M Series Deployment Guide

June 2020

8AL90621ENAA 01

Alcatel·Lucent Enterprise

Legal notice

Disclaimer

While efforts were made to verify the completeness and accuracy of the information contained in this documentation, this document is provided “as is”. To get more accurate content concerning Cross Compatibilities, Product Limits, Software Policy and Feature Lists, please refer to the accurate documents published on the Business Partner Web Site.

In the interest of continued product development, ALE International reserves the right to make improvements to this documentation and the products it describes at any time, without notice or obligation.

The CE mark indicates that this product conforms to the following Council Directives:

- 2014/53/EU for radio equipment
- 2014/35/EU and 2014/30/EU for non radio equipment (including wired Telecom Terminal Equipment)
- 2014/34/EU for ATEX equipment
- 2011/65/EU (RoHS)
- 2012/19/EU (WEEE)

CE

Table of contents

M Series Deployment Guide

Table of contents

M Series Deployment Guide

Chapter

1

Introduction

This document describes the deployment of M Series DeskPhone sets with a third party SIP server.

The following sets are covered:

M3 DeskPhone 

M5 DeskPhone 

M7 DeskPhone 

The M Series DeskPhone Deployment Guide provides general guidance on setting up phone network, provisioning and managing phones.

This guide is not intended for end users, but for administrator with experience in networking who understand the basis of open SIP networks and VoIP endpoint environments.

As an administrator, this guide will enable you to do the following:

- Set up a VoIP network and provisioning server.
- Provision the phones with features and settings.
- Troubleshoot, upgrade and maintain phones.

The information detailed in this guide is applicable to the M Series DeskPhone sets running firmware version 2.10.13 or above (see: *Checking the software version of the phone set* on page 9)

Chapter

2 Glossary

DHCP	Dynamic Host Configuration Protocol
DM	Device Management = provisioning server
EDS	Easy Deployment Service
FQDN	Fully Qualified Domain Name
HTTP/HTTPS	Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MMI	Man Machine Interface
PoE	Power over Ethernet
RAM	Random Access Memory
SIP	Session Initiation Protocol
SSH	Secure Shell
URL	Uniform Resource Locator
USB	Universal Serial Bus
VCI	Vendor Class Identifier
WBM	Web Based Management
WAN	Wide Area Network

Chapter

3

Accessing phone set information

This chapter describes where M Series DeskPhone sets fit in your network, and provides basic initialization instructions of SIP phones.

3.1 Requirements

In order to perform as SIP endpoints in your network successfully, you need the following in deployments:

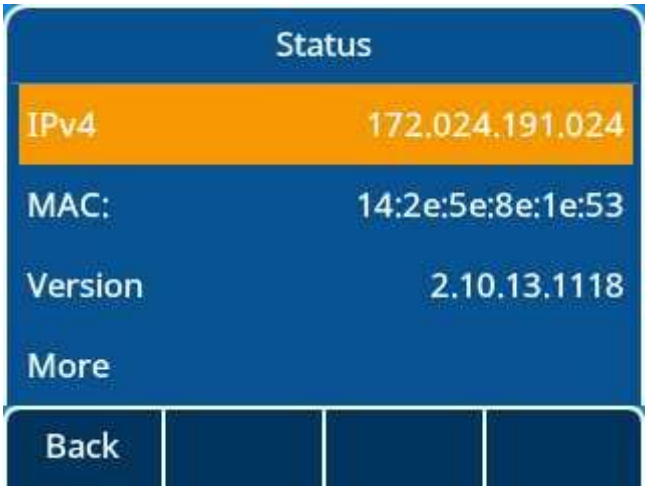
- M Series DeskPhone sets with compatible firmware (2.10 or above). To upgrade their firmware, see: Upgrading the firmware on page 34.
- A working IP network.
- An active SIP call server.
- A text editor, such as Notepad++, to create and edit configuration files.

3.2 Checking the device information

You can view the phone model information on the back of the phone. This label provides information on the phone model, SN and MAC address etc.

3.3 Checking the software version of the phone set

You can check the phone's software information by pressing the OK button in navigator keypad. This operation will allow the user to enter the status menu directly.

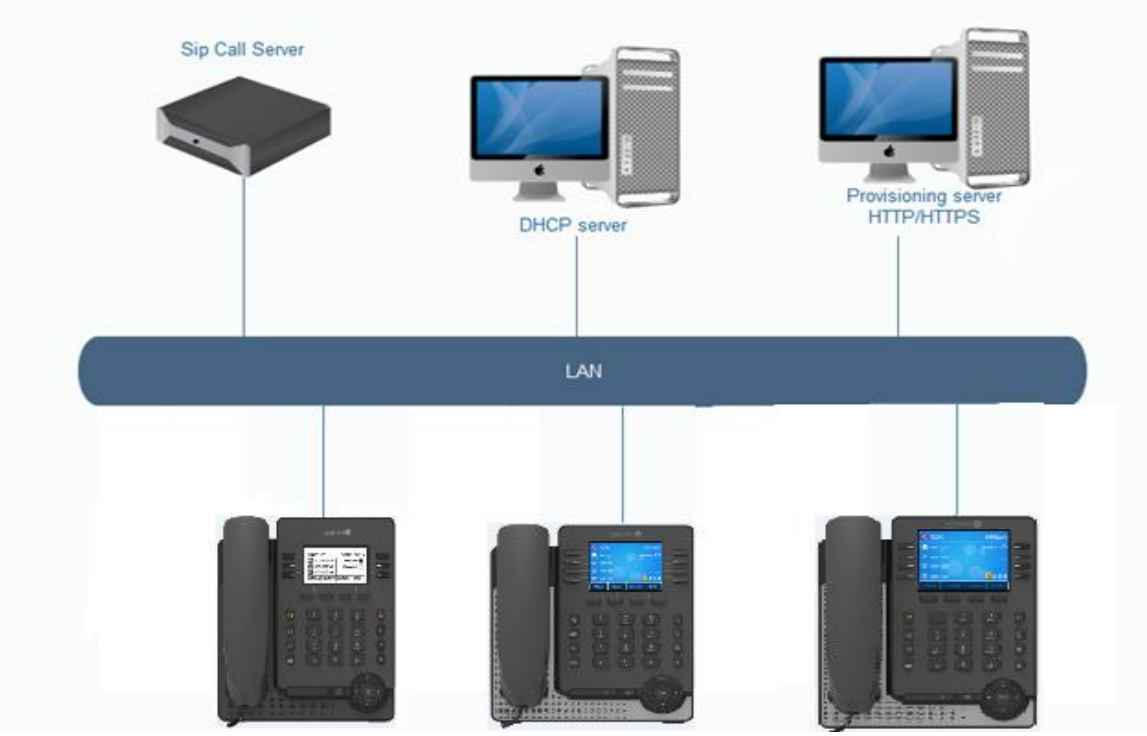


3.4 Checking the phone settings

After switching on the phone, press the "OK" button or "Menu" button and then select "Advanced settings" by pressing the navigator down key, then press the "OK" button to confirm, enter the password of "Admin" (password is "123456" by default).

3.5 Network topology

There are many ways to set up a phone network using ALE SIP phones. The following figure shows the simplest example of a network setup.



3.6 Verifying startup

The phone begins the initialization process by following steps after connecting to the power and network:

1. The power LED indicator glows blue.

2. The message “Welcome” appears on the phone screen when the IP phone starts up.

3. Press the OK key on navigator keypad to check the status of the phone quickly. Phone information, such as the valid IP address, MAC address, firmware version will be displayed on the screen.

Chapter

4

Phone set provisioning overview

This chapter gives general indication on the parameters that must be provisioned to start a set, the different ways to provision these parameters, and the priority rules between them.

Basically, parameters that must be provisioned are:

- IP parameters (IP address, netmask and router IP address)
- SIP account parameters (SIP server address, register name, username, password)
- DM URL, when SIP parameters are provisioned via SIP configuration files downloaded from a provisioning server

The different ways to provision these parameters are:

- IP parameters:
  - Statically via MMI: see Configuring IP parameters and SIP account parameters via MMI on page 12
  - Dynamically via DHCP
- SIP account parameters:
  - Manually:
    - Via MMI: see Configuring IP parameters and SIP account parameters via MMI on page 12
    - Via WBM: see Configuring IP parameters and SIP account parameters via WBM on page 13
  - Automatically via SIP configuration files downloaded from a provisioning server (DM server): see Building a SIP configuration file on page 28
- DM URL (required only in case of initialization with SIP configuration files):
  - Manually:
    - Via MMI: see Configuring the provisioning server URL via MMI on page 15
    - Via WBM: see Configuring the provisioning server URL via WBM on page 15
  - Automatically:
    - Via DHCP: see DHCP configuration for download path of SIP configuration files on page 22
    - Via EDS server: see Setting up auto-provisioning with EDS on page 32

The method you use depends on how many phones need to be deployed and what features and settings need to be configured. We recommend using manual provisioning as your primary provisioning method when just several phones are needed for testing.

Commissioning phone sets on page 18 details four possible scenarios:

	IP Parameters	**SIP parameters**	**DM URL**
Scenario 1	MMI	MMI	N/A
Scenario 2	DHCP	WBM	N/A
Scenario 3	DHCP	DM server	DHCP
Scenario 4	DHCP	DM server	EDS

Chapter 4 *Phone set provisioning overview*

4.1 Provisioning method priority

A priority order is defined between the different provisioning methods: settings you make using a higher priority provisioning method will override settings made using a lower priority method.

The priority order for setting provisioning is:

1. Settings received from the provisioning server (DM server)
2. Settings received from the DHCP server
3. Settings configured locally via MMI or WBM
4. Factory default settings

For the DM URL configuration, the priority is the following:

1. DM URL received from DHCP
2. DM URL configured via MMI or WBM
3. DM URL received from EDS

4.2 Configuring IP parameters and SIP account parameters via MMI

4.2.1 Configuring IP parameters via MMI

The setting menu of the MMI can be accessed when the phone is starting up:

1. At initialization (from **step 1: System initialization**), press the * and # keys to access the MMI.
2. Enter the admin password (the default admin password for the phone out of box is `123456`).
3. Press the softkeys **IP param** > **IP config** > **IPv4 settings** to access the IP parameters setting page. This page allows you to select the initialization mode (The default DHCP mode is dynamic) and to configure network parameters if static mode is selected.
4. Press the softkey next to **IPv4 mode** to switch to **Static**.
5. Complete the set IP parameters:
   - **IP**: enter the set IP address
   - **S/net**: enter the IP subnet mask
   - **Router**: enter the default router IP address
6. Press the **OK** key to save modifications
7. Press release key to exit the settings menu.

The set automatically reboots to apply these settings changes.

4.2.2 Configuring SIP account parameters via MMI

The settings menu of the MMI can be accessed when the phone is starting up:

1. At initialization (from **step 1: System initialization**), press the * and # keys to access the MMI.
2. Enter the admin password (the default admin password for the phone out of box is `123456`).
3. Press down key on navigator keypad until the last page and press **SIP servers** softkey.

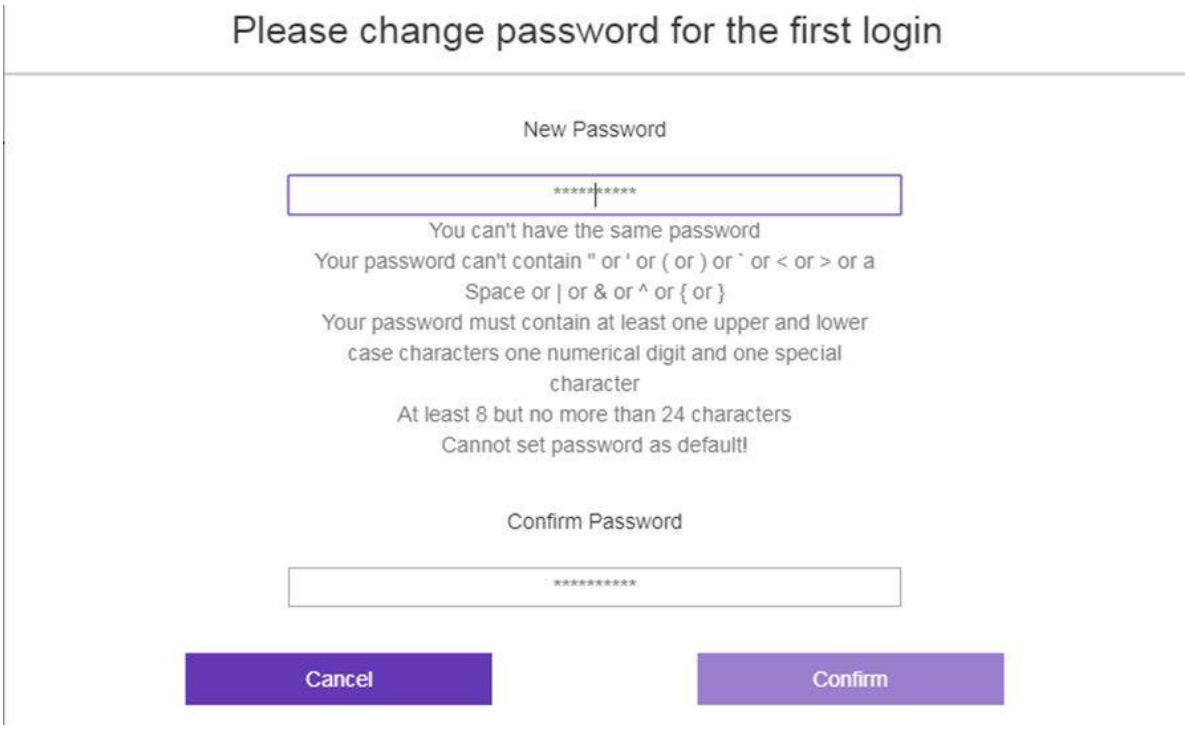
4. Select a SIP account and configure related SIP server connection parameters.
5. For details on SIP server parameters, see: SIP servers/groups/accounts on page 48.
6. Press the **OK** key to save modifications.
7. Press release key to exit the settings menu.

