Cisco IP Phone 6800, 7800, and 8800 Series Multiplatform Phones Troubleshooting FAQ
Contents

How to – Disable the initial credentials prompt after a factory reset? ........................................3
How to – Upgrade the firmware on the phone? ...........................................................................3
  Upgrade the firmware manually and locally, using TFTP or HTTP ........................................3
  Upgrade the firmware using a Provisioning Server ...............................................................6
How to – Upgrade the phone to certain level of firmware based on current firmware version? ........6
Where can I find the list of root CAs that the phone supports for SSL/TLS? .............................7
Where can I find documentation for MPP phones and Broadworks? .......................................7
How to – Factory reset MPP Phone? .......................................................................................7
How to – Install custom security certificates? ..........................................................................8
How to – Generate a Problem Report Tool (PRT) file? ............................................................8
How to – Take a Packet Capture (PCAP) using the MPP Phone? ............................................10
How to – Look at the running configuration on MPP phone (cfg.xml)? ..................................10
How to – Set debug level to DEBUG? ....................................................................................11
How to – Restrict access to parts of the Phone UI and User Web UI? .....................................12
  Set Phone UI User Mode to “Yes” ....................................................................................12
  Change the attributes you would like to restrict user access to ...........................................12
Time format not working as expected ....................................................................................13
  Time format settings priorities .......................................................................................14
How do conditional expressions work? (upgrades rules and profile rules) ...............................14
  Comparing Version Numbers .....................................................................................15
Operators .........................................................................................................................15
Examples ..........................................................................................................................15
Can I upgrade MPP phones from 10.X to 11.1.X and above? .................................................15
Dial Plan ............................................................................................................................16
  Overview .....................................................................................................................16
  Default dial plan .......................................................................................................16
  Dial Plan Examples ..................................................................................................16
Timers ...................................................................................................................................16
  Interdigit Timeout ......................................................................................................17
Can we convert Cisco Phones from MPP to Enterprise and vice versa? ....................................17
Does MPP support multiple directories? ...............................................................................18
How to configure LDAP? ......................................................................................................19
How to configure LDAP directory over TLS? ........................................................................20
Does MPP support Broadworks XSI Directory Reverse Name Lookup for inbound calls? .......21
Reverse Name Lookup for Incoming and Outgoing Calls .....................................................21
  Enable and Disable Reverse Name Lookup ..................................................................21
How does EDOS work and how to setup? ...........................................................................22
How to – Disable the initial credentials prompt after a factory reset?
When you factory reset a phone, by default, after the phone boots up, it will prompt you to set a password.
(Screenshot taken from a 6851).

There are two ways of disabling the above prompt. You can set the parameter from DMS, or you can set it manually on the Phone Web UI. Follow the below instructions

1. To disable using the provisioning server, set the below parameter to “No”:

   `<User_Password_Prompt ua="na">No</User_Password_Prompt>`

2. To disable via the Web UI, navigate to http://IP_ADDRESS_PHONE/admin/advanced
3. Go to Voice → System and set User Password Prompt to No

How to – Upgrade the firmware on the phone?
Upgrade the firmware manually and locally, using TFTP or HTTP

1. Download the desired firmware files from Cisco CCO (the following example uses firmware version 11.2.3MSR1-1)
2. Extract the zip file and save it to the TFTP or HTTP root folder (In this case the example shows the root folder of a Windows with an HTTP server enabled)

3. Login to http://IP_ADDRESS_PHONE/admin/advanced
4. Navigate to Voice   Provisioning
5. Scroll down to Firmware Upgrade and populate the Upgrade Rule with the location of the loads file, using the IP address of the TFTP/HTTP server in place of the one in the example (in this example http://10.10.30.104:8080/Cisco/cmterm-88xx.11-2-3MSR1-1_REL/sip88xx.11-2-3MSR1-1_loads is used)
6. Click on Submit All Changes. The phone should now download all the upgrade files and reboot. The time is dependent on the speed of the network connection/how fast the server can serve the files etc.

7. Verify if the upgrade was successful
Upgrade the firmware using a Provisioning Server

If your upgrade files are hosted on a provisioning server, you can push the upgrade rule from the server, pointing the phone to the appropriate upgrade URL.

