this virtual interface's virtual PPA to transmit data traffic. Therefore all frames transmitted by that NIC port are tagged with the VLAN ID of that Virtual Interface.

- **Protocol-based VLAN**: The NIC assigns a unique VLAN ID for each Layer 3 protocol (such as IPv4, IPv6, IPX, and so on). Therefore, the VLAN ID of outbound frames is different for each protocol. An inbound frame is dropped if the protocol and VLAN ID do not match.

- **IP subnet-based VLAN:** The NIC assigns a unique VLAN ID for each IP subnet it belongs to. Therefore, the VLAN ID of outbound frames is different for different destination subnets. An inbound frame is dropped if the IP subnet and VLAN ID do not match.



BASE STATION SETUP

After the admin have setup the Backbone switch, next is to configure the Base station via HTTP interface.

STEP 1 Connect the Base station to a private network via standard Ethernet cable (CAT-5).

STEP 2 Use one of the two methods to find the base IP

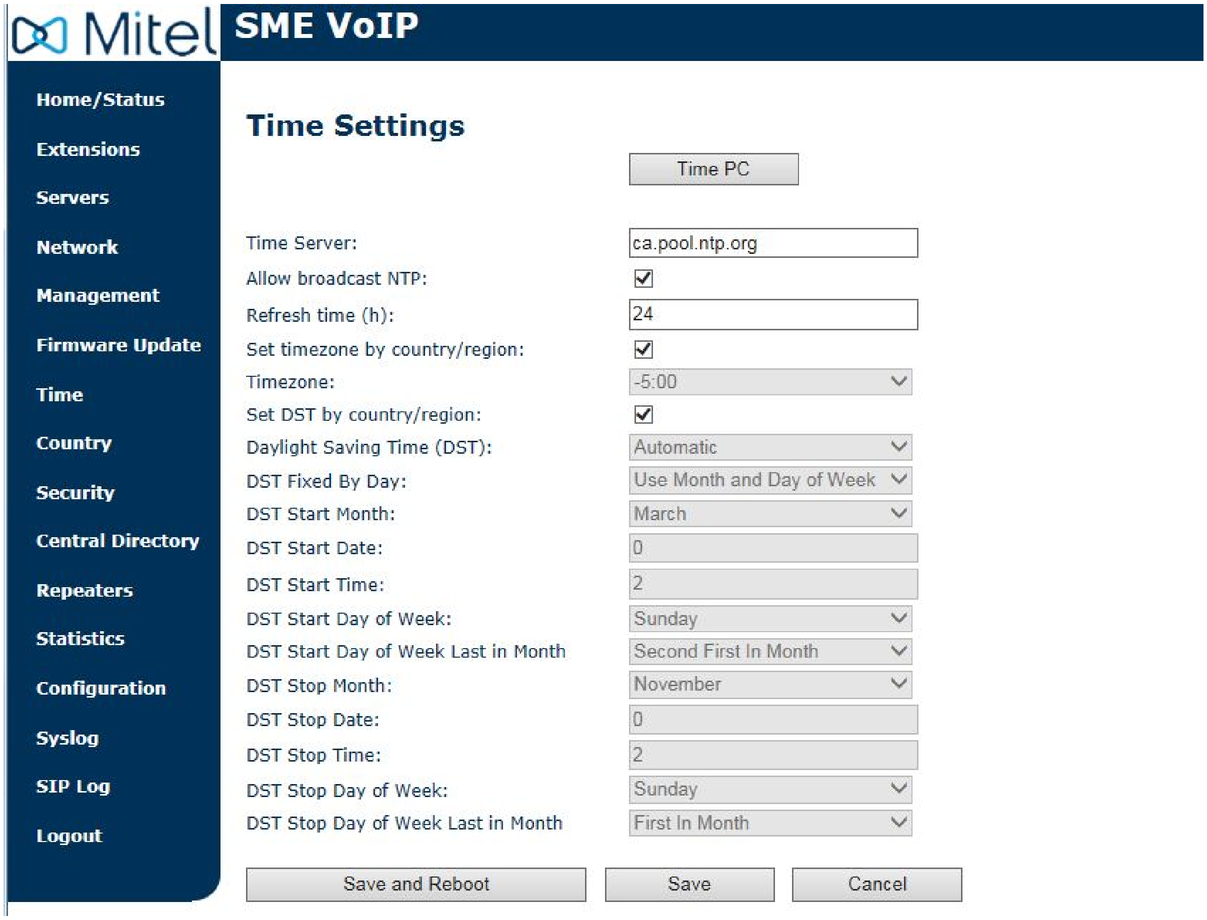
STEP 3 On the Login page, enter your authenticating credentials (the username and password is admin by default unless it is changed). Click OK button.

