Accessing and Managing Utility Server

Release 6.0
03-603628
Issue 1.0
June 2010

© 2010 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

- Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.
- Named User License (NU). End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the

Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://www.avaya.com/support/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya® and Avaya Aura™ are trademarks of Avaya Inc.

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

All non-Avaya trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: Utility Server overview....7

Accessing Utility Server applications....8

Chapter 2: Utility Admin....9

Common....9

Viewing legal notice....9

Miscellaneous....9

Ping host....9

IPv6 Ping Host....10

Upload files....10

IP Phone Tools....10

IP Phone Settings Editor....10

IP phone backup and restore....14

IP phone firmware manager....15

Display stations....16

Display server firmware....16

Upload phone firmware....17

CM Login....17

Schedule control....17

DHCP Manager....19

DHCP....19

DHCP server status....19

Activate or deactivate DHCP....19

DHCP IP address pools....20

Show DHCP leases....22

DHCP server log....22

IPv6 DHCP Manager....23

IPv6 DHCP Server status....23

Activate/Deactivate IPv6 DHCP....23

IPv6 DHCP IP Address Pools....24

Show IPv6 DHCP Leases....25

IPv6 DHCP Sever Log....26

Gateway Firmware....26

Upload Gateway Firmware....26

Application Log View....27

TFTP server....27

Application Control....28

TFTP server....28

Application Log View....29

File server....29

Call detail recording....29

System database....30

MyPhone....30

Application Control....31

File server....31

Call detail recording....32

System database....33

MyPhone....34

Call Detail Record Tools....35
CDR database external access....35
CDR reports....37
CDR archive....37
CDR backups....38
CDR e-mails....38

Chapter 3: Directory Service Application....41
Configuring the Directory Service....41
Configuring the phones....41
General Settings....42
General Administration....42
LDAP Administration....43
Search Screen Settings....44
Detail Screen Settings....44
LDAP Filter Settings....45
Translation Language....45
External Numbers....46
Adding a new external number in the LDAP database....46
Editing an external number in the LDAP database....47
Deleting an external number from LDAP database....47

Index....49

Chapter 1: Utility Server overview

The Utility Server runs a number of utility applications that support or enhance the component applications facilitating a complete single box solution.

These Utility Server applications are briefly discussed in the following sections.

Utility Admin

Utility Admin enables you to configure and access various Utility Server applications, as follows:

- IP Phone file server: Supports the download of IP phone firmware and settings files. It also supports the back up and restore of IP Phone user configuration (for example, speed dial configurations.)
- IP Phone Settings Editor: Provides a web based tool for configuring the IP phone settings file. This significantly simplifies the process of making changes to the IP phone settings file and provides enhanced validation to help avoid mis-configurations.
- IP Phone firmware management: Enables you to upload new phone firmware to the file server.
- DHCP server: Provides basic DHCP server capabilities for supporting IP phones.
- Log viewer: Enables you to access the log files for all of the utility server applications.
- CDR Tools: Provides a CDR (Call Detail Records) collection capability that collects CDR records from Communication Manager and imports them into the Utility Server's database. It also provides some simple example reports to demonstrate how the CDR data in the database could be used by a system administrator.

MyPhone Admin

MyPhone Admin enables you to access some configuration elements of MyPhone and IP Phone operations, as follows:

- MyPhone Feature Buttons: Allows you to enable and disable the features available to the users of MyPhone.
- WML Links: The IP Phones have an ability to display a default WML page. This option enables you to configure the default WML page. On a general installation, the default page provides links to the Avaya Thin-Client LDAP Directory without a web address entry, and a System Message page.
- System Message: Enables you to configure the WML page. This typically contains a block of text which is relevant to every IP Phone user.
- Configure Directory Application: Enables you to configure the Avaya Thin-Client LDAP Directory through four options, namely General Administration, Search Administration, Details Administration, and Softkey Administration.

MyPhone

MyPhone enables you to configure the IP phones through a web interface. You can configure buttons, language settings, EC500, Enhanced Call forwarding and so on. It also enables you to change their station security codes and other parameters through the web interface.