An example of the parameter to set on your template file:

```
<Upgrade_Rule ua="na">http://DMS_ADDRESS/dms/spa7811-3PCC/sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>
```

How to – Upgrade the phone to certain level of firmware based on current firmware version?

In some occasions, you might need to upgrade the phone to a certain version of firmware based on its current version.

For instance, if you have any phones which are running on a firmware less or equal to sip78xx.11-0-0MPP-7 and you would like to upgrade to sip78xx.11-2-1MES-3, but at the same time, if you have phones which are
running a firmware greater or equal to sip78xx.11-2-1MES-3, and you would like to upgrade to sip78xx.11-3-1MES-1. You can use the below conditional upgrade rule:

\[
<\text{Upgrade Rule}\> (\$\text{SWVER le sip78xx.11-0-0MPP-7})? \text{http://DMS_SERVER/sip78xx.11-2-1MES-3.loads} \mid (\$\text{SWVER ge sip78xx.11-2-1MES-3})? \text{http://DMS_SERVER/sip78xx.11-3-1MES-1.loads}</\text{Upgrade Rule>}
\]

Conditions are highlighted on different colours above.

For more information, you can refer to the Conditional Expressions section of the Provisioning guide:


Where can I find the list of root CAs that the phone supports for SSL/TLS?
The trusted root stores can be found at the following URL:

https://www.cisco.com/security/pki/

These certificate bundles are the CAs that the phone will trust to issue certificates for servers/nodes being connected to from the phone.

Where can I find documentation for MPP phones and Broadworks?

Documentation for MPP phones can be found at the Cisco.com website.

There are several guides available such as (the below examples are for the 8800 series):

- Administration Guide
- Provisioning Guide
- End User Guide

You can also find the Partner Configuration Guide (PCG) at the https://xchange.broadsoft.com/website.

- https://xchange.broadsoft.com/node/1031047

How to – Factory reset MPP Phone?

There are three ways you can Factory Reset your phone

1. Using the Phone UI
   - Navigate to Settings → Device Administration → Factory Reset
2. Using the Web UI
   - Login to http://IP_ADDRESS_PHONE/admin/advanced
   - Go to Info → Debug Info
   - Click on Factory Reset
3. Using the URL

How to – Install custom security certificates?
In order to install a custom certificate to the MPP phone, you will need to configure the XML file to fetch the Custom CA Rule to the phone. See an example below:

```xml
<Custom_CA_Rule
  ua="na">http://IP_ADDRESS/Cisco/crca2099.pem</Custom_CA_Rule>
```

Verify that the Custom CA has been installed correctly.

1. Login to http://IP_ADDRESS_PHONE/admin/advanced/
2. Navigate to Info → Download Status

How to – Generate a Problem Report Tool (PRT) file?

1. Login to http://IP_ADDRESS_PHONE/admin/advanced/
2. Navigate to Info → Debug Info → Generate PRT
3. Select the Problem Description (if not sure, select “Other”)

4. Download the PRT file
How to – Take a Packet Capture (PCAP) using the MPP Phone?

1. Login to http://IP_ADDRESS_PHONE/admin/advanced/
2. Navigate to Info → Debug Info → Start Packet Capture

3. Download the PCAP file

FYI – the pcap is done at a wire level, not at an application level, therefore traffic encrypted by the phone will appear as encrypted frames in the generated pcap file.

How to – Look at the running configuration on MPP phone (cfg.xml)?

How to – Set debug level to DEBUG?

1. Login to http://IP_ADDRESS_PHONE/admin/advanced
2. Navigate to Voice → System → Debug Level (The exact location of the Debug Level option might vary within this page, depending on the phone model)
3. Click on Submit All Changes
How to – Restrict access to parts of the Phone UI and User Web UI?

It is possible to restrict the user access to the Web UI and Phone UI by changing the User Access (ua) attributes.

- Connection_Type ua=“rw”, you can read and change the information on the user phone web and phone screen.
- Connection_Type ua=“ro”, you can only read, not change, the information on the user phone web and phone screen.
- Connection_Type ua=“na”, you cannot access the information on the user phone web or phone screen.