STEP 4 Once you have authenticated, the browser will display front end of the Configuration Interface. The front end will show relevant information of the base station.

STEP 5 Create the relevant SIP server information in the system. Each service provider/customer should refer SIP server vendor on how to setup SIP servers.

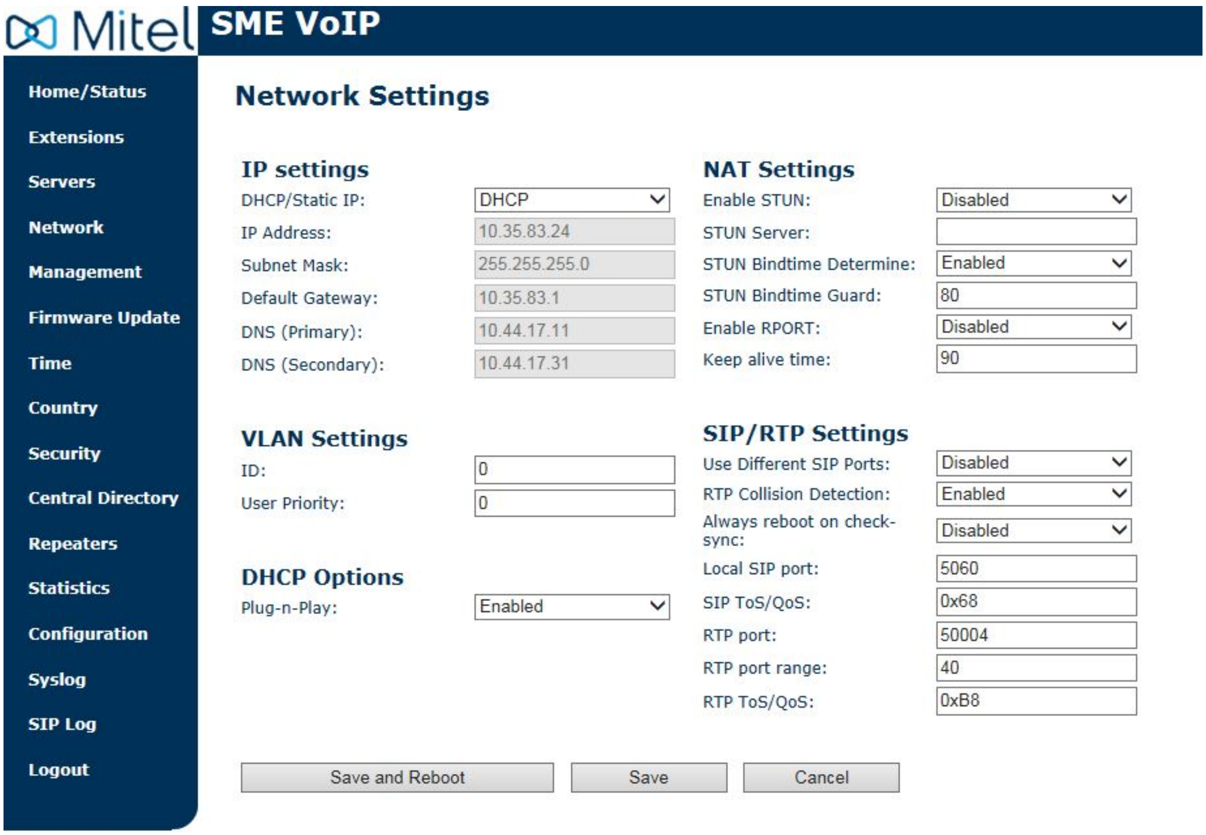
CONFIGURE TIME SERVER

STEP 6 Navigate to the Time settings and configure it. Scroll on the left column and click on **Time** url link to Open the **Time Settings** Page. Enter the relevant parameters on this page and press the **Save** button.



VLAN SETUP: BASE STATION

STEP 7 Navigate to the **Network** url > On the network page enter the relevant settings in the VLAN section > VLAN Id should be the same as those configured into the backbone.



APPENDIX C: LOCAL CENTRAL DIRECTORY FILE HANDLING

This appendix the Local Central Directory file format, import and configuration is described.

CENTRAL DIRECTORY CONTACT LIST STRUCTURE

The structure of Contact List is simple. The figure below shows an example of structure of Contact List in Text format and in Xml format. ***Contact name must not contain more than 23 characters and contact number must not contain more than 21 digits.***

.csv or **.txt**

File Edit Format View Help

```
Dennis Iversen,+4596322382
Torsten Krogh Elgaard,2381
Rune Thor Jensen,2445
Maija-Liisa Knudsen,2377
Jesper Jensen,2346
Kristian Kjaer,2447
Gitte Dyhr Petersen,2470
Sukesh Reddy,2749
Morten Fredegod,4726
Annemarie Dahl,2861
Hans Back,2721
Henrik Olsen,2733
Jens Martin Jensen,2782
Kenneth Skiveren,2363
Lars Christensen (RTX),2433
```

.xml

File Edit Format View Help

```
<IPPhoneDirectory>
<DirectoryEntry>
<Name>Mark Ross</Name>
<Telephone>100</Telephone>
<Office>+450123456789</Office>
<Mobile>+451123456789</Mobile>
<Fax>+452123456789</Fax>
</DirectoryEntry>
</IPPhoneDirectory>
```

.txt file limitations:

- Contact name must NOT be longer than 23 characters (name will be truncated)
- Contact name must NOT contain “,”
- Contact number must be limited to 21 digits (entry will be discarded, no warning)
- Contact number digits must be: +0123456789
- Contact number does not support SIP-URI
- Spaces between name section “,” and number section is not supported