MyPhone User Guide

MyPhone User Guide enables you to access the MyPhone documentation (a PDF file) without accessing the MyPhone application first.

Accessing Utility Server applications

The Utility Server administration web pages enable you to access various Utility Server applications and administer user settings and perform other administrative activities.

1. Enter the Utility Server URL on your web browser.
2. Click **Utilities** > **Utility Admin**.
3. Enter the user name.
4. Click **Logon**.
5. Enter the password.
6. Click **Logon**.
   The system displays the Utility Server menu.

Chapter 2: Utility Admin

Common

Viewing legal notice

Click **Common** > **Legal Notice**.

The Legal Notice page displays copyright and trademarks information.

The system always displays this page after you successfully log on to the Utility Server.

Miscellaneous

Ping host

You can confirm network connectivity between the Utility Server and other IP hosts.

Pinging a host

1. Click **Miscellaneous** > **Ping Host**.
2. On the Ping page, enter the Host Name or IP Address for the endpoint to ping.
3. Do one of the following:
    - Select the respective check box if you do not want the system to look up symbolic names for host addresses while pinging.

- Select the respective check box if you want the system to bypass normal routing tables and send directly to a host while pinging.

4. Click **Execute Ping** to ping the required endpoint and check the connectivity.

IPv6 Ping Host

You can confirm network connectivity between the Utility Server and other IPv6 hosts.

Pinging an IPv6 Host

1. Click **Miscellaneuos** > **IPv6 Ping Host**.
2. On the IPv6 page, enter the Host Name or IPv6 IP Address for the endpoint to ping.
3. Do one of the following:
   - Select the respective check box if you do not want the system to look up symbolic names for host addresses while pinging.
   - Select the respective check box if you want the system to bypass normal routing tables and send directly to a host while pinging.
4. Click **Execute Ping6** to ping the required endpoint and check the connectivity.

Upload files

You can run a web browser to upload a file to the Utility Server. You can upload either single file or a zipped file. In both cases, the file is transferred from the web browser session to the `/tmp` directory on Utility Server. Other applications can use this directory as a temporary store for files.

IP Phone Tools

IP Phone Settings Editor

You can configure settings for an IP phone using the IP Phone Settings Editor. Most Avaya IP phones use the 46xxsettings.txt file to configure phone related settings such as default WML

page and what options users can access from the handset. The IP phone settings editor allows easy editing of this file together with entry checking and help files.

Configuring view of IP Phone settings file

1. Select **IP Phone Settings Editor** from the left navigation menu.
   The system displays the IP Phone Settings Editor page.
2. Select the **Display file comments** check box to display the comments located in the 46xxsettings file. If this check box is cleared, the comments remain in the 46xxsettings file, but the system does not display them.
3. Select the **Display only active options** check box to display only the active settings on the IP phones. Other values remain in the 46xxsettings file as is, but the system does not display them.

Note:
Comment lines start with ##. Active lines start with SET command and contain options that are read by the IP phones. Lines within the file that start with ## SET are inactive. Currently the settings editor works only with values in uppercase. So, you must use uppercase for SET and parameter names in the file.

Editing IP Phone settings file

1. Do one of the following steps to select a settings file to edit:
   - Download the 46xxsettings.txt file from the Utility Server through http. This is the default method and lets you edit the 46xxsettings file that resides in the Utility Server. SIP and H.323 IP phones use the same 46xxsettings.txt file.

     Note:
     You can edit the URL address in the text box to download the file from a different http source. If you have a different file server in the network, then enter the URL for 46xxsettings.txt on that server. The application downloads the 46xxsettings.txt file for editing.

     The application cannot save back to the remote server. You must download the edited 46xxsettings.txt from the server on the save page and then upload it back to the original server.
   - Select **Upload IP phone settings or xml file** and then click **Browse** to upload a 46xxsettings.txt file or IpPhoneParameterDefinitions.xml file from a computer to the server.