The set automatically reboots to take apply settings changes.

4.3 Configuring IP parameters and SIP account parameters via WBM

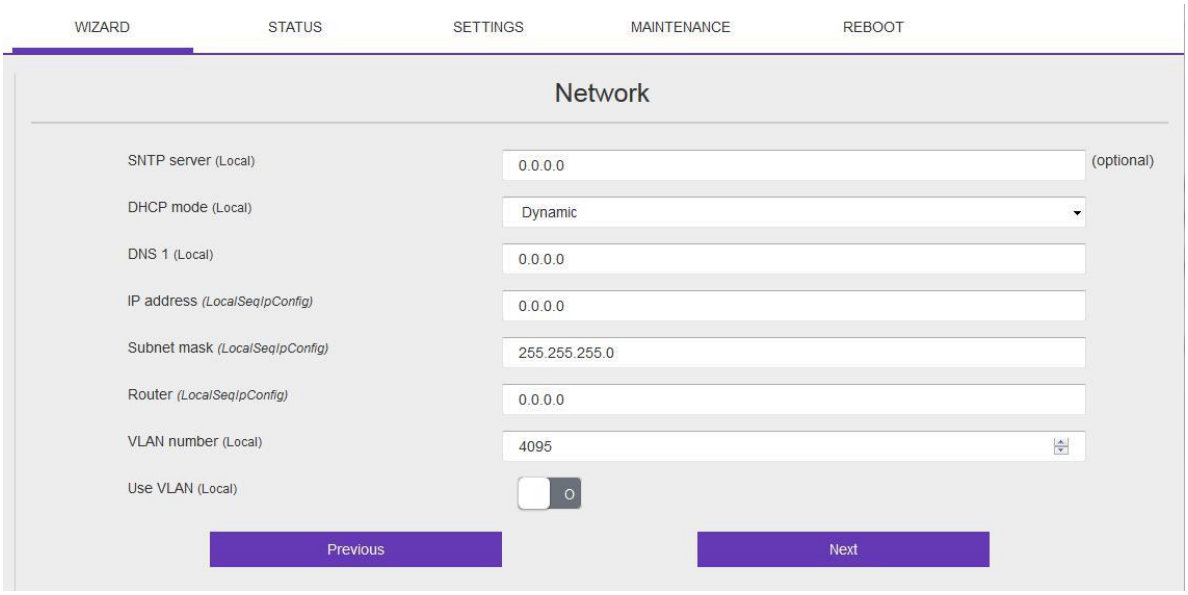
You can configure M Series DeskPhone sets via web user interface (WBM) when the phone has started up with proper IP parameters.

1. To find the IP address of the set, in the set user interface (MMI), select Settings > Network and read the IP address.
2. In a web browser, enter the URL: `https://[IP address]`, for example `https://192.168.0.10`
3. You are prompted to enter login/password:
   - login: enter **admin**
   - password: enter the password (default password is `123456`)
4. Click **Connect**
5. Change the password, and log in again with the new password



6. It is recommended to set up the phone via Wizard. Click the **Wizard start** to start the phone set configuration.

   The wizard includes five configuration steps as shown on the figure below. **Network** and **SIP** are mandatory for the first setup.



7. Enter the mandatory IP parameters in **Network** tab and press **Next**.

On the new page you can configure the SIP account parameters as shown in the following figure.

Note:

The parameters highlighted in red in the figure below are mandatory for the phone set registration on the SIP server.

8. Press **Next**. You can skip the configuration on **LDAP** and **User** as they are not mandatory for the phone configuration at the first registration on the SIP server. Make sure all the mandatory fields have been filled in with correct value, then press **Confirm**. The phone reboots to apply these settings changes.

4.4 Configuring the provisioning server URL via MMI

The setting menu of the MMI can be accessed when the phone is starting up:

1. At initialization (from **step 1: System initialization**), press the * and # keys to access the MMI.
2. Enter the admin password (the default admin password for the phone out of box is `123456`).
3. Press down key on the navigator keypad to access the next page, and press the **DM** softkey.
4. Press the button next to **URL**, and enter the complete URL (for example: `https:// <provisioning server IP address>/download`).
   Note:
   *If the server requests HTTPS digest authentication, complete the **Username** and **Password** fields with the appropriate credentials).*
5. Press the **OK** key to save modification.
6. Press release key to exit the settings menu.

   The set automatically reboots to download the SIP configuration file from the provisioning server.

4.5 Configuring the provisioning server URL via WBM

You can configure M Series DeskPhone sets via web user interface (WBM) when the phone has started up with proper IP parameters.

1. To find the IP address of the set, in the set user interface (MMI), select Settings > Network and read the IP address.
2. In a web browser, enter the URL: `https://[IP address]`, for example `https:// 192.168.0.10`
3. You are prompted to enter login/password:
   - login: enter **admin**
   - password: enter the password (default password is `123456`)
4. Click Connect
5. If needed, change the password, and login again with the new password
6. Go to Settings > Network > DM
7. In the DM URL field, enter the complete URL (for example: `https://<provisioning server IP address>/download`).
   Note:
   *If the server requests HTTPS digest authentication, complete the **Username** and **Password** fields with the appropriate credentials).*
8. Press **Apply** to save modification.

   A reboot pop-up opens.
9. Press **Reboot now**.

   The set automatically reboots to download the SIP configuration file from the provisioning server.

4.6 Central provisioning with SIP configuration files

You can set up M Series DeskPhone sets using a SIP configuration file, downloaded by the set from a provisioning server using HTTP or HTTPS. The SIP configuration file contains necessary information to allow the M Series DeskPhone sets to register on the SIP server. The file name format is `config.{mac-address}.xml`.

For more information on the SIP configuration file content and structure, see:

- Description of the SIP settings in configuration file on page 47
- SIP configuration file templates on page 43

To configure a provisioning server in your network environment, see: Provisioning server setup overview on page 24.

The download path of SIP configuration file can be provisioned:

- Via DHCP: see Setting up a DHCP server on page 21
- Via EDS: see Setting up auto-provisioning with EDS on page 32
- Statically:
  - Via MMI: see Configuring the provisioning server URL via MMI on page 15
  - Via WBM: see Configuring the provisioning server URL via WBM on page 15

Chapter

5

Connecting the phone set to the customer network

Connecting the phone set to the customer network:

- If the phone set is powered by PoE:

  a. Plug the RJ45 cable into the set LAN connector

  b. Connect the RJ45 cable to the customer network via a PoE hub/switch (IEEE802.3af compliant)

- If the phone set is not powered by PoE, plug the AC/DC external adapter to the set power supply connector (DCSV) and connect the plug to the power supply

Once the phone set is connected and powered up, it automatically starts initializing.

The phone set begins the initialization process by following steps after connecting to the power and network:

1. The call and message LED indicators glow blue.

2. The message “Welcome” appears on the phone screen when the phone set starts up.

3. The main phone screen displays the following:

- Firmware version on the top of the screen
- Each initialization step, from step 1 to 5

4. Press right key on navigator keypad to enter the settings menu. The phone screen then displays the valid IP address, MAC address, phone configuration, firmware version, help for navigator key usage, and more.

Chapter

6

Commissioning phone sets

This chapter describes basic initialization instructions of M series DeskPhone sets.

Four scenarios are described:

6.1 Scenario 1: IP static initialization on LAN, no SIP configuration file

Scenario 1 describes the commissioning of a set on the LAN with IP static initialization (no DHCP server) and without SIP configuration files (no provisioning server). In this scenario, all the configuration is performed via the set MMI.

Before beginning: you must know the following:

- IP parameters of the set (IP address, netmask, router IP address)
- SIP parameters: SIP call server information (IP addressing, domain, authentication)

Prerequisites:

- The M Series DeskPhone firmware is 2.10.13 or above.

  At initialization, the firmware version is displayed at the top of the screen: see: Checking the software version of the phone set on page 9

To commission the set:

1. Configure the phone set on the SIP call server as needed according to the SIP server documentation

2. Connect the set: see Connecting the phone set to the customer network on page 17

3. Access the phone set user interface (MMI) and configure the following:

a. Change the initialization mode from **Dynamic** (default mode) to **Static**: see: Configuring IP parameters via MMI on page 12

b. Configure the IP parameters of the phone set: see: Configuring IP parameters via MMI on page 12

c. Configure SIP parameters (via a SIP account): see: Configuring SIP account parameters via MMI on page 12

6.2 Scenario 2: IP dynamic configuration on LAN, no SIP configuration file

Scenario 2 describes the commissioning of a set on the LAN with IP dynamic initialization (provision of standard IP parameters by DHCP server) and without SIP configuration files (no provisioning server). In this scenario, the sets gets its IP parameters from the DHCP server and SIP parameters are configured manually via WBM.

Before beginning: you must know the following:

- SIP parameters: SIP call server information (IP addressing, domain, authentication)

Prerequisites:

- The M series DeskPhone firmware is 2.10.13 or above.

At initialization, the firmware version displays on the top of the screen: see: Checking the software version of the phone set on page 9

- A DHCP is operational on the LAN (no specific configuration required): see Setting up a DHCP server on page 21

To commission the set:

1. Configure the phone set on the SIP call server as needed according to the SIP server documentation
2. Connect the set: see Connecting the phone set to the customer network on page 17
3. Read the IP address on the phone set display
4. Access the phone set configuration via WBM: see Configuring IP parameters and SIP account parameters via WBM on page 13
5. Configure SIP parameters

6.3 Scenario 3: IP dynamic configuration on LAN with SIP configuration file (zero touch)

Scenario 3 describes the commissioning of a set on the LAN with IP dynamic initialization (provisioning of standard IP parameters by DHCP server) and with SIP configuration file which will be downloaded during set initialization from a provisioning server, whose URL is provided by the DHCP server: this requires a specific configuration on the DHCP server. In this scenario, the set starts without any manual operation via MMI or WBM (zero touch).

Before beginning: you must know the following:

- SIP parameters: SIP call server information (IP addressing, domain, authentication): this information is required to build the configuration file

Prerequisites:

- The M series DeskPhone firmware is 2.10.13 or above.

  At initialization, the firmware version displays on the top of the screen: see: Checking the software version of the phone set on page 9
- The phone set must initialize in dynamic mode (default mode)
- A DHCP is operational on the LAN and configured to provide the URL of the provisioning server (DM URL): see Setting up a DHCP server on page 21 and DHCP configuration for download path of SIP configuration files on page 22
- A provisioning server is operational on the LAN: see Setting up a provisioning server on page 24

To commission the set:

1. Configure the phone set on the SIP call server as needed according to the SIP server documentation
2. Create and configure the SIP configuration file: see: Building a SIP configuration file on page 28
3. Deploy the SIP configuration file in the provisioning server relative directory
4. Connect the set: see Connecting the phone set to the customer network on page 17

   After startup, the set automatically begins initialization process. After the last initialization step, the set registers to the SIP server.

6.4 Scenario 4: IP dynamic configuration on WAN with SIP configuration file (zero touch)

Scenario 4 describes the commissioning of a set on the WAN with IP dynamic initialization (provisioning of standard IP parameters by DHCP server) and with SIP configuration files which will be downloaded during

set initialization from a provisioning server, whose URL is provided by the EDS server: this requires a specific configuration on the EDS server. In this scenario, the set starts without any manual operation via MMI or WBM (zero touch).

Before beginning: you must know the following:

- SIP parameters: SIP call server information (IP addressing, domain, authentication): this information is required to build the configuration file

Prerequisites:

- The M series DeskPhone firmware is 2.10.13 or above.

  At initialization, the firmware version displays on the top of the screen: see: Checking the software version of the phone set on page 9
- The phone set can reach the WAN
- The phone set must initialize in dynamic mode (default mode)
- A DHCP is operational on the LAN (no specific configuration required): see Setting up a DHCP server on page 21
- A provisioning server is operational on the WAN or Cloud: see Setting up a provisioning server on page 24
- A profile associated to the phone MAC address has been created on the EDS server to provision DM URL and certificate relative URL: see Setting up auto-provisioning with EDS on page 32

To commission the set:

1. Configure the phone set on the SIP call server as needed according to the SIP server documentation
2. Create and configure the SIP configuration file: see: Building a SIP configuration file on page 28
3. Deploy the SIP configuration file in the provisioning server relative directory
4. Connect the set: see Connecting the phone set to the customer network on page 17

   After startup, the set automatically begins initialization process. After the last initialization step, the set registers to the SIP server.