Please note: In order for the phone to honour the User Access attributes, you have to set Phone UI User Mode to “Yes”

Set Phone UI User Mode to “Yes”
1. Select Voice → System.
2. Under System Configuration in the Phone-UI-User-Mode field, choose Yes.
3. Click Submit All Changes.

You may also change the below parameter in the xml file:

- `<Phone-UI-User-Mode ua="na">Yes</Phone-UI-User-Mode>`

Change the attributes you would like to restrict user access to

In this example, I will be restricting user access to Speed Dials.

Below is a screen shot of the phone screen before the change:
1. In the XML resync file, change the user attribute from “rw” or “ro” to “na”

```xml
<!-- Speed Dial -->
<Speed_Dial_2_Name ua="na"/>
<Speed_Dial_2_Number ua="na"/>
<Speed_Dial_3_Name ua="na"/>
<Speed_Dial_3_Number ua="na"/>
<Speed_Dial_4_Name ua="na"/>
<Speed_Dial_4_Number ua="na"/>
<Speed_Dial_5_Name ua="na"/>
<Speed_Dial_5_Number ua="na"/>
<Speed_Dial_6_Name ua="na"/>
<Speed_Dial_6_Number ua="na"/>
<Speed_Dial_7_Name ua="na"/>
<Speed_Dial_7_Number ua="na"/>
<Speed_Dial_8_Name ua="na"/>
<Speed_Dial_8_Number ua="na"/>
<Speed_Dial_9_Name ua="na"/>
<Speed_Dial_9_Number ua="na"/>
```

After the change is made and the phone downloaded the new config file from the server, you will notice that the speed dial option has been removed from the phone interface. See below:

Restricting access to speed dials is only an example of what can be restricted. The same settings would also apply to a large variety of attributes in the phone.

**Time format not working as expected**

There are a number of reasons why the time format might be displayed incorrectly on the phone interface. It is important to understand at this point, what time format settings takes priority.

There are three ways time format can be set on the phone.
1. By default (phone out of the box), time format is set by the Language Selection and locale, so for instance, if your language selection is French and Locale is set to fr-FR, time format will be set to 24h by default. If your language selection is English-US and Locale is set to en-US, time format will be 12h. (bear in mind that out of the box default will be English-US and en-US, so time format will be 12h.

2. You can set it up manually on Web UI or Phone UI. See example below:

   ![Time settings](image)

   Set

   Time format  12hr
   Date format   day/month

3. Time format can also be set by your provisioning server, by setting the below parameter:

   `<Time_Format ua="rw">12hr</Time_Format>`

Time format settings priorities

1. If time format is being set from DMS, it will always take priority over User settings or Locale.
2. When time format is NOT set on DMS (meaning that the parameter shown above is removed from the configuration file), the phone will pick up the standard from the Language Selection and Locale settings.
3. If time format is NOT being set from DMS, User settings will take priority over Locale. This means that the user will be able to change the time format and the change will be consistent after resyncs and reboots.

How do conditional expressions work? (upgrades rules and profile rules)

Conditional expressions can be used to apply a particular profile rule or upgrade rule, based on various factors, for example the phone model or firmware version.
Comparing Version Numbers
Multiplatform phones (MPP) formal release software version uses this format, where BN==Build Number:

- sip88xx.v1-v2-v3MPP-BN

The comparing string must use the same format. Otherwise, it results in a format parsing error.
In the software version, v1-v2-v3-v4 can specify different digits and characters, but must start with a numeric digit. When comparing the software version, v1-v2-v3-v4 is compared in sequence, and the leftmost digits take precedence over the latter ones.
If v[x] includes only numeric digits, the digits are compared; if v[x] includes numeric digits + alpha characters, digits are compared first, then characters are compared in alphabetical order.