The IpPhoneParameterDefinitions.xml contains help and entry information for the editor. At present, the latest version of IpPhoneParameterDefinitions.xml file is included in the Utility Server, and will be available on the Avaya support site for the later releases. The latest version of the 46xxsettings.txt file is available on the Avaya support site.

Note:

If the 46xxsettings file size is very large, the system takes approximately 5–10 seconds to load the file.

2. Click **Proceed with selected values** to edit the selected file.
   The system displays the 46xxsettings.txt page with four colums, namely **Activate**, **Parameter**, **Value**, and **Add Edit Delete**. See IP Phone Setting Editor field descriptions on page 14.
3. Do one of the following steps, as required:
   - Performing basic IP Phone settings editing on page 12
   - Checking IP Phone settings syntax on page 12
   - Performing advanced IP Phone settings editing on page 13

Performing basic IP Phone settings editing

Do one of the following steps:

- To activate a setting or deactivate a setting in the file, click the check box in the **Activate** column. If the check box is checked, the value is exposed within the file and the IP phones will use that value.
- To change a value of a setting, change the value in the text box.

Note:

You must save the changes every time by using the **Commit** button at the bottom of the page.

Checking IP Phone settings syntax

Do one or more of the following steps as required:

- If the system displays a setting with orange border, it indicates that the setting is not found in the xml file in the system and can be invalid. Correctly specify such settings.
- If the system displays any values with red border, it indicates that the values are incorrect and the IP phones cannot understand them. Click on a settings value to see the detailed information on the problem and correct the value.

Performing advanced IP Phone settings editing

Do one or more of the following steps:

- To reload the settings and return to the current line, click **R**. This is useful if you have changed a setting and want to verify if it is correct
- To add a line, click **+**. The page reloads and the system displays a drop down menu with all the available IP phone options in alphabetical order. The real lines in the file are displayed above and below the add line. Select the required option and enter the required value in the text box. Click **Add Line**. The line will be added below the current line.
- To add a comment, go to statement or raw text and click **+**. Select the **Comment** option from the bottom of the drop down menu, and click **Add Line**.
- To edit an entire line, click **<**. The page reloads and the line is displayed exactly as it appears in the file. Edit the text as required, and click **Save Line**. You can also edit the comment lines using the same procedure.
- To delete a line, select the line and click **-**. If you accidentally delete a line, you can reload the original settings file by clicking **IP Phone Settings Editor** from the left navigation menu. Any changes are not saved to the file until the final page is displayed and a save option is selected.

Saving IP Phone settings

1. After you are done with all the changes, click **Save New Settings File**.
2. On the Output Screen page, do one of the following steps:
   - Click **Save 46xxsettings.txt file to this server** to save the file in the Utility Server.

- Click either the **46xxsettings.txt(comments included in file)** link or the **46xxsettings.txt(no comments)** link to download the file to your computer.

IP Phone Setting Editor field descriptions

Name	Description
Activate	This column contains a checkbox. If this checkbox is selected, it signifies that the setting is active and ready to be read by the IP Phones. If the checkbox is cleared, the setting is inactive and appears commented out in the settings file and the IP phones do not read the settings.
Parameter	Displays comments and settings values. Comments span through both the columns and you can edit them using the edit line button in the next column. The system displays the IP phone settings name in the parameter column and their current value are displayed in the **Value** column.
Value	Displays comments and settings values. Comments span through both the columns and you can edit them using the edit line button in the next column. The system displays the IP phone settings name in the parameter column and their current value are displayed in the **Value** column.
Add Edit Delete Reload	Contains buttons to add a new line, to edit the entire line, to delete a line, or reload the page. **Add**: Adds a line or a comment. **Edit**: Edits an entire line or the comment lines. **Delete**: Deletes a line. **Reload**: Reloads the page validating any changes.

IP phone backup and restore

You can use the IP Phone Backup and Restore option to back up and restore individual IP phone settings. The IP Phone Backup and Restore option enables you to compress the backup files into a ZIP file and store it locally, and then restore an existing backup file to the Utility Server's repository of IP phone backup files.