Chapter

7 Setting up a DHCP server

This chapter details the configuration of the DHCP server to be performed when M Series DeskPhone sets initialize in dynamic mode.

The DHCP can be used to provide standard IP parameters only (see Commissioning phone sets on page 18: scenarios 2, 4) or standard IP parameters and the DM URL (see Commissioning phone sets on page 18: scenario 3). When the DM URL is not provisioned by the DHCP server, no specific configuration is required on the DHCP server: only standard IP parameters are required.

You can skip this section if M Series DeskPhone sets initialize in static mode (see Commissioning phone sets on page 18: scenario 1).

If configured for dynamic IP address, the M Series DeskPhone set retrieves its network configuration parameters from the DHCP server during step 3 of its initialization.

DHCP option configuration for IPv4 on page 21 details the list of DHCP options supported by M Series DeskPhone sets.

DHCP configuration for download path of SIP configuration files on page 22 describes how to configure the download path of SIP configuration files on the DHCP server.

Note:

Configuring the download path is not required when auto-provisioning with EDS is used.

7.1 DHCP option configuration for IPv4

The following table lists common DHCP options for IPv4 supported by M Series DeskPhone sets.

Parameter	DHCP option	Description
Subnet Mask	1	Specify the client's subnet mask
Router	3	Specify a list of IP addresses for routers on the client's subnet
Domain Name Server	6	Specify a list of domain name servers available to the client
Host Name	12	Specify the name of the client. (sent by default)
Domain Server	15	Specify the domain name that client should use when resolving hostnames via DNS
Network Time Protocol Servers	42	Specify a list of NTP servers available to the client by IP address
Vendor-Specific Information	43	Identify the vendor-specific information
Vendor Class Identifier	60	Identify the vendor type (ictouch.0)

Parameter	DHCP option	Description
DM server	66	Identify one DM URL (link for SIP configuration file downloading), or IP address or FQDN with optional port: see *DHCP configuration for download path of SIP configuration files on page 22* *Note:* *DM stands for Device Management server and is another name for provisioning server.*
option 43 > sub-option 67	67	Sub-option of Option 43, to define the DM path: *DHCP configuration for download path of SIP configuration files on page 22*
Default user class	77	ictouch.class0

Table 7.1: Configuration for DHCP Option 12, Option 60 and Option 77

	M3	M5	M7
VCI (dhcp option 60) (not modifiable)	ictouch.0	ictouch.0	ictouch.0
Default user class (option 77) (not sent by default)	ictouch.class0	ictouch.class0	ictouch.class0
Default hostname (option 12) (sent by default)	M3-XXYYZZ*	M5-XXYYZZ	M7-XXYYZZ

Note: *XXYYZZ is last 3 bytes of MAC address

7.2 DHCP configuration for download path of SIP configuration files

The table below describes the different possibilities for the configuration on the DHCP server of the download path for SIP configuration files.

You can ignore this section if auto-provisioning with EDS is used (see Commissioning phone sets on page 18: scenario 4).

Table 7.2: Configuration of download path on DHCP

Option 66	Option 43 > sub option 67 (full path)	Option 43 > sub option 67 (relative path)	Download path
		√	Invalid combination
√			https://option 66/
√		√	https://option 66/sub-option 67/
	√		Sub-option 67
√	√		Sub-option 67

Table 7.3: Configuration example for download path

Option 66	Option 43 > sub option 67 (full path)	Option 43 > sub option 67 (relative path)	Download path
192.168.2.2/ale/config			https://192.168.2.2/ale/config
192.168.2.2		ale/config	https://192.168.2.2/ale/config
	192.168.2.2/ale/config		https://192.168.2.2/ale/config
	http://192.168.2.2/ale/config		http://192.168.2.2/ale/config

Chapter

8 Setting up a provisioning server

8.1 Provisioning server setup overview

A provisioning server is necessary when SIP configuration files are used (see Commissioning phone sets on page 18: scenarios 3, 4).

You can skip this section if M Series DeskPhone sets initialize without SIP configuration files (see Commissioning phone sets on page 18: scenarios 1, 2).

M Series DeskPhone sets support the following transport protocols for provisioning:

The HTTP/HTTPS provisioning server can be set up on the local LAN. Use the following procedure as a recommendation if this is your first provisioning server setup.

To set up the provisioning environment:

1. Install an HTTP/HTTPS server application or locate a suitable existing server.

2. Create an account and home directory.

3. Set security permissions for the account.

Once the setup has been completed, create the SIP configuration files required for set commissioning (see: Building a SIP configuration file on page 28), and copy them in the HTTP/HTTPS provisioning server relative directory.

If the M Series DeskPhone set has retrieved a DM URL from the DHCP server, it downloads the configuration file from the provisioning server during step 4 of its initialization.

Note:

The DM URL which is configured in the DHCP server corresponds to the path of the SIP configuration files stored on the provisioning server.

8.2 Example with the Apache HTTP server setup

Configure a Windows server system (or virtual system) to set up an Apache web server with following standard steps. When the Apache web server has been successfully installed, create a directory on this server to store the SIP configuration files or firmware binary files, and get the download URL for set commissioning.

To set up an Apache HTTP server

1. Go to *www.apache.org* and download the last version of Apache web server

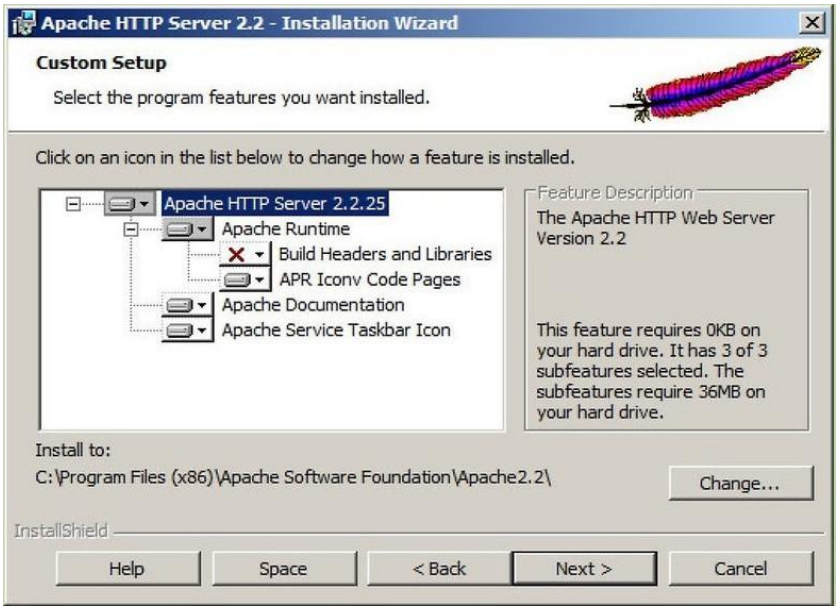
2. Install the Apache web server

When installing Apache, you are asked to enter your domain name, network name, and e-mail address. You can add any value in these fields. The format must be:

- Domain name: `example.com`
- Network name: `www.example.com`
- E-mail address: `user@example.com`

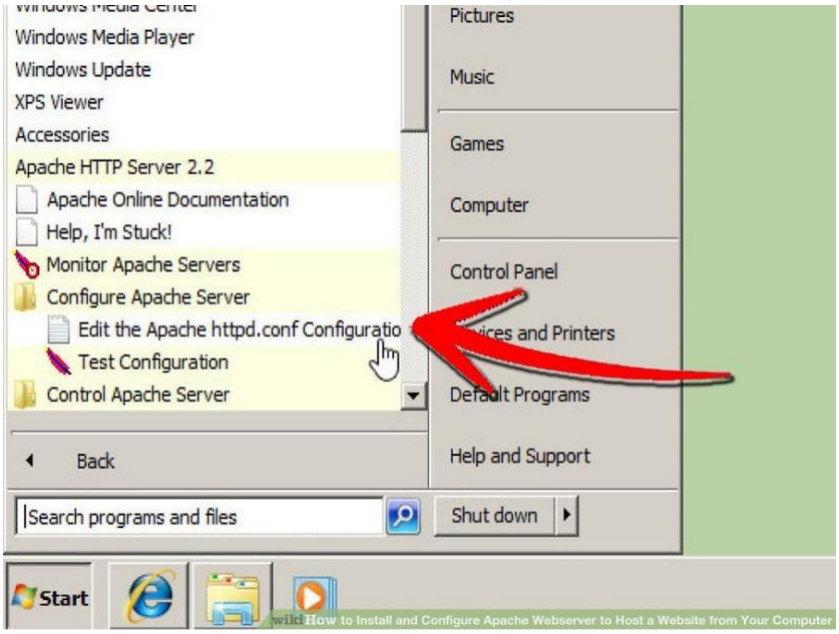
3. Click **Next**

4. Select the Apache HTTP server from the radio button list

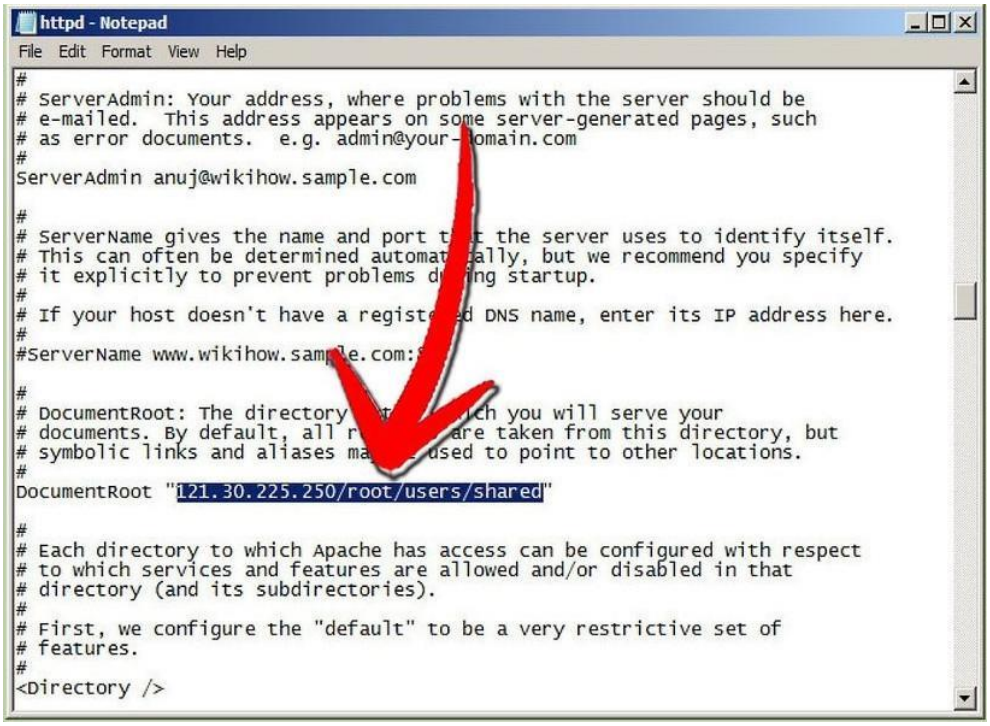


An error message is displayed such as: "Apache could not be configured. Edit your Apache.conf file"

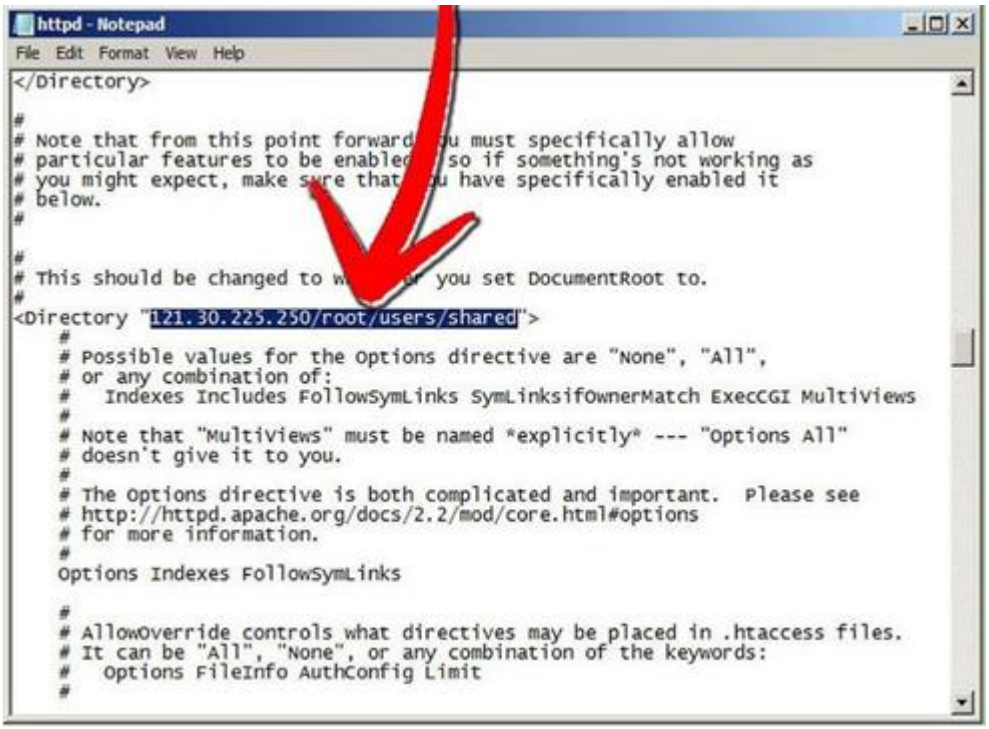
5. Go to: **Start** > **Programs** > **Apache HTTP Server <version number>** > **Configure Apache Server** > **Edit the Apache httpd.conf Configuration File**