Example of Valid Version Number:
- sipyyyy.11-0-0MPP-BN

Example comparison:
sip88xx.11-0-0MPP-BN > sip88xx.9-3-1-7MPP-BN

Operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>Alternate Syntax</th>
<th>Description</th>
<th>Applicable to Integer and Version Operands</th>
<th>Applicable to Quoted String Operands</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>eq</td>
<td>equal to</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>!=</td>
<td>ne</td>
<td>not equal to</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>&lt;</td>
<td>lt</td>
<td>less than</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>&lt;=</td>
<td>le</td>
<td>less than or equal to</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>&gt;</td>
<td>gt</td>
<td>greater than</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>&gt;=</td>
<td>ge</td>
<td>greater than or equal to</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>AND</td>
<td></td>
<td>and</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Examples
In the example below, the rule checks if the phone’s firmware is greater or equal to sip78xx.11-0-0MPP-7. If this is true, then the phone will upgrade to sip78xx.11-2-1MES-3.loads, otherwise ("|" is used to denote the next possible result), it will upgrade to sip78xx.11-0-0MPP-7.loads.

<Upgrade_Rule ua="na">($SWVER ge sip78xx.11-0-0MPP-7)? HTTP://SERVER_ADDRESS/sip78xx.11-2-1MES-3.loads| HTTP://SERVER_ADDRESS/sip78xx.11-0-0MPP-7.loads </Upgrade_Rule>

Can I upgrade MPP phones from 10.X to 11.1.X and above?
In order to upgrade from 10.X such as 10.4 firmware to 11.1.X and above, we need to upgrade to 11.0.0 first. It’s a double jump upgrade.
We can either upgrade the phone manually, which does not scale well, or configure the upgrade rule with a conditional expression in order to do so.

For more information on how conditional expressions work, please refer to “How do conditional expressions work (upgrades rules and profile rules)” section in the FAQ guide.

Dial Plan

Overview
Dial plans determine how digits are interpreted and transmitted. They also determine whether the dialled number is accepted or rejected. You can use a dial plan to facilitate dialling or to block certain types of calls such as long distance or international.

A dial plan contains a series of digit sequences, separated by the | character. The entire collection of sequences is enclosed within parentheses. Each digit sequence within the dial plan consists of a series of elements that are individually matched to the keys that the user presses.

White space is ignored but can be used for readability.

Default dial plan
All phones will come with a default US dial plan as follows:

- (*xx)[3469]11\0(2-9)xxxxxx|1xxx(2-9)xxxxxxS0|xxxxxxxxxxx.)

Dial Plan Examples

- (*xx)#xx|x.
- *xx|#xx|x. |+x.
- (*xx|#xx|+x.)
- (P60|xx. |+x. |*x. |*x. |*x. )
- (xx|[3469]11\0|00|[2-9]xxxxxx|1xxx(2-9)xxxxxxS0|xxxxxxxxxxx. |#xx. |#xx. |#xx. )
- (*#xx|*xx#|*xx*|*xx|*xx|*xx.|#xx.|0[1-9]xxxxxxxS0|00[1-9]|x.|157150|118xx|99950|11250|x. |+x.)

Timers
Off-Hook timer settings can be configured in two places. Directly in the dial plan string or in the Dial Tone configuration.

- SYNTAX: (Ps:<n> | dial plan)

s: The number of seconds; if no number is entered after P, the default timer of 10 seconds applies. With the timer set to 0 seconds, the call transmits automatically to the specified extension when the phone goes off hook.

n: (optional): The number to transmit automatically when the timer expires; you can enter an extension number or a DID number. No wildcard characters are allowed because the number is transmitted as shown. If you omit the number substitution, <n>, the user hears a reorder (fast busy) tone after the specified number of seconds.

- <Dial_Plan_1_ ua="">({P60}|(xx. |+x. |*x. |#x. |*x. ))</Dial_Plan_1_>
It can also be configured by modifying the value highlighted below.

- `<Dial_Tone ua="na">350@-19,440@-19;60(/0/1+2)</Dial_Tone>`

Interdigit Timeout
There are two interdigit timers on the phone, the interdigit long timer and the interdigit short timer.

This interdigit long timer applies as long as the dialled digits do not match any digit sequences in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated as incomplete, and the call is rejected. The default value for the interdigit long timer is 10 seconds.

The interdigit short timer applies when the dialled digits match at least one digit sequence in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated. If the entry is valid, the call proceeds. If the entry is invalid, the call is rejected. The default value for the interdigit short timer is 3 seconds.

Both the interdigit long and interdigit short timers can be changed using a L and S value respectively at the start of the dial plan, similar syntax as the off hook timer value (a P value at the start of the dial plan).