Backing up an IP Phone settings file

1. Click **Configuration Tools** > **IP Phone Backup and Restore** .
2. Click **Create Backup** to create a new ZIP file of the IP Phone backup files. After creating the backup file, the system provides you a link to download the newly created ZIP file.

Restoring an IP Phone settings file

1. Click **Configuration Tools** > **IP Phone Backup and Restore** .
2. Click **Browse** to locate an existing ZIP file of the IP Phone backup files.
3. Click **Upload Backup** to upload the backup files to restore later.

IP Phone Backup and Restore button descriptions

Name	Description
Create Backup	Creates a new ZIP file of the IP Phone backup files. After creating the backup file, the system provides you a link to download the newly created ZIP file.
Upload Backup	Uploads a backup ZIP file to the Utility Server's repository of IP Phone backup files.

IP phone firmware manager

This application enables you to perform controlled resetting of H.323 IP stations registered on Communication Manager to load new settings or upgrade firmware on IP phones.

Note:
You cannot reset IP stations that are not logged in or are logged in with unnamed registrations using this application.

Display stations

This page displays the IP stations registered with Communication Manager configured using Communication Manager login.

Display Stations field descriptions

Name	Description
Extension	Extension number on Communication Manager.
Type	The station type as set on the station form.
Connected Type	The actual type of station that is connected.
Model	The type of IP phone that is connected.
Network Region	The IP network region the phone is in.
IP address	The IP address as seen on Communication Manager of the IP endpoint.
Firmware Version	The current version of firmware on the IP endpoint.
Firmware on the Utility Server	The firmware version stored locally on the Utility Server.

Display Stations button descriptions

Name	Description
Update Table	This button forces the IP Phone Firmware Manager application to log into Communication Manager and update the Phone Firmware Manager database with the station information.
Refresh Page	This button refreshes the current web page with the current information in the Phone Firmware Manager database.

Display server firmware

This page displays the firmware stored locally on Utility Server. If you set an IP phone to use Utility Server, the system upgrades the IP phone to the release listed in this page after a reset.

Upload phone firmware

This feature provides a centralized deployment feature for IP Phone Firmware.

Manage Firmware button descriptions

Name	Description
View	Displays the information of the selected firmware package.
Unpack	Unpacks each package of phone firmware separately (extract files from the ZIP archive).
Activate	Activates the selected firmware package and makes it available to the Utility Server.
Deactivate	Deactivates the selected firmware package and remove it from the web server.
Remove	Deletes the extracted files as well as the ZIP archive.

CM Login

This page contains the login for Communication Manager.

CM Login button descriptions

Name	Description
Change Callserver	Saves any changes made to the settings on the CM Login page.
Test Connection	Checks the connections and logins.

Schedule control

This page enables you to select the IP phones to reset and specify the period for reset. You can also configure the system to reset an IP phone if the IP phone fails to upgrade, or if you do not want to reset a station that is currently active on a call.

You can reset the IP phones based on network-region, IP phone type, certain firmware loads, extension, or extension ranges. You can also speciy the date and time to reset the IP phones.

Schedule Control field descriptions

Name	Description
Select Phones	Lets you select an IP phone or all the IP phones to reset based on the phone type and firmware.
Select Start Time	Time at when the reset operation starts. You can either choose to reset a phone immediately or set a date and time for the reset operation at a later time.
Select Stop Time	Time at when the system stops the reset or reboot operation. You can specify the date and the time for the reset operation.
Select whether a phone may be updated while being active	If this option is set to no, the system does not reset the phones that are currently active on a call.
Select whether a phone running the latest firmware should be reset	If this is set the system resets only those phones that are not running the same version of the firmware on the Utility Server. You must set this option to yes if you have made any changes to the 46xxsettings.txt file that the phones use.
Enter the minimum delay between handling of phones	The number of seconds the system waits between resetting of phones to prevent the file server being overloaded.
Enter the maximum number of error retries per phone	The number of times the system retries to reset a phone in the event it fails to upgrade the phone to the firmware on Utility Server. The number of retries is limited by the stop time specified by the **Select Stop Time** field.
Enter the minimum delay between error retries	The number of seconds the system waits before trying to reset the same phone again.
Select when error retries are re-scheduled	Schedules the number of attempts for resetting a phone when there is an error in resetting at the end of the scheduled period or during the scheduled period.