6. Go to the **DocumentRoot** line
7. Change the document root to point to the location of your website folder, using the character "/" instead of "\"



8. Repeat this operation for <Directory "drive:/location">



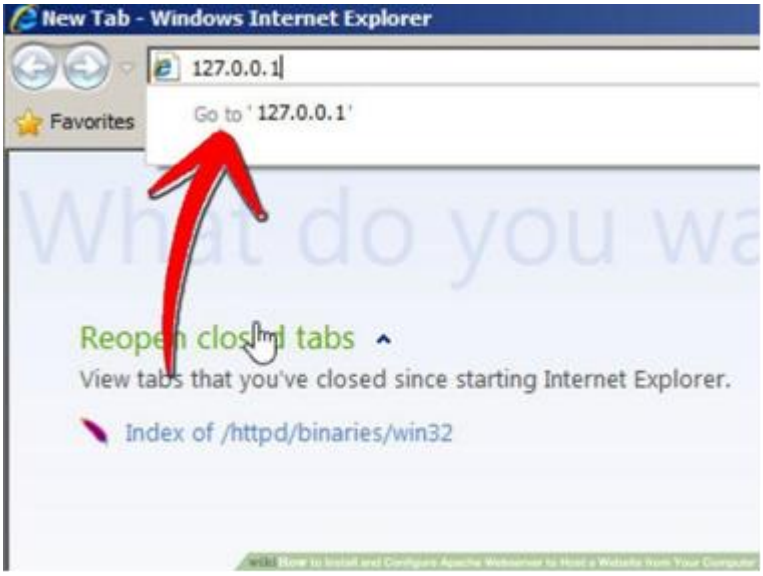
9. To verify your configuration, go to Apache in your taskbar and stop the service

10. Restart the service

If the service does not start, modify the Apache httpd.conf configuration file properly

11. Once the service is restarted, open a web browser and enter `localhost` or `127.0.0.1` in the address bar

Chapter 8 Setting up a provisioning server



Note that, for most of users, to establish one Apache server is too complex, we strongly recommend you using some software tool to simulator Apache server, like MobaXterm, HFS etc.. These tools can also provide HTTP service but they are very easy to download and configure. See: Example with MobaXterm tool for provisioning on page 28.

8.3 Building a SIP configuration file

Before beginning, you must have the following:

- The MAC address of the phone set required for the name of the SIP configuration file (`config.{mac address of the phone set}.xml`, for example `config.00809fe7021e.xml`): see Checking the device information on page 9
- A text editor, such as Notepad++, to create and edit configuration file

Build the SIP configuration file required for set commissioning:

1. Install an HTTP server application or locate a suitable existing server.

For details on the file structure, name and minimum settings, see: SIP configuration file templates on page 43.

2. Complete the SIP configuration file according to your needs.

For details on the available settings, see: Description of the SIP settings in configuration file on page 47.

Once created, copy the SIP configuration file in the HTTP/HTTPS provisioning server relative directory.

8.4 Example with MobaXterm tool for provisioning

Step1: Preparing the config file: `config.{mac-address}.xml`

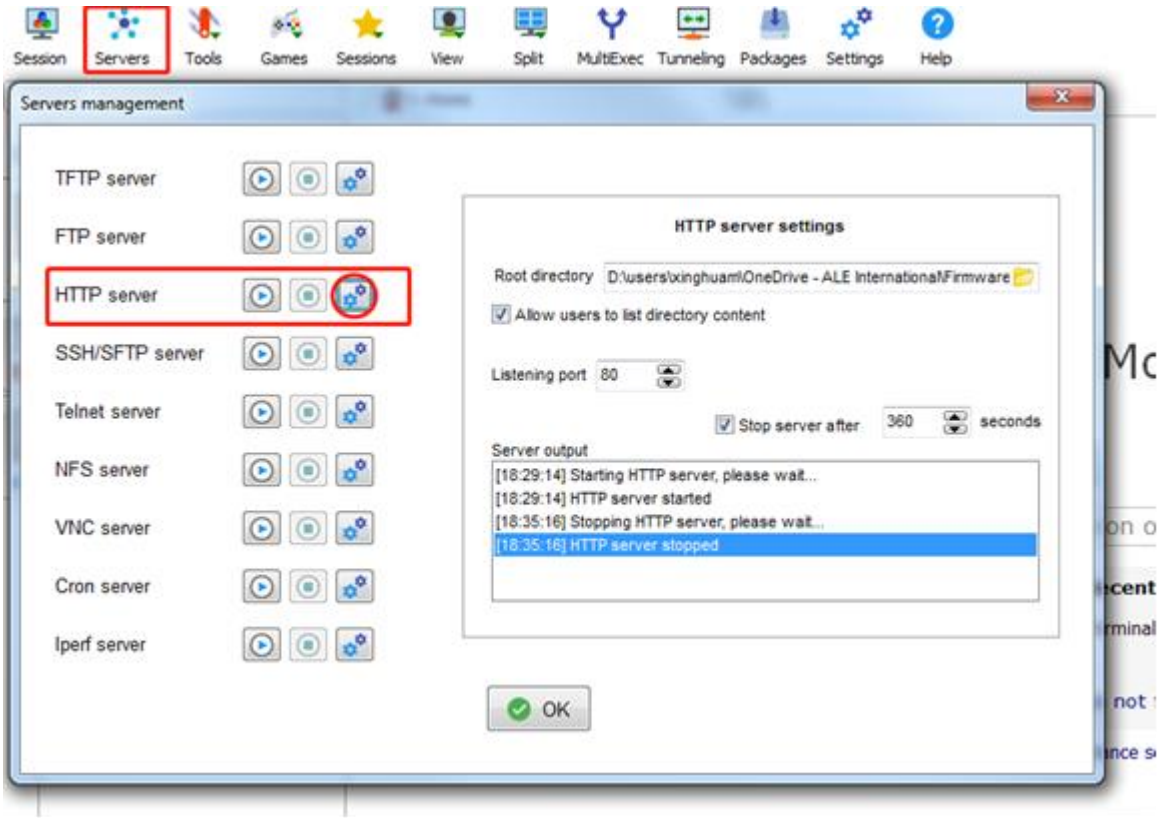
In the config file the following contents should be included at the least:

```
<?xml version="1.0" encoding="UTF-8" ?>
<settings>
<setting id="SIPServer1Address" value="TestSipDomain.sipserver.com" override="true"/>
<setting id="SIPGroup1DeviceUri" value="Testnumber" override="true"/>
<setting id="SIPGroup1AuthenticationPassword" value="TestSipPassword" override="true"/>
<setting id="DmAdminPasswd" value="000000" override="true"/>
</settings>
```

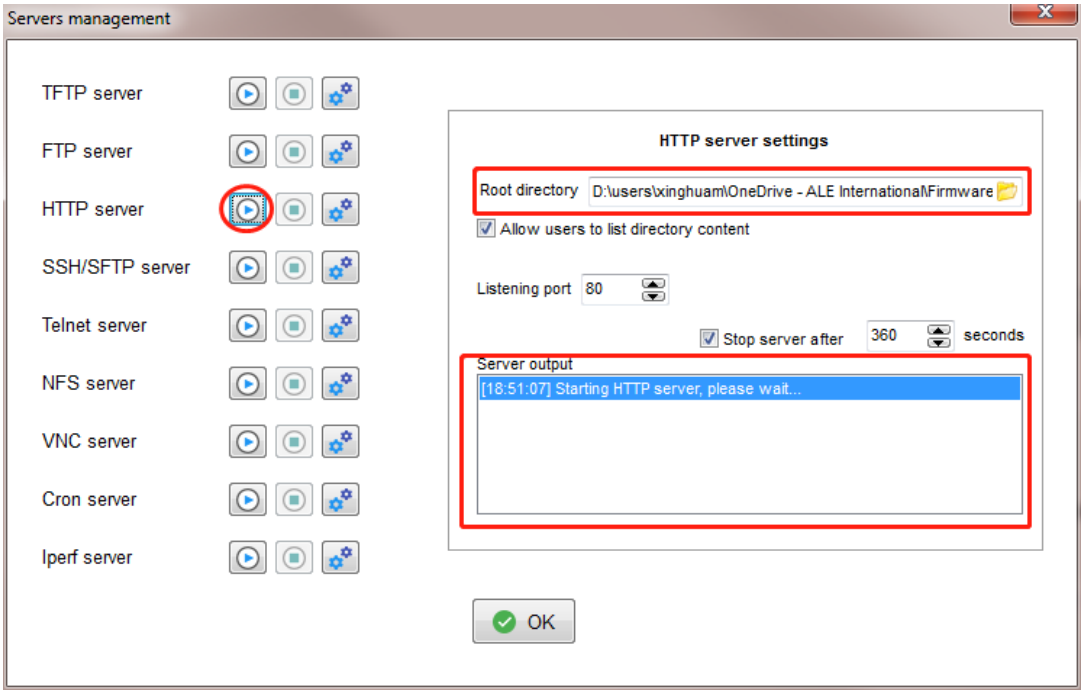
Note: For details on the file structure, see: SIP configuration file templates on page 43.

Step2: Install the MobaXterm tool on your PC.

Step3: Open the tool and go to “Servers → HTTP server → “settings” (red circle)



Step 4: Copy the path with the config file saved on your PC in “Root directory” and then press  to run the HTTP server on your PC.

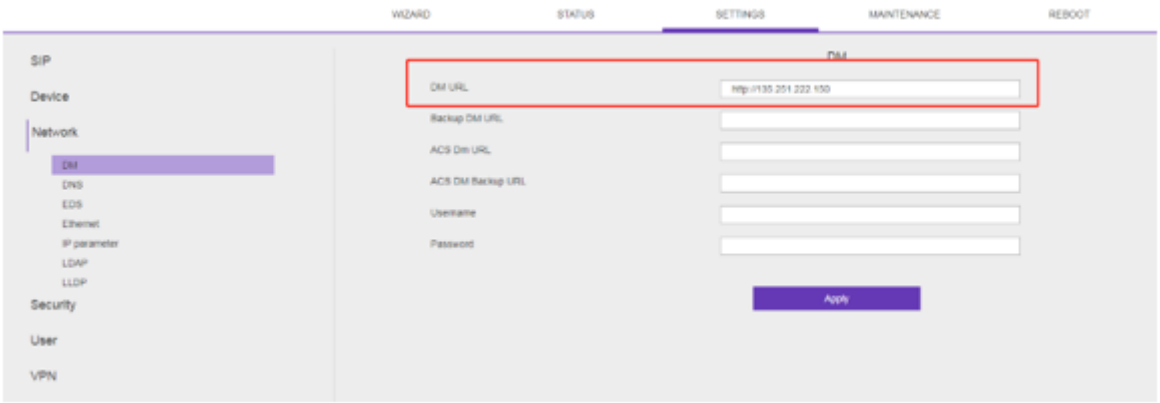


Note: you will see the “Starting HTTP server, please wait…” log in “Server output” box.

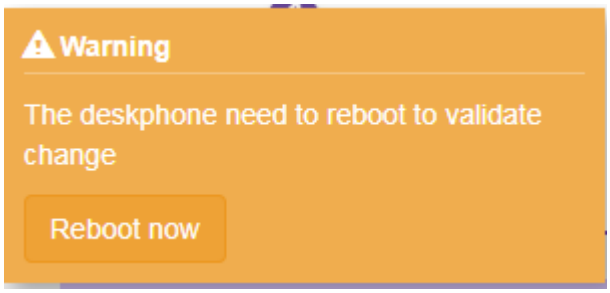
Step 5: Check the IP address of your PC, “135.251.222.150” for example.

Step 6: Log in the phone via web with default password “123456” and then change the password to complex one like “Ale123!@”.

Then go to Settings---> Network---> DM---> DM URL, and fill in the path. The path is equal to the value of blue box field shown in the image1.



Step 7: Press “Apply”. Then press “Reboot now” in the warning page.



Step 8: The phone will restart and then download the config file.

When the phone is starting up its admin password will be “000000” which is defined in config file with sentence *“<setting id="DmAdminPasswd" value="000000" override="true"/>”*

You can define the password by modifying the value.

Chapter

9

Setting up auto-provisioning with EDS

M Series DeskPhone sets support zero touch deployment by the Easy Deployment Service (EDS). You can contact the ALE EDS administrator *account.eds@al-enterprise.com* to create an account.