Can we convert Cisco Phones from MPP to Enterprise and vice versa?
It is possible to convert Cisco IP Phones 78xx/88xx to Multiplatform Phones (MPP) and vice versa by using the Cisco upgrade tool [https://upgrade.cisco.com](https://upgrade.cisco.com).
Does MPP support multiple directories?
Cisco MPP phones support the following directories:

- XSI Directory
  - Enterprise
  - Group
  - Personal
  - Enterprise Common
  - Group Common
- LDAP Directory
- XML Directory
- Local Directory (Personal Address Book)

As from 11.2.3 firmware, it is possible to search across all XSI directories by using the search All feature (Search ALL, will only search XSI. It will now work with any other directory types.

Please note that its only possible to display one XSI directory option at once.

All directories, with exception of Personal Directory, can be configured under **Voice ➔ Phone**

The Personal Directory can be configured by the user using the Web UI or the Phone UI.
How to configure LDAP?

1. Login to http://IP_ADDRESS_PHONE/admin/advanced
2. Navigate to **Voice → Phone → LDAP**
3. Set **LDAP Dir Enable** to **Yes**
4. Fill out the following fields with their respective values based on your LDAP Server
<LDAP_Dir_Enable ua="na">Yes</LDAP_Dir_Enable>
<LDAP_Corp_Dir_Name ua="na">LDAP Directory</LDAP_Corp_Dir_Name>
<LDAP_Server ua="na">10.10.10.123:389</LDAP_Server>
<LDAP_Search_Base ua="na">OU=001 Cisco Users; DC=domain; DC=com</LDAP_Search_Base>
<LDAP_Client_DN ua="na">ldapaccount@domain.com</LDAP_Client_DN>
<LDAP_Username ua="na">ldapaccount@domain.com</LDAP_Username>
<!-- <LDAP_Password ua="na">*************</LDAP_Password> -->
<LDAP_Auth_Method ua="na">Simple</LDAP_Auth_Method>
<LDAP_Last_Name_Filter ua="na">sn:(sn=$VALUE*)</LDAP_Last_Name_Filter>
<LDAP_First_Name_Filter ua="na">cn:(cn=$VALUE*)</LDAP_First_Name_Filter>
<LDAP_Search_Item_3 ua="na">
<LDAP_Item_3_Filter ua="na"/>
<LDAP_Display_Attrs ua="na">a=givenName,n=Firstname;a=sn,n=Lastname;a=telephoneNumber,n=Office,t=p;a=mobile,n=Mobile,t=p; a=homePhone,n=Home,t=p; a=mail, n=Email</LDAP_Display_Attrs>
<LDAP_Number_Mapping ua="na"/>

Please note that the above configuration is an example only. Configuration format for any of the fields above might vary according to your infrastructure.

How to configure LDAP directory over TLS?

1. Login to http://IP_ADDRESS_PHONE/admin/advanced
2. Navigate to Voice → Phone
3. In the LDAP section, enter a server address in the Server field.

For example, enter ldaps://<ldaps_server>[:port]

where:
- ldaps:// = The server string starts with ldaps:// before you enter the IP address or domain name
- ldaps_server = IP address or domain name
- port = Port number. Default: 636
Does MPP support Broadworks XSI Directory Reverse Name Lookup for inbound calls?

No.

Reverse Name Lookup for Incoming and Outgoing Calls
Reverse name lookup searches for the name of a number in an incoming, outgoing, conference, or transfer call. The reverse name lookup acts when the phone cannot find a name using the service provider directory, Call History, or your contacts. Reverse name lookup needs a valid LDAP Directory or XML Directory configuration.

The reverse name lookup searches the phone's external directories. When a search succeeds, the name is placed in the call session and in the call history. For simultaneous, multiple phone calls, reverse name lookup searches for a name to match the first call number. When the second call connects or is placed on hold, reverse name lookup searches for a name to match the second call.

Reverse name lookup is enabled by default.