Schedule Control button descriptions

Name	Description
Schedule Phone Firmware Update	Schedules the IP Phone Firmware update according to the settings in the Schedule Control page.

DHCP Manager

DHCP

DHCP (Dynamic Host Configuration Protocol) is a method for endpoints to automatically obtain IP addresses. Any client configured to use DHCP can obtain an IP address from the server automatically allowing easier management of IP endpoints and efficient use of IP addresses.

The Utility Server DHCP uses the Linux DHCPD. Advanced users familiar with Linux DHCPD can edit the dhcpd.conf directly and the application supports this. Any entry that is not displayed on the Web-based DHCP editor is stored in the file.

DHCP server status

You can use the **DHCP Server Status** option to check whether the DHCP server is running or not.

Viewing DHCP server status

Click **DHCP Manager** > **DHCP Server Status**.
The system displays whether the DHCP service is running or not.

Activate or deactivate DHCP

Activate/Deactivate DHCP enables you to activate or deactivate the DHCP server. When you activate the server, a status message from the service is displayed. If the DHCP server moves to a running state, it means that the dhcpd.conf file is correctly created and the DHCP server has started. If there is a problem in the dhcpd.conf file, the DHCP server will not start and an error message will be displayed indicating the likely cause of the problem.

Activating and deactivating DHCP server

1. Click **DHCP Manager** > **Activate/Deactivate DHCP**.
   The DHCP Service Control page displays the status of the DHCP server.
2. Click **Activate DHCP Server** or **Deactivate DHCP Sever** to activate or deactivate the DHCP server based on the current status of the DHCP server.

DHCP Service Control button descriptions

Name	Description
Activate DHCP Server	Activates the DHCP server. If the DHCP Service Control page displays the status of DHCP service as **RUNNING**, then you do not need to activate the DHCP server again.
Deactivate DHCP Server	Deactivates DHCP server.
Load last working DHCPD conf file	Loads the DHCPD file containing your settings that you used to run the DHCP Server last time.

DHCP IP address pools

You can use the DHCP IP Address Pools option to configure DHCP IP addresses. You can add subnets to existing networks, view the subnet details for existing networks, edit subnet details or remove the subnets for a network range.

Viewing DHCP subnets

1. Click **DHCP Manager** > **DHCP IP Address Pools**.
2. Select a network from the list for which you want to view the subnet details.
3. Click **View Subnet**. The raw details of the file are displayed showing all values in the range.

Adding a DHCP subnet

1. Click **DHCP Manager** > **DHCP IP Address Pools**.
2. Click **Add Subnet**.
3. Enter a network and netmask for the new subnet.
4. Click **Add Subnet**.

Editing DHCP subnets

1. Click **DHCP Manager** > **DHCP IP Address Pools**.
2. Select the network for which you want to edit the subnet details.
3. Click **Edit Subnet** to edit a subnet.
4. On the DHCP Server IP Address Pools page, edit the details as required.

   Note:

   In case you are unsure of a value to enter, click the blue question mark to see a description of what should be entered in the field
5. Click **Commit Changes and restart DHCPD**.

Removing DHCP subnets

1. Click **DHCP Manager** > **DHCP IP Address Pools**.
2. Select a network from the list if you want to remove the subnets for the particular network range.
3. Click **Remove Subnet** to remove all the subnet in the DHCP network.
4. Click **OK** in the confirm message window to confirm the remove operation.

Show DHCP leases

You can view the DHCP lease information. This page shows the percentage of IP addresses in use and what endpoints currently have which addresses. This is useful for knowing when pools are nearly all used.