ALE EDS is a server side service that helps M Series DeskPhone sets to connect to the provisioning server on first startup. The service is deployed on the Internet Cloud.

The EDS server enables the provisioning of sets with the DM URL and certificates, allowing them to initialize from the WAN (see Commissioning phone sets on page 18: scenario 4), without requiring a specific configuration of the DHCP server.

When the set starts in dynamic mode and no provisioning server URL (DM URL) is configured via MMI or received from DHCP, it tries to connect to the ALE EDS server, whose address is hard-coded in its software. The server verifies the set's MAC address, and searches a profile for the set in the database.

The provisioning server URL and certificate relative URL are provided in the profile. The set downloads certificate, connects to the provisioning server via this URL, and downloads its SIP configuration file.

Note:

Auto-provisioning with EDS does not apply to phone sets initializing in static mode.

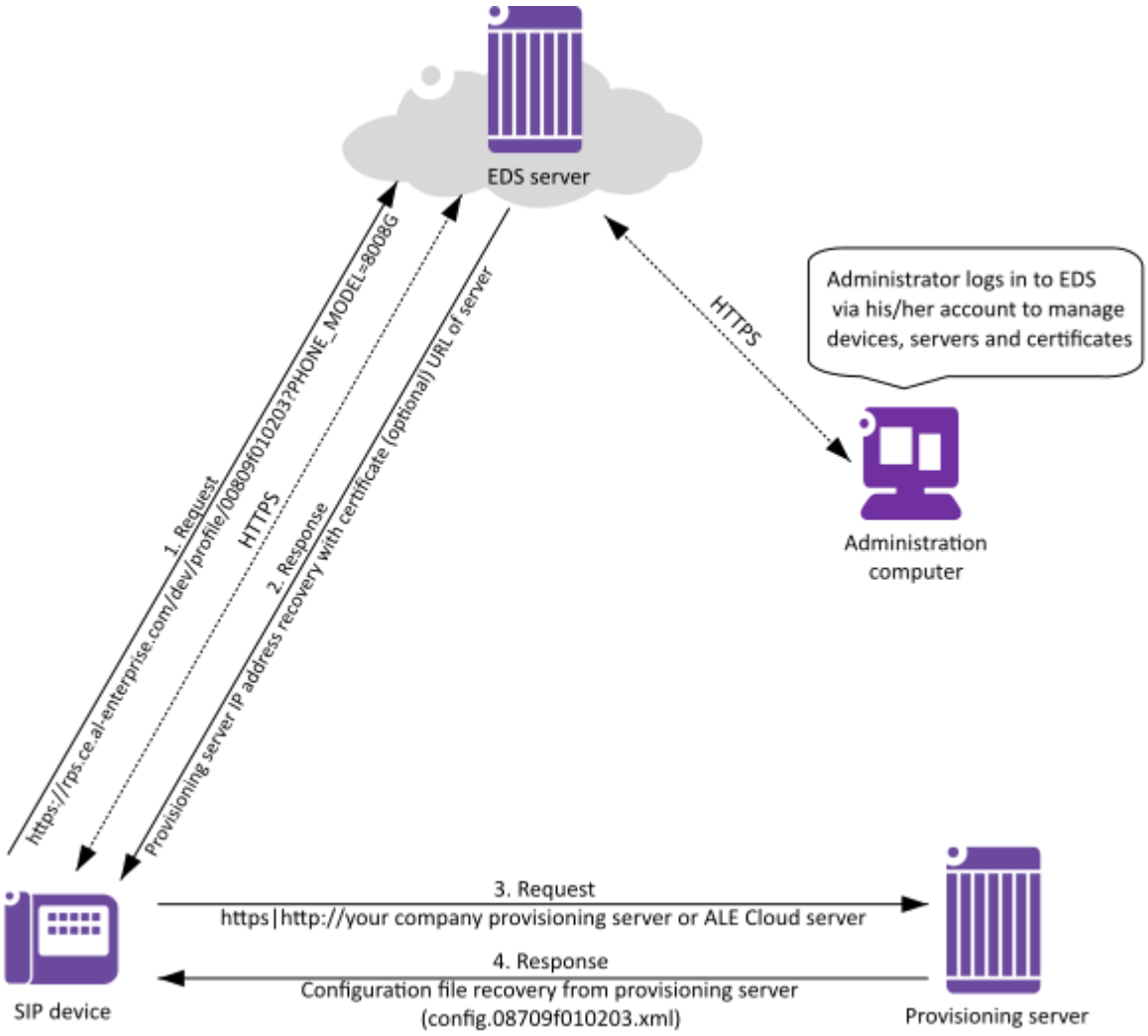


Figure 9.1: Auto provisioning process with EDS

Chapter

10 Upgrading the firmware

This chapter details the firmware upgrade of M Series DeskPhone sets.

Before upgrading firmware, you need to know the following:

- Do not close and refresh the browser when the IP phone is upgrading firmware via web user interface.
- Do not unplug the network cables and power cables when the IP phone is upgrading firmware.

10.1 Upgrading by WBM

1. Put the new firmware version on your local PC

2. Connect to the set WBM (as explained in Configuring IP parameters and SIP account parameters via WBM on page 13) and go to: **Maintenance** > **Binary Update**

3. Click **Add binary files**

4. Select the binary file:
- bin9000N
- sip9000N

Note:

The header file is not necessary when upgrading by WBM.

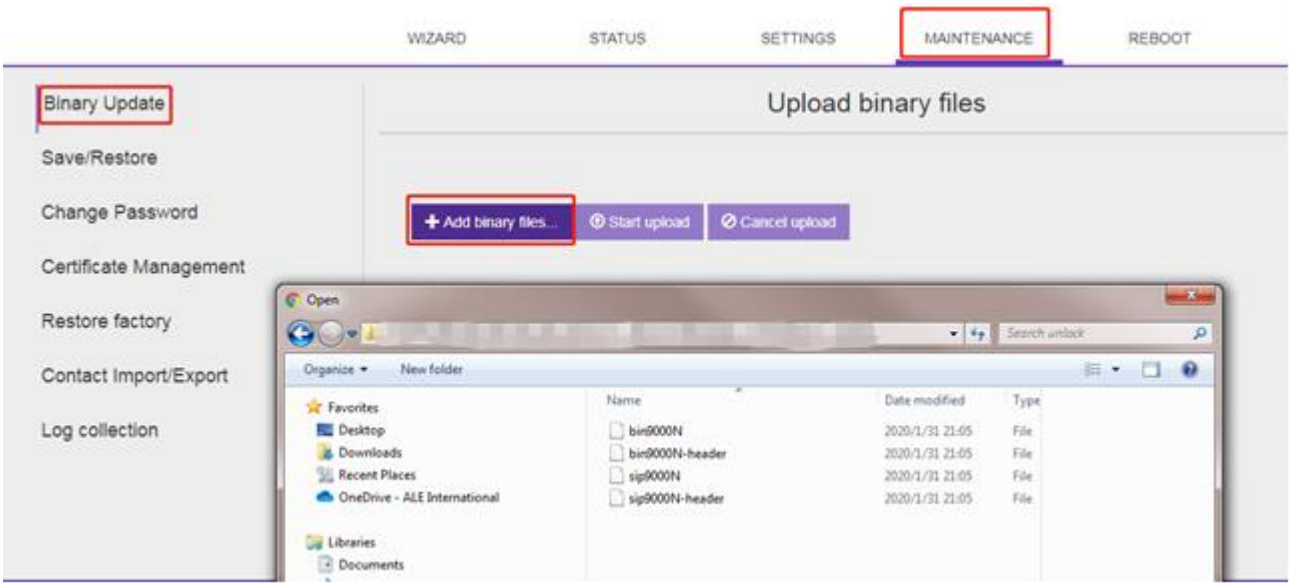


Figure 10.1: Binary file selection example

5. Click **Start upload**

Once downloaded, the phone installs the new binary and reboots. The whole process takes about 10 minutes in background (except reboot). A message is displayed when the binary upgrade is successfully completed.

On the phone set, you can check the version from the settings menu (see: Checking the software version

of the phone set on page 9).

10.2 Upgrading by configuration file

You can upgrade the M Series DeskPhone sets using the SIP provisioning server and SIP configuration with relevant parameters.

M Series DeskPhone sets can be upgraded by downloading firmware binary files from a provisioning server whose URL must be defined in the SIP configuration file (i.e. `config.{mac-adress}.xml`, for example `config. 00809fe7021e.xml`).

Settings:

```
<setting id="DmEnetcfgUpgradeFile" value="upgrade URL" override="true"/>
```

Description:

Set up the upgrading URL. Enter the firmware binary file in the directory of provisioning server, for example the URL could be `http://192.168.2.2/ale/firmware`. Then this settings should be:

```
<setting id="DmEnetcfgUpgradeFile" value="http://192.168.2.2/ale/firmware" override="true"/>
```

You can trigger an immediate upgrade by resetting manually the M Series DeskPhone set, or enable automatic update by adding settings described below in the SIP configuration file.

Automatic update operates in the following way:

- The phone polls for new binary once a day at the time defined by `DmAdmcfgUpdateTimeStart`
- To prevent all sets from updating at the same time, `DmAdmcfgUpdateTimeDelta` can be configured so that each set will update at a random time between `DmAdmcfgUpdateTimeStart` and `DmAdmcfgUpdateTimeStart` + `DmAdmcfgUpdateTimeDelta`. In this way, upgrade parameters are the same for all sets, but each sets will update at a different time.
- If the directory contains a different version (older or newer), the set updates with this version
- If no binary file is available on the server, or the version is the same, nothing happens

The following settings are for the SIP configuration file template used for the phone upgrade at phone startup (no daily polling for automatic update).

```
<?xml version="1.0" encoding="UTF-8" ?>
<settings>
<setting id="DmAdmcfgUpdateTimeEnable" value="true" override="true"/>
<setting id="SIPServer1Address" value="TestSipDomain.sipserver.com" override="true"/>
<setting id="SIPGroup1DeviceUri" value="Testnumber" override="true"/>
<setting id="DmEnetcfgUpgradeFile" value="http://192.168.2.2/ale/firmware" override="true"/>
</settings>
```

1. Prepare the SIP configuration file and put it on the SIP provisioning server
2. Enter the firmware binary on the SIP provisioning server
3. Start the phone

   The phone downloads the SIP configuration file and reboots to enter the upgrading process. The phone reboots automatically after completing the entire upgrading process.
4. When the phone restarts, check that it has been upgraded to the desired version (see: Checking the software version of the phone set on page 9)

Chapter

11 Troubleshooting

11.1 Activating SSH

Some procedures in the following sections require to connect to the phone set via SSH. By default, SSH is deactivated and must be enabled via WBM, or `DmSecucfgSsh` parameter in the SIP configuration file of the phone set.

Once SSH is enabled, you can connect as admin by SSH. SSH login is "admin" and password is the same as admin password for MMI and WBM.

11.1.1 Activating SSH via WBM

1. Connect to the set WBM and go to: **Settings** > **Security** > **SSH**
2. Enable **SSH activation** and click **Apply**

11.1.2 Activating SSH via SIP configuration file

1. Download the target SIP configuration file from the HTTP/HTTPS provisioning server relative directory
2. Edit the SIP configuration file via a text editor
3. Insert or modify the `DmSecucfgSsh` command line as follows:

```
<setting id="DmSecucfgSsh" value="true" override="true"/>
```

4. Upload the target SIP configuration file to the HTTP/HTTPS provisioning server relative directory
5. Reboot the phone set

11.2 Terminal information check (mandatory)

It is mandatory to provide the terminal information for each issue.

```
$id full       // To get the hardware & software information
$config       // To get the phone configuration
```

11.3 Collecting debug information (getlogs command)

The `getlogs` command allows you to collect and store debug information (logs) in an archive file. By default, this archive file is stored in the `/tmp` folder, with its filename provided on the console.

```
getlogs [usb[fallback] | flash [leds|popup|onreboot]] [list|clean|help]
```

Where:

- `usb[fallback]`: default storage on USB disk with or without fallback to flash storage
- `flash`: default storage on flash storage
- `leds|popup`: to list LEDs or show a pop-up window when obtaining logs

- `onreboot`: to delay the request to obtain logs at the next reboot
- `list|clean`: to list or clean logs on flash storage

Examples:

- Get logs immediately. Logs are stored in the `/tmp` folder and do not survive a reset.

```
getlogs
############### ... building archive file ...
############### /tmp/00809FF7794C-logs-output.log
############### /tmp/00809FF7794C-logs.tar.gz
############### ... please wait for the prompt ...
############### WARNING !!! Since the /tmp folder is not flashed, the file will not survive a
reset ###############
############### /tmp/00809FF7794C-logs.tar.gz can now be downloaded
```

- Get logs immediately to USB key, provided that a USB disk is present.

```
getlogs usb
```

- Get logs immediately to flash (`/data/getlogs/`) that can survive a reset.

```
getlogs flash
```

- Get logs on to flash reboot. Logs are stored in `/data/getlogs`.

```
getlogs flash onreboot
```

- Get logs on to a USB disk on reboot. Logs are stored on the connected USB disk

```
getlogs usb onreboot
```

- Get logs on to a USB disk on reboot. Logs are stored on the connected USB disk or (if not present) on flash.

```
getlogs usb fallback onreboot
```

11.4 Collecting system logs

The following commands allow you to collect the system logs of the phones.

```
$ cd /log/
$ ls -l
$ tar cvzf /tmp/syslog.tgz *.*
```

Several types of system logs are stored in the folder `/log/`:

- `Defence.log`
- `Reset.log`
- `log.rcS`
- `pltf.log`
- `upgrade.log`

After executing above commands, you may download the `syslog.tgz` file under /tmp/ and send it to ALE International for further analysis.