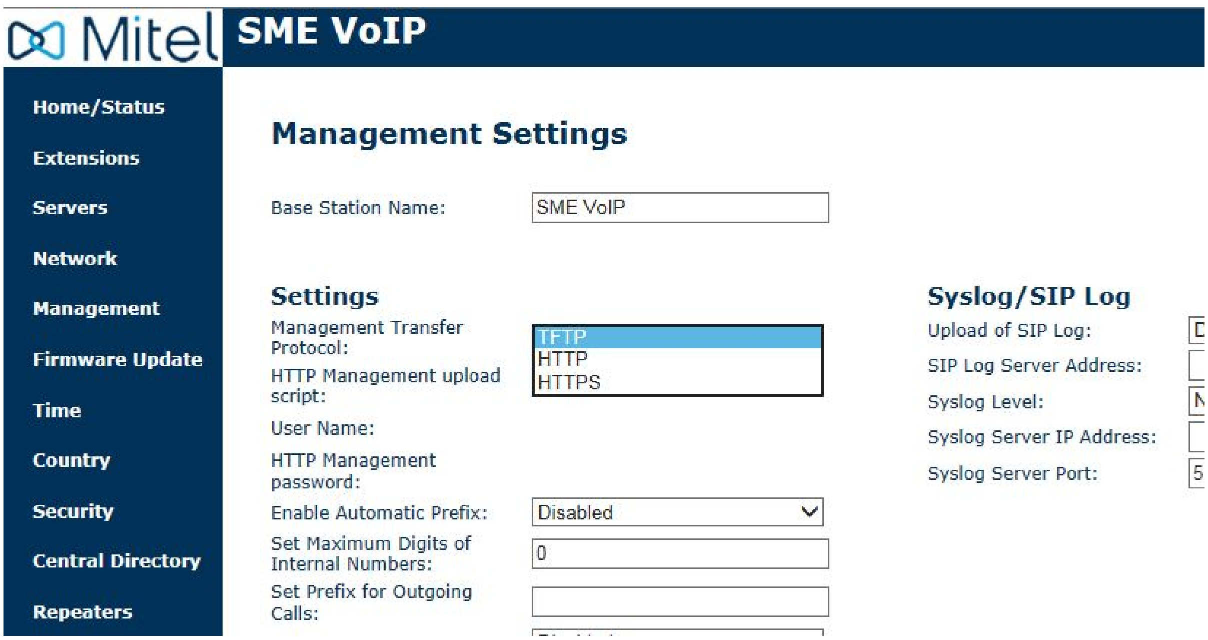
CENTRAL DIRECTORY CONTACT LIST FILENAME FORMAT

The Contact list is saved as file format: **.txt .csv** or **.xml**

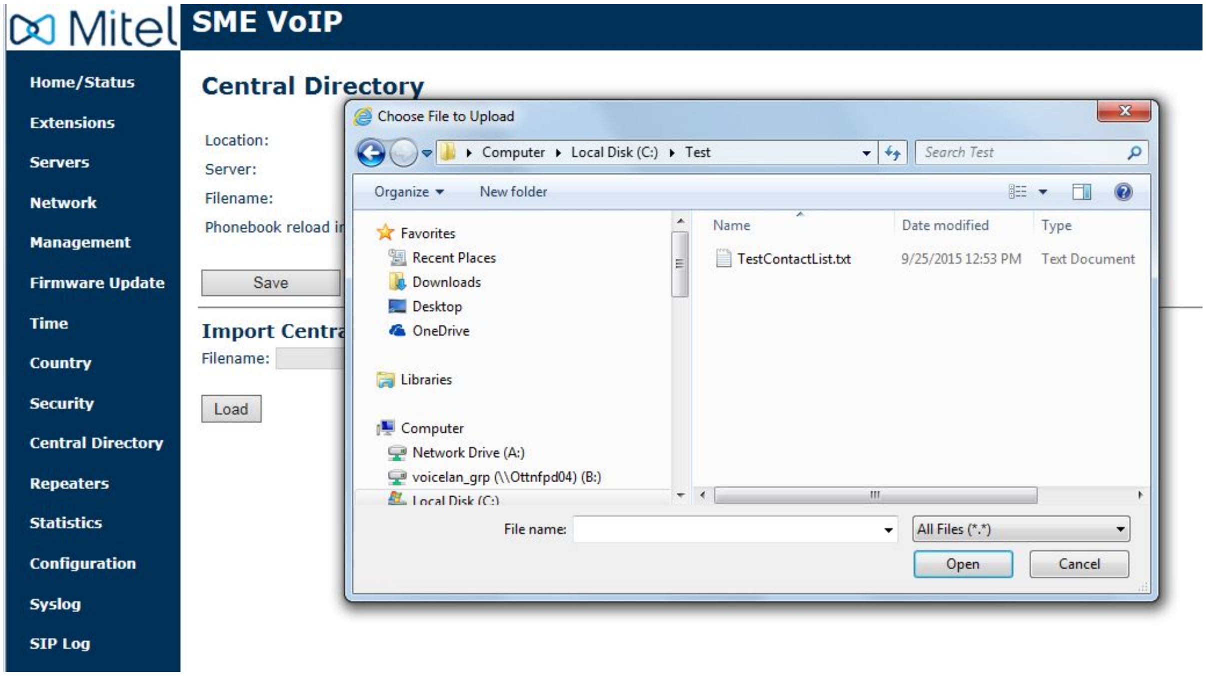
IMPORT CONTACT LIST TO CENTRAL DIRECTORY

On the **Central Directory** page, the admin should click on **Browse** button and the **Choose File to Load** dialog window will be shown.