Viewing DHCP lease information

Click **DHCP Manager** > **Show DHCP Lease**.
The DHCP Leases Display page shows two pieces of information:

a. Range of IP ports available, number of IP ports in use, and percentage of IP ports in use.

b. IP ports, their last usage duration, and their binding states.

DHCP Leases Display field descriptions

Name	Description
Range Start	Start of the range of IP addresses that can be used in DHCP.
Range End	End of the range of IP addresses that can be used in DHCP.
Range Size	Total number of IP addresses available in the range for DHCP.
IP addresses in use	Total number of IP addresses that are currently in use within the range of IP addresses.
Percentage in use	Percentage for the number of IP addresses in use within the range of IP addresses.
Binding State	The current status for an IP address. The available options are Active and Free. Active: An endpoint is currently using the IP address. Free: An endpoint has returned the IP address to the pool.
MAC Address	IP addresses for a particular computer or laptop. This address is used for physical identification of a particular Ethernet code.

DHCP server log

You can view the server logs. This may be helpful in troubleshooting DHCP related problems.

Viewing DHCP log files

1. Click **DHCP Manager** > **DHCP ServerLog**.
2. On the View DHCP Log Files page, click **View Log** to see the DHCP log files and lease files.

IPv6 DHCP Manager

IPv6 DHCP Server status

You can use the IPv6 DHCP Server Status option to check whether the IPv6 DHCP server is running or not.

Viewing IPv6 DHCP Server status

Click **IPv6 DHCP Manager** > **IPv6 DHCP Server Status**.

The system displays whether the IPv6 DHCP service is running or not.

Activate/Deactivate IPv6 DHCP

Activate/Deactivate IPv6 DHCP enables you to activate or deactivate the IPv6 DHCP server using this server. When you activate the server, a status message from the service displays. If the IPv6 DHCP server moves to a running state, it means that the `dhcpd.conf` file is correctly created and the IPv6 DHCP server has started. If there is a problem in the `dhcpd.conf` file, the IPv6 DHCP server will not start and an error message will be displayed indicating the likely cause of the problem.

DHCP Service Control button descriptions

Name	Description
Activate DHCP Server	Activates the DHCP server. If the IPv6 DHCP Service Control page displays the status of DHCP service as RUNNING, then you do not need to activate the DHCP server again.
Deactivate DHCP Server	Deactivates IPv6 DHCP server.
Load last working DHCPD conf file	Loads the DHCPD file containing your settings that you used to run the DHCP Server last time.

Activating and deactivating IPv6 DHCP server

1. Click **IPv6 DHCP Manager** > **Activate/Deactivate IPv6 DHCP**. The IPv6 DHCP Service Control page displays the status of the IPv6 DHCP server.
2. Click **Activate DHCP Server** or **Deactivate DHCP Sever** to activate or deactivate the DHCP server based on the current status of the DHCP server.
3.

IPv6 DHCP IP Address Pools

You can use the IPv6 DHCP IP Address Pools option to configure IPv6 DHCP IP addresses. You can update DHCP address to existing networks for a network range.

IPv6 DHCP Server IP Address Pools field descriptions

Name	Description
DHCP v6 Start Address	Enter the valid IPv6 address without prefix.
DHCP v6 Stop Address	Enter the valid IPv6 address without prefix.
DHCP v6 Prefix Address	Enter the prefix address. It is identical to the start and stop addresses.

Updating DHCP IPv6 values

1. Click **IPv6 DHCP Manager** > **IPv6 DHCP IP Address Pools**.
2. On the IPv6 DHCP Server IP Address Pools page, click **Update DHCP v6 Values** to update the DHCP Server IPv6 address.

Show IPv6 DHCP Leases

You can view the IPv6 DHCP lease information. This page shows the percentage of IP addresses in use and what endpoints currently have which addresses. This is useful for knowing when pools are nearly all used.