11.5 Collecting SIP telephony trace

If the issue is related to SIP telephony, below commands are necessary for debugging.

The different trace levels are:

- `debug`
- `emerg`
- `err` (default level)
- `info`
- `notice`
- `warning`

The type of logs collected depends on the level: for example, the `err` level allows you to collect only the error logs, whereas the `debug` level allows you to collect all logs.

Note:

The `debug` level takes more CPU load and memory usage which has an impact on the phone performance. That's why the level should be set to `debug` only for debugging purposes, and should be set back to `err` when there are no more errors or after all the necessary log information has been captured.

To get the SIP general information and status:

```
$ dumpsip                  //To show the basic SIP settings
$ dumpTelephony          //To show the SIP telephony status
```

To check and set the trace level and collect the trace of telephony:

```
$ level                    //To show the trace level
   ACTIVITY          LEVEL      SUPPORT        DESTINATION
ApplicationManager   err        file       /var/log/ApplicationManager.log
ictaudio             err        file       /var/log/ictaudio.log
ICTCliGateLite       err        file       /var/log/ICTCliGateLite.log
ictsipua             err        file       /var/log/ictsipua.log
LoggerModule         err        file       /var/log/LoggerModule.log
no facility          err        file       /var/log/no facility.log
Platform             err        file       /var/log/Platform.log
SettingsManager      err        file       /var/log/SettingsManager.log
sipmmi               err        file       /var/log/sipmmi.log
Telephony            err        file       /var/log/Telephony.log   //location of Telephony log
$ level Telephony debug     //To set the Telephony log to debug level
```

11.6 Collecting core dump files after crash issue

If a crash issue is detected, collect the related core dump files as below:

```
$  cd /data/core/
$ ls -l
drwxrwxr-x      2 admin     admin           400 Jul 31   15:20 .
drwxr-xr-x      6 root      root            424 Aug  3    2017 ..
-rw-r--r--      1 root      root      332221 Jul 31 15:20 core.ictbtmgr.gz     //core dump file
-rw-r--r--      1 root      root      177122 Jul  4   2006 core.ictsipua.gz    //core dump file
-rw-r--r--      1 root      root      1335296 Jun 23 10:22 core.sipapp_mgr.gz  //core dump file
```

11.7 Collecting audio trace

To check and set the trace level and collect the trace of audio:

```
$ level                  //To show the trace level
```

```
  ACTIVITY              LEVEL      SUPPORT           DESTINATION
ApplicationManager      err        file       /var/log/ApplicationManager.log
ictaudio                err        file       /var/log/ictaudio.log    //location of ictaudio
log
ICTCliGateLite          err        file       /var/log/ICTCliGateLite.log
ictsipua                err        file       /var/log/ictsipua.log
LoggerModule            err        file       /var/log/LoggerModule.log
no facility             err        file       /var/log/no facility.log
Platform                err        file       /var/log/Platform.log
SettingsManager         err        file       /var/log/SettingsManager.log
sipmmi                  err        file       /var/log/sipmmi.log
Telephony               err        file       /var/log/Telephony.log
$ level ictaudio debug  //To set the ictaudio log to debug level
```

```
$ voicemode             //To check current voice mode.
$ rtp 0                 //To check current rtp status
$ rtp 1                 //To check current rtp status
```

11.8 Collecting dbus messages

The dbus messages deal with communications between different applications (processes) in the phone.

Export the dbus messages into a file as below, and download this file for ALE International analysis.

```
$ cd /tmp/
$ dbus-monitor > /tmp/dbuslog    //To save the dbus messages into a file.
```

11.9 Collecting trace after MMI issue

For MMI issues, it is better to record a video for better understanding.

To collect the trace for MMI:

```
$ level                 //To show the trace level
   ACTIVITY             LEVEL      SUPPORT          DESTINATION
ApplicationManager      err        file       /var/log/ApplicationManager.log
ictaudio                err        file       /var/log/ictaudio.log
ICTCliGateLite          err        file       /var/log/ICTCliGateLite.log
ictsipua                err        file       /var/log/ictsipua.log
LoggerModule            err        file       /var/log/LoggerModule.log
no facility             err        file       /var/log/no facility.log
Platform                err        file       /var/log/Platform.log
SettingsManager         err        file       /var/log/SettingsManager.log
sipmmi                  err        file       /var/log/sipmmi.log    //location of sipmmi log
Telephony               err        file       /var/log/Telephony.log
$ level sipmmi debug    //To set the sipmmi log to debug level
```

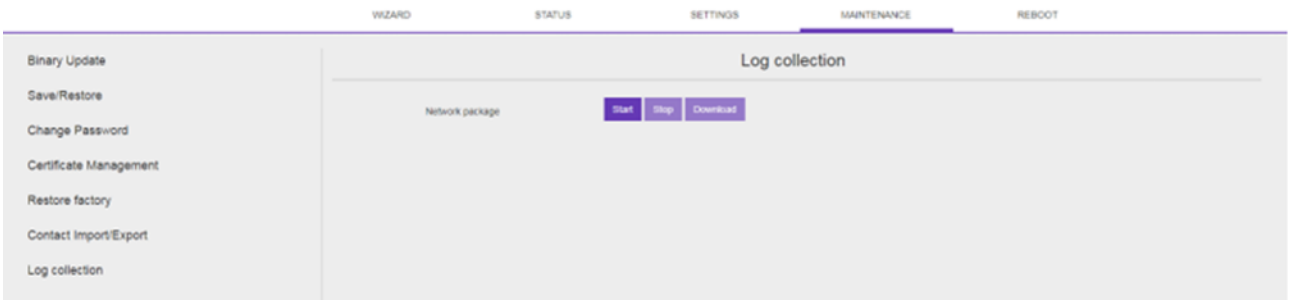
11.10 Accessing logs

You can retrieve the SIP phone log files from WBM or using a syslog server.

11.10.1 Accessing logs from the set Web Management

To capture network traces via WBM:

1. Log in to WBM and go to: **Maintenance** > **Log collection**

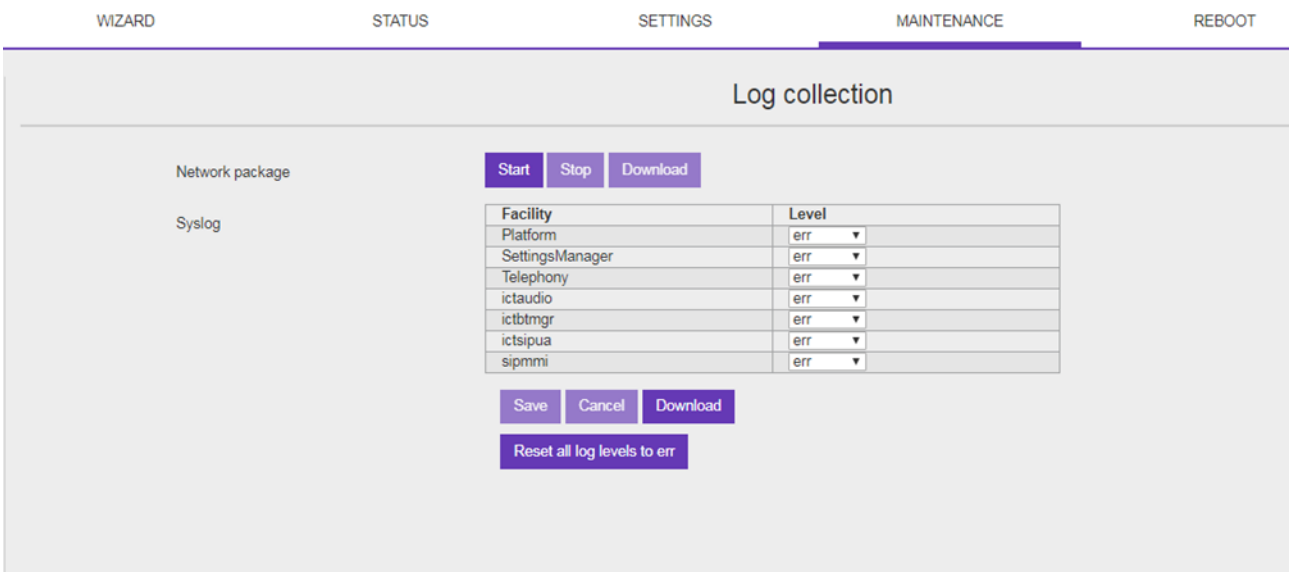


2. Press the **Start** button to start the network capturing

3. Once the capturing trace is done, press the **Download** button to save the trace on your PC

To set the log level and download logs via WBM:

1. Log in to WBM and go to: **Maintenance** > **Log collection**



2. Select the trace/log levels for the different facilities and click **Save**

Note:

The `debug` level takes more CPU load and memory usage which has an impact on the phone performance. That's why the level should be set to `debug` only for debugging purposes, and should be set back to `err` when there are no more errors or after all the necessary log information has been captured.

3. Click **Download** to save traces/logs on your PC

11.10.2 Accessing logs from a syslog server

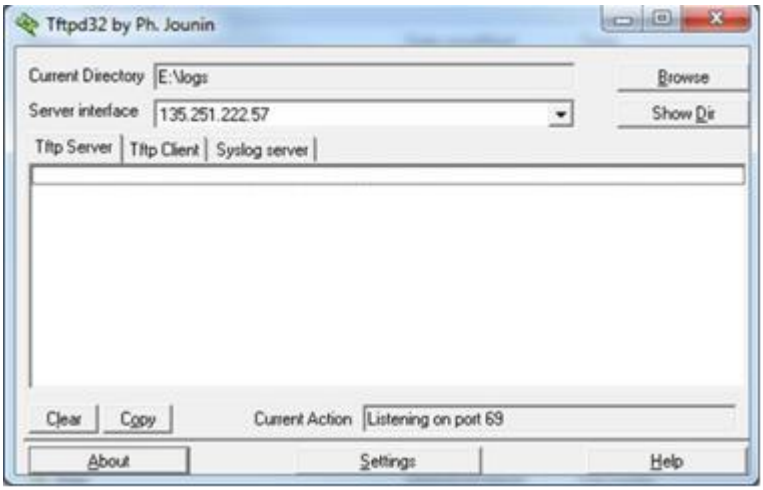
To retrieve SIP phone log files using a syslog server:

1. Connect to the device under test via SSH and login as admin

2. Use the following command to change all logs with debug level

```
$ level all debug
```

3. Install and start up a syslog server locally. For example:



4. Log in to WBM and go to: **Settings** > **Device** > **Net Log**
5. Fill in the related contents and enable **User netlog**

You will obtain the log files via syslog server.

11.11 Factory Reset

11.11.1 Factory reset from MMI

To perform a factory reset from the MMI:

1. On the phone set, press the navigator right key to display the menu list
2. Select **Advance Setting** and enter the password (default password:123456)
3. Press the navigator down key to display the last page and select **Restore factory**

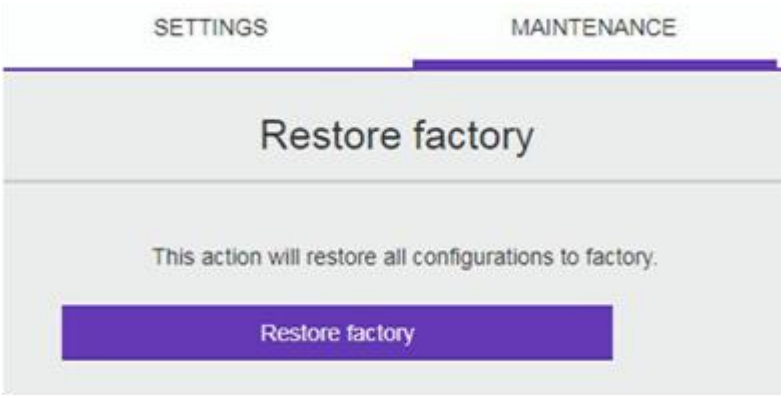
4. Select **OK** to confirm

11.11.2 Factory reset from WBM

To perform a factory reset from the phone web based interface:

1. Log in to WBM and go to: **Maintenance** > **Restore factory**

2. Click **Restore factory**



The phone restarts with all parameters restored to their factory values: this includes IP parameters and the set restarts in dynamic mode.

Chapter

12

Appendixes

12.1 SIP configuration file templates

The configuration file must be named as config.xxxxxxxxxxxx.xml, and xxxxxxxxxxxx is the mac address of the phone.