Reverse name lookup searches the directories in the following order:

1. Phone contacts
2. Call History
3. LDAP Directory
4. XML Directory

Please note, the phone searches the XML directory using this format:
directory_url?n=incoming_call_number

Example: For a multiplatform phone using a third-party service, the phone number (1234) search query has this format, http://your-service.com/dir.xml?n=1234

Enable and Disable Reverse Name Lookup
Before enabling or disabling Reverse Name Lookup, be sure to configure one of the following:

- LDAP Corporate Directory
- XML Directory

1. Login to http://IP_ADDRESS_PHONE/admin/advanced
2. Navigate to Voice → Phone
3. In the Supplementary Services area, set the Reverse Phone Lookup Serv to:
   - Yes — Enable the reverse name lookup feature.
• **No** – Disable the reverse name lookup feature.

You can also configure Reverse Name Lookup via the xml file:

```xml
<Reverse_Phone_Lookup_Service ua="na">Yes</Reverse_Phone_Lookup_Service>
```

**How does EDOS work and how-to setup?**

**Introduction**

EDOS is a Cisco Cloud provisioning platform used for Zero Touch Provisioning. It automatically provisions the device out of the box and provides a “plug and play” user experience.

**Behind the scenes**

1. Service Provider/Distributor creates a Profile before / during the order process to ensure all the MAC addresses get automatically mapped to the profile when order is shipped.
2. Once customer receives the device and plugs into the network, device calls Cisco Cloud/RC EDOS server.
3. Cisco Cloud looks up profile based on device’s MAC address, then provides profile to device.
4. Device is redirected to the SP Provisioning Server.
5. SP Provisioning Server provides configuration information to device.
Sample EDOS Configuration Profile

```xml
<?xml version="1.0" encoding="UTF-8"?>
<device>
  <flat-profile>
    <Primary_DNS>12.45.67.89</Primary_DNS>
    <Provision_Enable>Yes</Provision_Enable>
    <Resync_On_Reset>Yes</Resync_On_Reset>
    <Resync_Periodic>7200</Resync_Periodic>
    <Resync_Error_Retry_Delay>30</Resync_Error_Retry_Delay>
    <Profile_Rule>http://yourserver.com/$PN/$PSN.xml</Profile_Rule>
  </flat-profile>
</device>
```

Device Profile Setup Flow

Account Setup
Use cisco.com credentials to login to CDA web portal (https://software.cisco.com/software/cda/home) and request “Distributed Customer” role
Create a profile

1. Login to https://software.cisco.com/software/cda/home using your Cisco account
2. Navigate to Profile Management and Add Profile

3. Select the appropriate PID

4. Select “Create a New Profile”, enter the profile name, upload the profile xml file and click on Add Mapping”
Associate a MAC Address to the Profile

1. Login to https://software.cisco.com/software/cda/home using your Cisco account
2. Navigate to MAC Address Management
3. Enter a MAC Address and click on Validate

4. When you click on Validate, a pop-up window will appear. Select the MAC Address and click on Proceed
5. Select the profile name and click on Submit

Phone Localisation
Daylight Savings Time Rule Configuration
Daylight savings configuration can be found under Voice → Regional → Time
Daylight Savings Time Rule Examples

The following example configures daylight savings time for the USA, starting at midnight on the first Sunday in April and ending at midnight on the last Sunday in October

- Start=4/1/7; end=10/1/7; save=1

The following example configures daylight savings time for New Zealand, starting at midnight on the first Sunday of October and ending at midnight on the third Sunday in March

- Start=10/1/7; end=3/22/7; save=1
  - 22 in the example above means after the 22nd of the month

The following example configures daylight savings time for the UK, starting at 01:00 on the last Sunday in March and ending at 02:00 on the last Sunday in October

- Start=3/-1/71; end=10/-1/72; save=1

Daylight Savings can also be configured using the below xml parameters:

```
<Set_Local_Date__mm_dd_yyyy__ ua="na"/>
<Set_Local_Time__HH_mm__ ua="na"/>
<Time_Zone ua="na">GMT</Time_Zone>
<Time_Offset__HH_mm__ ua="na"/>
<Ignore_DHCP_Time_Offset ua="na">Yes</Ignore_DHCP_Time_Offset>
<Daylight_Saving_Time_Rule ua="na">Start=4/1/7; end=10/-1/7; save=1</Daylight_Saving_Time_Rule>
<Daylight_Saving_Time_Enable ua="na">Yes</Daylight_Saving_Time_Enable>
```

Phone Display Language/Dictionary Server Script
You can change the phone display language by using the dictionary server script and language selection.