On the **Choose File to Upload** dialog window, navigate to the directory or folder that contains the right file to be imported to the base station > Click on **Open** button.



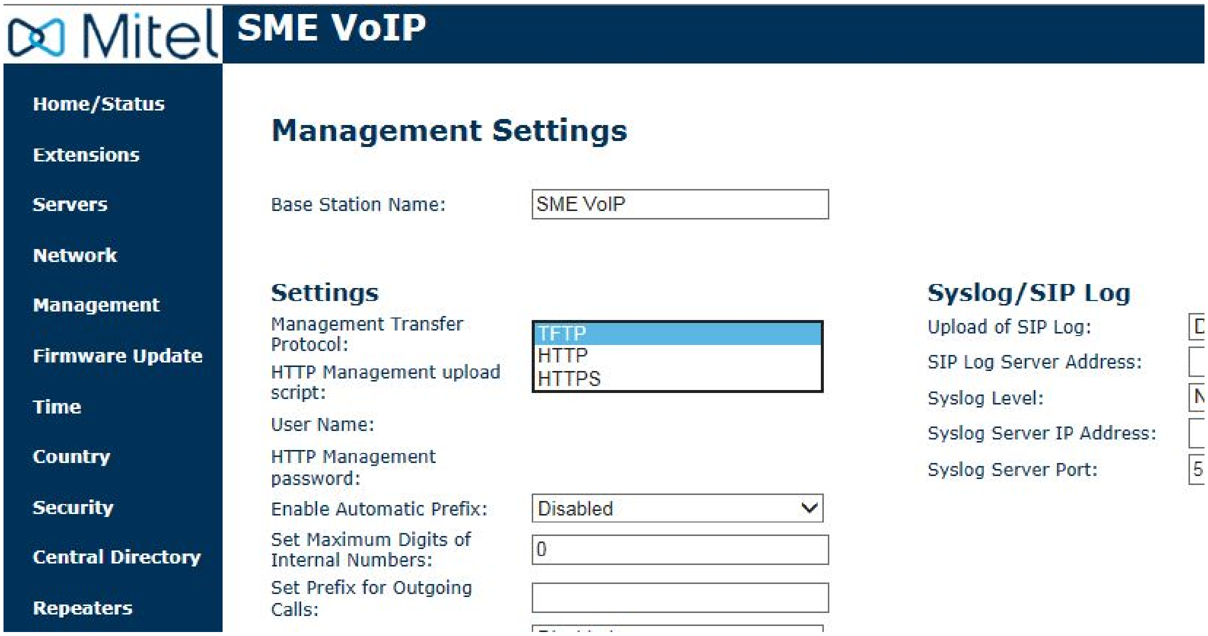
Next, click on the **Load** button. This will import the contents of contacts in the selected file into the relevant Base station.



The figure below shows the import procedure is in process.

CENTRAL DIRECTORY USING SERVER

Alternative way to import a Contact List is to get it from a server. Click Management to access the Management Settings page, then select the protocol of your server (TFTP/HTTP/HTTPS) in Management Transfer Protocol, then save the setting by clicking Save.



Go back to Central Directory page and enter Server IP address (inclusive the path in the end of the address) and Filename of the contact list, then save the setting by clicking Save. (See example below).

Then reboot the Base station to ensure that the changes take effect.

VERIFICATION OF CONTACT LIST IMPORT TO CENTRAL DIRECTORY

On the Handset, navigate to Central Directory. The contact list should be populated with the list of contacts that you uploaded to the base station.