Note: Only Account1 configuration template involved in the following template. You can extend it to another 5 accounts as M Series DeskPhone supports 6 accounts.

```
<?xml version="1.0" encoding="UTF-8" ?>
 <settings>

                    <!--SIP Parameters-->
                    <setting id="SIPRegisterRetry" value="300" override="true"/>
                    <setting id="SIPLocalSipPort" value="5060" override="true"/>
                    <setting id="SIPLocalSipsPort" value="5061" override="true"/>
                    <setting id="SIPLocalSrtpPort" value="30000" override="true"/>
                    <setting id="SIPLocalSrtcpPort" value="30001" override="true"/>
                    <setting id="SIPLocalRtpPort" value="6000" override="true"/>
                    <setting id="SIPLocalRtcpPort" value="6001" override="true"/>

                    <!--Audio-->
                    <setting id="AudioToneCountry" value="1" override="true"/>
                    <setting id="AudioDtmfFeedbackEnable" value="false" override="true"/>
                    <setting id="AudioSidetoneHandset" value="0" override="true"/>
                    <setting id="AudioHearingAidEnable" value="false" override="true"/>
                    <setting id="Audiodiffserv" value="46" override="true"/>
                    <setting id="AudioUseCustomTone" value="false" override="true"/>

                    <!--Device Management Parameters-->
                    <setting id="DmAdmcfgCfgfilePollingEnable" value="true" override="true"/>
                    <setting id="DmAdmcfgCfgfilePollingTimeout" value="3600" override="true"/>
                    <setting id="DmEnetcfgDns1" value="" override="true"/>
                    <setting id="DmEnetcfgDns2" value="" override="true"/>
                    <setting id="DmLldpcfgPowerPriority" value="2" override="true"/>
                    <setting id="DmEnetcfgSntp" value="" override="true"/>
                    <setting id="DmEnetcfgSntpRefreshPeriod" value="3600" override="true"/>
                    <setting id="DmWpa8021xcfgMode" value="OFF" override="true"/>
                    <setting id="DmSecucfgPcPort" value="true" override="true"/>
                    <setting id="DmSecucfgPcPortVlanFilter" value="false" override="true"/>
                <setting id="DmSecucfgSsh" value="false" override="true"/>
                    <setting id="DmAdminPasswd" value="123456" override="true"/>
                    <setting id="DmSecucfgArpSpoofing" value="false" override="true"/>
                    <setting id="DmSecucfgArpSpoofingTimer" value="500" override="true"/>

                    <!--Firmware Upgrading-->
                    <setting id="FirmwareUpdate" value="1" override="true"/>
                    <setting id="DmEnetcfgUpgradeFile" value="" override="true"/>
                    <setting id="DmAdmcfgUpdateTimeEnable" value="true" override="true"/>
                    <setting id="DmAdmcfgUpdateTimeStart" value="04:00" override="true"/>
                    <setting id="DmAdmcfgUpdateTimeDelta" value="5" override="true"/>

                    <!--Dailing Rule-->
                    <setting id="DialingToneEnabled" value="true" override="true"/>
                    <setting id="Server1DialingRuleCountryCode" value="" override="true"/>
                    <setting id="Server1DialingRuleAreaCode" value="" override="true"/>
                    <setting id="Server1DialingRuleExternalPrefix" value="" override="true"/>
                    <setting id="Server1DialingRuleMinNumberLength" value="" override="true"/>
                 <setting id="Server1DialingRuleExternalPrefixExceptions" value="" override="true"/>

                    <!--Forward setting -->
                  <setting id="ForwardModeAccount" value="0" override="true"/>
                  <setting id="TelephonyFwdMethod1" value="0" override="true"/>
                <!--phone mode -->
                    <setting id="ForwardImmState" value="false" override="true"/>
                    <setting id="ForwardImmDest" value="" override="true"/>
                    <setting id="ForwardImmOnCode" value="" override="true"/>
                    <setting id="ForwardImmOffCode" value="" override="true"/>
```

```
    <setting id="ForwardBusyState" value="false" override="true"/>
    <setting id="ForwardBusyDest" value="" override="true"/>
<setting id="ForwardNoReplyState" value="false" override="true"/>
    <setting id="ForwardNoReplyDest" value="" override="true"/>
    <setting id="ForwardNoReplyOnCode" value="" override="true"/>
    <setting id="ForwardNoReplyOffCode" value="" override="true"/>

    <!--DND setting -->
 <setting id="DndModeAccount" value="0" override="true"/>
 <setting id="TelephonyDndMethod1" value="0" override="true"/>

    <!--phone mode -->
    <setting id="TelephonyDndState" value="false" override="true"/>
    <setting id="TelephonyDndOnCode" value="" override="true"/>
    <setting id="TelephonyDndOffCode" value="" override="true"/>

    <!--Account1 setting -->
    <!--Account1 SIP settings-->
    <setting id="SIPGroup1AuthenticationName" value="Registername" override="true"/>
    <setting id="SIPGroup1AuthenticationPassword" value="password" override="true"/>
    <setting id="SIPGroup1DeviceUri" value="Username" override="true"/>
<setting id="SIPGroup1DisplayName" value="display name" override="true"/>
    <setting id="SIPGroup1DtmfMode" value="2" override="true"/>
    <setting id="SIPGroup1SessionTimer" value="0" override="true"/>
    <setting id="SIPGroup1SessionTimerRefresher" value="0" override="true"/>
    <setting id="SIPGroup1SIPsURIUsage" value="false" override="true"/>
    <setting id="SIPGroup1SrtpWorkingMode" value="0" override="true"/>
    <setting id="SIPGroup1TLSAnticipation" value="false" override="true"/>
    <setting id="SIPGroup1TransportMode" value="0" override="true"/>
    <setting id="SIPGroup1ServerType" value="0" override="true"/>
    <setting id="SIPServer1Address" value="sip server address" override="true"/>
    <setting id="SIPServer1GenericPollingTimer" value="40" override="true"/>
    <setting id="SIPServer1GroupNumber" value="1" override="true"/>
    <setting id="SIPServer1KeepAliveEnable" value="true" override="true"/>
    <setting id="SIPServer1Port" value="5060" override="true"/>
    <setting id="SIPServer1RegisterExpire" value="3600" override="true"/>
    <setting id="SIPServer1FailoverAddress" value="" override="true"/>
    <setting id="SIPServer1FailoverPort" value="5060" override="true"/>
    <setting id="SIPServer1FailoverRegisterExpire" value="3600" override="true"/>
    <setting id="SIPServer1SwitchoverTimer" value="60" override="true"/>
    <setting id="TelephonyVmNumber1" value="" override="true"/>
    <setting id="SIPMessageWaitingIndicationUri1" value="" override="true"/>
    <!--Audio SIP account 1-->
    <setting id="AudioPayloadTypes1" value="101;96" override="true"/>
    <setting id="AudioVad1" value="false" override="true"/>
    <setting id="SIPPreferredVocoder1" value="0;8;18;9;98;125" override="true"/>
    <setting id="AudioPacketTime1" value="20;20;20;20;20;20" override="true"/>

    <!--Auto Answer account1-->
    <setting id="TelephonyInterphonyStatus1" value="false" override="true"/>

    <!--Intercom account1-->
    <setting id="SIPAutoAnsweredAllowed1" value="true" override="true"/>
    <setting id="SIPAutoAnsweredMute1" value="false" override="true"/>
    <setting id="SIPAutoAnsweredTone1" value="true" override="true"/>
    <setting id="SIPAutoAnsweredBarge1" value="false" override="true"/>
    <setting id="SIPGroup1IntercomType1" value="0" override="true"/>
<!--Dailing Rule Account 1-->
    <setting id="DialingRuleEnableHistory1" value="false" override="true"/>
    <setting id="DialingRuleEnableContact1" value="true" override="true"/>
    <setting id="DialingRuleEnableForward1" value="true" override="true"/>
    <setting id="DialingRuleEnableManual1" value="false" override="true"/>

 <!--custom mode account 1 -->
    <setting id="ForwardImmState1" value="false" override="true"/>
    <setting id="ForwardImmDest1" value="" override="true"/>
    <setting id="ForwardImmOnCode1" value="" override="true"/>
    <setting id="ForwardImmOffCode1" value="" override="true"/>
    <setting id="ForwardBusyState1" value="false" override="true"/>
    <setting id="ForwardBusyDest1" value="" override="true"/>
    <setting id="ForwardBusyOnCode1" value="" override="true"/>
<setting id="ForwardBusyOffCode1" value="" override="true"/>
    <setting id="ForwardNoReplyState1" value="false" override="true"/>
    <setting id="ForwardNoReplyDest1" value="" override="true"/>
    <setting id="ForwardNoReplyOnCode1" value="" override="true"/>
    <setting id="ForwardNoReplyOffCode1" value="" override="true"/>
```

```
<!--custom mode account 1-->
    <setting id="TelephonyDndState1" value="false" override="true"/>
    <setting id="TelephonyDndOnCode1" value="" override="true"/>
    <setting id="TelephonyDndOffCode1" value="" override="true"/>
 <!--LDAP-->
<setting id="LDAPEnabled" value="true" override="true"/>
<setting id="LDAPFieldsMapping" value="{ &quot;firstname&quot; :
&quot;givenname&quot;, &quot;name&quot; : &quot;sn&quot;, &quot;officephone&quot; :
&quot;telephonenumber&quot;}" override="true"/>
<setting id="LDAPLogin" value="default" override="true"/>
<setting id="LDAPPassword" value="default" override="true"/>
<setting id="LDAPServerUrl" value="" override="true"/>
<setting id="LDAPFilter" value="(|(givenname=*%1*)(sn=*%1*))" override="true"/>
<setting id="LDAPSearchBase" value="o=ALE,o=directoryRoot" override="true"/>

    <!--BLF resource list setting-->
    <setting id="BLFListInitPosType" value="" override="true"/>

    <!--Programm key-->
    <setting id="PhoneProgKey1Type" value="" override="true"/>
    <setting id="PhoneProgKey1Account" value="" override="true"/>
    <setting id="PhoneProgKey1Label" value="" override="true"/>
    <setting id="PhoneProgKey1Number" value="" override="true"/>
    <setting id="PhoneProgKey1Extension" value="" override="true"/>
    <setting id="PhoneProgKey2Type" value="" override="true"/>
    <setting id="PhoneProgKey2Account" value="" override="true"/>
    <setting id="PhoneProgKey2Label" value="" override="true"/>
    <setting id="PhoneProgKey2Number" value="" override="true"/>
    <setting id="PhoneProgKey2Extension" value="" override="true"/>
    <setting id="PhoneProgKey3Type" value="" override="true"/>
    <setting id="PhoneProgKey3Account" value="" override="true"/>
    <setting id="PhoneProgKey3Label" value="" override="true"/>
    <setting id="PhoneProgKey3Number" value="" override="true"/>
    <setting id="PhoneProgKey3Extension" value="" override="true"/>
    <setting id="PhoneProgKey4Type" value="" override="true"/>
    <setting id="PhoneProgKey4Account" value="" override="true"/>
    <setting id="PhoneProgKey4Label" value="" override="true"/>
    <setting id="PhoneProgKey4Number" value="" override="true"/>
    <setting id="PhoneProgKey4Extension" value="" override="true"/>
    <setting id="PhoneProgKey5Type" value="" override="true"/>
    <setting id="PhoneProgKey5Account" value="" override="true"/>
    <setting id="PhoneProgKey5Label" value="" override="true"/>
    <setting id="PhoneProgKey5Number" value="" override="true"/>
    <setting id="PhoneProgKey5Extension" value="" override="true"/>
    <setting id="PhoneProgKey6Type" value="" override="true"/>
     <setting id="PhoneProgKey6Account" value="" override="true"/>
    <setting id="PhoneProgKey6Label" value="" override="true"/>
    <setting id="PhoneProgKey6Number" value="" override="true"/>
    <setting id="PhoneProgKey6Extension" value="" override="true"/>
    <setting id="PhoneProgKey7Type" value="" override="true"/>
    <setting id="PhoneProgKey7Account" value="" override="true"/>
    <setting id="PhoneProgKey7Label" value="" override="true"/>
    <setting id="PhoneProgKey7Number" value="" override="true"/>
    <setting id="PhoneProgKey7Extension" value="" override="true"/>
    <setting id="PhoneProgKey8Type" value="" override="true"/>
    <setting id="PhoneProgKey8Account" value="" override="true"/>
    <setting id="PhoneProgKey8Label" value="" override="true"/>
    <setting id="PhoneProgKey8Number" value="" override="true"/>
    <setting id="PhoneProgKey8Extension" value="" override="true"/>
    <setting id="PhoneProgKey9Type" value="" override="true"/>
    <setting id="PhoneProgKey9Account" value="" override="true"/>
    <setting id="PhoneProgKey9Label" value="" override="true"/>
    <setting id="PhoneProgKey9Number" value="" override="true"/>
    <setting id="PhoneProgKey9Extension" value="" override="true"/>
    <setting id="PhoneProgKey10Type" value="" override="true"/>
    <setting id="PhoneProgKey10Account" value="" override="true"/>
    <setting id="PhoneProgKey10Label" value="" override="true"/>
    <setting id="PhoneProgKey10Number" value="" override="true"/>
    <setting id="PhoneProgKey10Extension" value="" override="true"/>
    <setting id="PhoneProgKey11Type" value="" override="true"/>
    <setting id="PhoneProgKey11Account" value="" override="true"/>
    <setting id="PhoneProgKey11Label" value="" override="true"/>
    <setting id="PhoneProgKey11Number" value="" override="true"/>
    <setting id="PhoneProgKey11Extension" value="" override="true"/>
    <setting id="PhoneProgKey12Type" value="" override="true"/>
    <setting id="PhoneProgKey12Account" value="" override="true"/>
```

```
                <setting id="PhoneProgKey12Label" value="" override="true"/>
                <setting id="PhoneProgKey12Number" value="" override="true"/>
                <setting id="PhoneProgKey12Extension" value="" override="true"/>
                <setting id="PhoneProgKey13Type" value="" override="true"/>
                <setting id="PhoneProgKey13Account" value="" override="true"/>
                <setting id="PhoneProgKey13Label" value="" override="true"/>
                <setting id="PhoneProgKey13Number" value="" override="true"/>
                <setting id="PhoneProgKey13Extension" value="" override="true"/>
                <setting id="PhoneProgKey14Type" value="" override="true"/>
                <setting id="PhoneProgKey14Account" value="" override="true"/>
                <setting id="PhoneProgKey14Label" value="" override="true"/>
                <setting id="PhoneProgKey14Number" value="" override="true"/>
            <setting id="PhoneProgKey14Extension" value="" override="true"/>
                <setting id="PhoneProgKey15Type" value="" override="true"/>
                <setting id="PhoneProgKey15Account" value="" override="true"/>
                <setting id="PhoneProgKey15Label" value="" override="true"/>
                <setting id="PhoneProgKey15Number" value="" override="true"/>
                <setting id="PhoneProgKey15Extension" value="" override="true"/>
                <setting id="PhoneProgKey16Type" value="" override="true"/>
                <setting id="PhoneProgKey16Account" value="" override="true"/>
                <setting id="PhoneProgKey16Label" value="" override="true"/>
                <setting id="PhoneProgKey16Number" value="" override="true"/>
                <setting id="PhoneProgKey16Extension" value="" override="true"/>
                <setting id="PhoneProgKey17Type" value="" override="true"/>
                <setting id="PhoneProgKey17Account" value="" override="true"/>
                <setting id="PhoneProgKey17Label" value="" override="true"/>
                <setting id="PhoneProgKey17Number" value="" override="true"/>
                <setting id="PhoneProgKey17Extension" value="" override="true"/>
                <setting id="PhoneProgKey18Type" value="" override="true"/>
                <setting id="PhoneProgKey18Account" value="" override="true"/>
                <setting id="PhoneProgKey18Label" value="" override="true"/>
                <setting id="PhoneProgKey18Number" value="" override="true"/>
                <setting id="PhoneProgKey18Extension" value="" override="true"/>
                <setting id="PhoneProgKey19Type" value="" override="true"/>
                <setting id="PhoneProgKey19Account" value="" override="true"/>
                <setting id="PhoneProgKey19Label" value="" override="true"/>
                <setting id="PhoneProgKey19Number" value="" override="true"/>
                <setting id="PhoneProgKey19Extension" value="" override="true"/>
                <setting id="PhoneProgKey20Type" value="" override="true"/>
                <setting id="PhoneProgKey20Account" value="" override="true"/>
                <setting id="PhoneProgKey20Label" value="" override="true"/>
                <setting id="PhoneProgKey20Number" value="" override="true"/>
                <setting id="PhoneProgKey20Extension" value="" override="true"/>

            <!--M3 Modle phones can't support below parameters of program key 21-28-->

                <setting id="PhoneProgKey21Type" value="" override="true"/>
                <setting id="PhoneProgKey21Account" value="" override="true"/>
                <setting id="PhoneProgKey21Label" value="" override="true"/>
                <setting id="PhoneProgKey21Number" value="" override="true"/>
                <setting id="PhoneProgKey21Extension" value="" override="true"/>
                <setting id="PhoneProgKey22Type" value="" override="true"/>
                <setting id="PhoneProgKey22Account" value="" override="true"/>
                <setting id="PhoneProgKey22Label" value="" override="true"/>
                <setting id="PhoneProgKey22Number" value="" override="true"/>
                <setting id="PhoneProgKey22Extension" value="" override="true"/>
                <setting id="PhoneProgKey23Type" value="" override="true"/>
                <setting id="PhoneProgKey23Account" value="" override="true"/>
                <setting id="PhoneProgKey23Label" value="" override="true"/>
                <setting id="PhoneProgKey23Number" value="" override="true"/>
                <setting id="PhoneProgKey23Extension" value="" override="true"/>
                <setting id="PhoneProgKey24Type" value="" override="true"/>
                <setting id="PhoneProgKey24Account" value="" override="true"/>
                <setting id="PhoneProgKey24Label" value="" override="true"/>
                <setting id="PhoneProgKey24Number" value="" override="true"/>
                <setting id="PhoneProgKey24Extension" value="" override="true"/>
                <setting id="PhoneProgKey25Type" value="" override="true"/>
                <setting id="PhoneProgKey25Account" value="" override="true"/>
                <setting id="PhoneProgKey25Label" value="" override="true"/>
                <setting id="PhoneProgKey25Number" value="" override="true"/>
                <setting id="PhoneProgKey25Extension" value="" override="true"/>
                <setting id="PhoneProgKey26Type" value="" override="true"/>
                <setting id="PhoneProgKey26Account" value="" override="true"/>
              <setting id="PhoneProgKey26Label" value="" override="true"/>
                <setting id="PhoneProgKey26Number" value="" override="true"/>
                <setting id="PhoneProgKey26Extension" value="" override="true"/>
                <setting id="PhoneProgKey27Type" value="" override="true"/>
```

```
                    <setting id="PhoneProgKey27Account" value="" override="true"/>
                    <setting id="PhoneProgKey27Label" value="" override="true"/>
                    <setting id="PhoneProgKey27Number" value="" override="true"/>
                    <setting id="PhoneProgKey27Extension" value="" override="true"/>
                    <setting id="PhoneProgKey28Type" value="" override="true"/>
                    <setting id="PhoneProgKey28Account" value="" override="true"/>
                    <setting id="PhoneProgKey28Label" value="" override="true"/>
                    <setting id="PhoneProgKey28Number" value="" override="true"/>
                    <setting id="PhoneProgKey28Extension" value="" override="true"/>

</settings>
```