Configuration can be found under Voice → Regional → Language

To enable the options, set up a dictionary for each language that you want to include. To do this, specify a pair of the dn and xn parameters and values in the Dictionary Server Script field, for each language that you want to include.

Example for including French and German:
Based on the above Dictionary Server Script, in order to change the Phone Display Language to French, follow these steps:

1. Login to http://IP_ADDRESS_PHONE/admin/advanced
2. Navigate to Voice → Regional → Language
3. Change the values as per screenshot below

Please note that your Language Selection will have to match the descriptive name given on the Dictionary Server Script, in the case French.

How to configure Call Park?

Configure Call Park on Broadworks

1. Login to your Broadworks platform
2. Navigate to Resources → Assign Group Services

3. Add “Call Park” to Assigned Services
Configure Call Park on MPP

1. Login to http://IP_ADDRESS_PHONE/admin/advanced
2. Navigate to **Voice** → **Phone** → **Supplementary Services**
3. Enable Call Park Service (the default value is “Yes”)

4. Configure Call Park feature access code
   a. Navigate to **Voice** → **Regional** → **Vertical Service Activation Codes**
   b. Input the Activation Codes for Call Park and Call Unpark

When configuring call park, the Call Park Code and the Call Unpark Code must match the Feature Access Code configured on the server.

You can also configure the above setting using the below xml parameters:

```
<Call_Park_Code ua="rw">*68</Call_Park_Code>
<Call_Unpark_Code ua="rw">*88</Call_Unpark_Code>
```
Add Call Park to a Programmable Line Key and Key Expansion Module Line Key
In addition to using the service activation codes and softkey, you can also add a Call Park to a Programmable Line Key or Expansion Module Line Key.

Programmable Line Key
1. Login to http://IP_ADDRESS_PHONE/admin/advanced
2. Navigate to Voice → Phone
3. Chose which Line Key you would like to use (Line Key 2,3,4 etc.. )
4. Under Extension, set it to “Disabled”
5. Specify the Extended Function using the following format:
   a. `fnc=prk;sub=$USER@$PROXY;nme=CallPark-Slot1`
   i. ie: `fnc=prk;sub=1002010@sipurash22.com;nme=CallPark-Slot1`

Key Expansion Module Line Key
1. Login to http://IP_ADDRESS_PHONE/admin/advanced
2. Navigate to Voice → Att Console → Unit 1
3. Chose which Unit 1 key you would like to use
4. Enter the function string using the following format:
   a. `fnc=prk;sub=$USER@$PROXY;nme=CallPark-Slot1`
   i. ie: `fnc=prk;sub=1002010@sipurash22.com;nme=CallPark-Slot1`
How to - Configure BLFs with Speed Dials and Call Pickup?

**Configure Broadworks Server**
1. Login to your Broadworks Server
2. Navigate to **Group → Users** and select the user who will be monitoring using BLF
3. Navigate to **Client Applications → Busy Lamp Field**
4. Specify the List URI
5. Select Users which you would like to monitor

**Configure the MPP Phone**
1. Login to [http://IP_ADDRESS_PHONE/admin/advanced](http://IP_ADDRESS_PHONE/admin/advanced)
2. Navigate to **Voice → Att Console**
3. Configure the BLF List URI (previously created on the server)
4. Set “BLF List Feature Options” to “blf+sd+cp” (this is the default)
5. Configure a Line Key to Monitor a Single User’s Line
   a. Navigate to **Voice → Phone**
   b. Select a line key on which to configure a busy lamp field
   c. Select Disabled to disable the extension
   d. In the Extended Function field, enter a string in this format:
      i. `fnc=blf;sub=xxxx@$PROXY;usr=yyyy@$PROXY`
      ii. `fnc=blf;sub=xxxx@$PROXY;ext=yyyy@$PROXY`
   1. Where:
      a. `fnc=blf` means function=busy lamp field
      b. `sub=the URI to which the SUBSCRIBE message should be sent. For a BroadSoft server, this name must be identical to the name defined in the List URI: sip: parameter. xxxx is the name that is`
defined in List URI:sip: parameter. Replace xxxx with the exact defined name. $PROXY is the server. Replace $PROXY with the server address or name

c.  usr/ext=the user that the busy lamp field monitors. yyyy is user id of the phone that the busy lamp field monitors. Replace yyyy with the exact user id of the monitored phone. $PROXY is the server. Replace $PROXY with the server address or name