12.2 Description of the SIP settings in configuration file

Sections below give a description for the main SIP settings in the configuration file. The list of settings is not exhaustive.

12.2.1 Firmware upgrading

Parameter	Default	Value range	Mandatory	Description
DmEnetcfgUpgradeFile			N	Downloading URL for firmware binary files
DmAdmcfgUpdateTimeEnable	false	true; false	N	True: the phone will check the binary version. If different from current version, the upgrading process will be triggered. False: the phone will not check the binary information any more.
DmAdmcfgUpdateTimeStart	00:00		N	Defines when the phone will check if the binary has changed during the last 24 hours. Time format supported: HH:MM
DmAdmcfgUpdateTimeDelta	0	[0,1440]		In order to prevent all terminals from starting an upgrade at the same time, this setting will add a random value between 0 and 1440 min before the value defined with DmAdmcfgUpdateTime Start. In this way, upgrade parameters can be configured with the same values for all sets, but each sets will update at different time.

12.2.2 SIP servers/groups/accounts

Note:

SIP Group1/Server1 is mandatory for the main SIP server (other groups are not described in this document)

Parameter	Default	Value range	Mandatory	Description
SIPServer1Address			Y	SIP Server1 address
SIPServer1Port	5060	0-65535	N	SIP Server1 port number for registration
SIPServer1GroupNumber	1	1-4	N	Group number of this SIP Server1
SIPGroup1ServerType	0	0:Default 4:swyx 5:uaCSTA 6:BroadSoft 7:Asterisk 8:3cx 9:SIPWISE 10.MetaSwitch	N	Server type for group1 Note: DO NOT USE 1,2,3 which are ALEInternational solutions
SIPGroup1DomainName			N	Group1 SIP server domain name
SIPGroup1AuthenticationRealm			N	Group1 SIP authentication realm
SIPGroup1AuthenticationName			N	Group1 SIP authenticate name. Mandatory if SIP server requests authentication
SIPGroup1AuthenticationPassword			N	Group1 SIP authenticate password Mandatory if SIP server requests authentication
SIPGroup1DisplayName			N	Group1's display name
SIPGroup1DtmfMode	2	0:None 1:InBand 2:RFC2833 3:RFC4733 4:SIP_INFO 5:SIP_INFO +RFC2833		Defines the DTMF mode
SIPGroup1DeviceUri			Y	Group1's device URL used for registration

12.2.3 Outbound proxy

In some network topologies, outbound proxy will be used for SIP registration. The related parameters to be used in the case are listed below.

Parameter	Default	Value range	Mandatory	Description
SIPGroup1OutBoundProxyAddress			N	Outbound proxy address for group1
SIPGroup1OutBoundProxyPort	5060	0-65535	N	Outbound proxy port for group1 *Note:* *The DNS SRV will be enabled while set port 0 with valid outbound proxy.*

12.2.4 SIP-TLS/SRTP

To deploy the phone to be working in SIP-TLS & SRTP mode, below parameters should be configured in that sip Group.

Parameter	Default	Value range	Mandatory	Description
SIPGroup1TransportMode	0	0:UDP 1:TCP 2:TLS	N	Protocol used on transport layer for server group1
SIPGroup1SrtpWorkingMode	0	0:none 1:Best effort 2:Strict	N	SRTP mode used on transport layer for server group1
SIPCertificateUrl			N	URL for download the SIP server certificate
SIPSslPeerVerify	false	true false	N	Whether to enable the peer verify for SIPs
SIPSslVersion	0	0: All 1: TLS1.0 2: TLS1.2	N	SSL version supported by terminal

12.2.5 Management of SSL connection

Parameter	Default	Value range	Mandatory	Description
DmSecucfgSsh	false	true false	N	Enables SSH connections
DmAdminPasswd			N	Used to set password for the user **admin**

12.2.6 SNTP&Timezone

Parameter	Default	Value range	Mandatory	Description
DmEnetcfgSntp			N	SNTP Server
DmAdmcfgTimeZoneUtoffset		-11:00 -10:00 -9:30 -9:00 -8:00 -7:00 -6:00 -5:00 -4:30 -4:00 -3:30 -3:00 -2:30 -2:00 -1:00 0 +1:00 +2:00 +3:00		Offset time from UTC time

		+3:30 +4:00 +4:30 +5:00 +5:30 +5:45 +6:00 +6:30 +7:00 +8:00 +8:45 +9:00 +9:30 +10:00 +10:30 +11:00 +11:30 +12:00 +12:45 +13:00 +13:30 +14:00		
DmAdmcfgTimeZoneLocation				Country or area name of time zone, useful when DST enable is auto
DmAdmcfgDstEnable	0	0,1		0 is disable, 1 is enable
DmAdmcfgDstType	week	Week date		DST is set by week or by date
DmAdmcfgDstStartMonth	Jan	Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec		
DmAdmcfgDstStartWeek	5	1,2,3,4,5		1 is first, 2 is second, 3 is third, 4 is fourth, 5 is last
DmAdmcfgDstStartDate	1			
DmAdmcfgDstStartHour	0	[0.23]		
DmAdmcfgDstEndMonth	Dec	Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec		
DmAdmcfgDstEndWeek	5	1,2,3,4,5		1 is first, 2 is second, 3 is third, 4 is fourth, 5 is last
DmAdmcfgDstEndDate	30			
DmAdmcfgDstEndHour	23	[0,23]		
DmAdmcfgDstOffset	60	[-300,300]		Offset time when DST is on, in minutes

12.2.7 Customized logo of screensaver

Parameter	Default	Value range	Mandatory	Description
ScreensaverLogoURL			N	URL for download the customized Logo of screen saver

12.2.8 LDAP

Parameter	Default	Value range	Mandatory	Description
PhoneProgKey[1,28]Type	0	0 - Not Used 1 - Speed Dial 59 - BLF 2 - BLF List 3 - Do Not Disturb 4 - Directory 5 - VoiceMail 6 - Conference 7 - Forward 8 - Transfer 9 - Group Listening 10 - HeadSet 11 - Hot Desking 12 - Phone Lock 13 - Prefix 14 - DTMF 15 - Direct Pickup 16 - Group Pickup 17 - Call Park 18 - Recall 19 - XML Browser 21 - Intercom 23 - AudioHub 58 - Hold 60 - Account	N	The type of phone program key
PhoneProgKey[1,28]Account	1	1-8	N	The account index of phone program key. 1: Account 1 2: Account 2 3: Account 3 4: Account 4 5: Account 5 6: Account 6 7: Account 7 8: Account 8
PhoneProgKey[1,28]Label			N	The label of phone program key
PhoneProgKey[1,28]Number			N	The number of phone program key
PhoneProgKey[1,28]Extension			N	The extension of phone program key

END OF DOCUMENT