6. (Optional) You can configure the busy lamp field to work with any combination of speed dial or call pickup. To enable the busy lamp field to work with speed dial or call pickup, enter a string in the following format in the Extended Function field:

a.  fnc=blf+sd+cp;sub=xxxx@$PROXY;usr=yyyy@$PROXY
    i.  Where:
        1.  sd= speed dial
        2.  cp= call pickup

7. You can also configure the Key Expansion Module line keys as BLF+SD+CP

   a. Navigate to Voice → Att Console
   b. Select a key expansion module line key
   c. Enter a string in the appropriate format
      i.  fnc=blf+sd;sub=xxx@proxy;ext=monitored userID@proxy
      ii. fnc=blf+sd+cp;sub=xxx@proxy;ext=monitored userID@proxy
      iii. fnc=blf+sd;sub=xxx@proxy;ext=monitored userID@proxy
Why Cisco phones do not trust our DMS security certificate?

In some cases, the provisioning server might have a security certificate signed by a trusted CA, but the server does not have the intermediate certificate installed. Please check that you have the full chain of trust installed on your server.

You can obtain a copy of your intermediate certificate from your CA and install it directly on the phone, as a test (using the custom CA parameter), before uploading it to your server.

How to – Install a custom security certificate to the phone?

1. Login to [http://IP_ADDRESS_PHONE/admin/advanced](http://IP_ADDRESS_PHONE/admin/advanced)
2. Navigate to Voice → Provisioning → CA Settings
3. Input the Custom CA Rule, pointing to the certificate (in the example below, we are pointing to EDOS

You can also configure a Custom CA Rule via the xml file by using the below parameter:

```xml
<Custom_CA_Rule ua="na">https://webapps.cisco.com/software/edos/callhome/rootca?id=xxx</Custom_CA_Rule>
```

Where can I find the client root and subordinate certificates that the phones use for SSL/TLS?

Introduction

All MPP phones have a Cisco signed client certificate, but they might vary depending on firmware and/or hardware version. The quickest way of establishing which client certificate the phone is using, is to enable HTTPS and check what SSL certificate the phone is presenting.

Enable HTTPS

1. Login to [http://IP_ADDRESS_PHONE/admin/advanced](http://IP_ADDRESS_PHONE/admin/advanced)
2. Navigate to Voice → System
3. Set “Enable Protocol” to “HTTPS
4. Change the Web Server Port number (on this case we are using the default HTTPS 443 port) – Note: by changing the protocol to HTTPS, the phone will not change to port 443 automatically, you can to change it manually
5. Click on Submit All Changes
Check Client Certificate in Firefox

1. Login to https://IP_ADDRESS_PHONE/admin/advanced
2. Firefox will give you a security warning.
   a. Click on “Advanced” and “Accept the Risk and Continue”
3. Click on “Show Site Information”
4. Click on “Show Connection Details”

5. Click on “More Information”

6. Click on “View Certificate”
Check Client Certificate in Chrome

1. Login to https://IP_ADDRESS_PHONE/admin/advanced

2. Chrome will give you a security warning
   a. Click on “Advanced” and “Proceed”

3. Click on “Not secure” followed by “Certificate”
All Cisco root and subordinate certificates can be found at the following URL:

https://www.cisco.com/security/pki/

If web access is not available for any reason, use `openssl (s_client -connect)` to connect to the phone in order to check the issuer of the phone certificate which will be a subordinate certificate which will correspond to an entry on the PKI site, and to also check the issuer of the subordinate certificate, which will again be another Cisco certificate on the PKI site.

If the issuer of the subordinate certificate does not appear using the `s_client` command, then again use `openssl (x509 -in [cert_name] -text -noout)` to analyse the downloaded subordinate certificate in order to find out which root certificate issued the subordinate certificate. Again, the root certificate will correspond to an entry on the PKI site.