IPv6 DHCP Leases Display field descriptions

Name	Description
Range Start	Start of the range of IPv6 addresses that can be used in DHCP.
Range End	End of the range of IPv6 addresses that can be used in DHCP
Range Size	Total number of IPv6 addresses available in the range for DHCP.
IP addresses in use	Total number of IPv6 addresses that are currently in use within the range of IP addresses.
Percentage in use	Percentage for the number of IPv6 addresses in use within the range of IP addresses.
Binding State	The current status for an IPv6 address. The available options are Active and Free. Active: An endpoint is currently using the IPv6 address. Free: An endpoint has returned the IPv6 address to the pool
MAC Address	IPv6 addresses for a particular computer or laptop. This address is used for physical identification of a particular Ethernet code.

Viewing DHCP lease information

Click **IPv6 DHCP Manager** > **Show IPv6 DHCP Lease**.

The IPv6 DHCP Leases Display page shows the following information:

- Range of IP ports available, number of IP ports in use, and percentage of IP ports in use.
- IP ports, their last usage duration, and their binding states.

IPv6 DHCP Sever Log

You can view the server logs. This may be helpful in troubleshooting IPv6 DHCP related problems.

Viewing IPv6 DHCP log files

1. Click **IPv6 DHCP Manager** > **IPv6 DHCP Server Log**.
2. On the View IPv6 DHCP Log Files page, click **View Log** to see the DHCP log files and lease files.
3.

Gateway Firmware

Upload Gateway Firmware

This feature enables Utility Server to support TFTP access for Media Module and Media Gateway Firmware. The Upload Gateway Firmware enables you to view the firmware. You can also upload a new file of firmware to be uploaded on the Utility Server.

Viewing Gateway firmware

1. Click **Gateway Firmware** > **Upload Gateway Firmware**.
2. On the Upload Gateway Firmware page, click **Display Firmware Directory** to see the Gateway Firmware.

Uploading Gateway Firmware

1. Click **Gateway Firmware** > **Upload Gateway Firmware**.
2. On the Upload Gateway Firmware page, click **Browse** to navigate to the file you need to upload.
3. Click **Upload Gateway Firmware and Activate** to upload Gateway firmware.

Application Log View

TFTP server

You can view and download the TFTP server access log files. You can also view the archive log files.

Viewing TFTP Server Access Log

1. Click **Application Log View** > **TFTP Server**.
2. Click **View Log** which appears in front of TFTP Server Access Log to view the TFTP sever access log.

Viewing archive log files

1. Click **Application Log View** > **TFTP Server**.
2. Click **View Log** which appears in front of View Archive Log Files to view the archive log files.

Application Control

TFTP server

You can view the current status of the TFTP server, also, whether the server will automatically restart or reboot. You can start or stop the server to configure its operation after a reboot.

Control TFTP Server buttons descriptions

Name	Description
Start the TFTP server	Starts the TFTP server.
Stop the TFTP server	Ends the TFTP server.
Enable Autostart of the TFTP server	Enables autostart of the TFTP server.
Disable Autostart of the TFTP server	Disables the autostart of the TFTP server.

Application Log View

File server

You can view and download the file server log files, that is, the access and error log files for HTTP, HTTPS and Watchdog file, and also download the history log files. The system maintains the secure and non-secure access logs separately and also provides separate log files for access monitoring and recording of errors. You can filter the File Server logs to only display access entries made by Avaya IP Phones. The Watchdog file is unique to the Utility Server. The Watchdog tests the file server on a regular basis and restarts the server if it detects any problem.

You can use the File Server option to view the current status of the file server and check whether the server restarts automatically on a reboot. You can conduct a configuration file test and restart the file server. You can also change the level of logging for the file server independently for insecure (HTTP) and secure (HTTPS) access. You must restart the file server for making any changes to the log levels effective.

Note:
Error logs do not support filtering.

Viewing file server log files

1. Click **Application Log View** > **File Server**.
2. Click **View Log** to view a particular log file, for example, HTTP, HTTPS, and Watchdog.
3. Click **Download File Server Log** on the respective log file page to download the log file.

Call detail recording

The Call Detail Recording applications are responsible for handling the Call Detail Records (CDR) that are produced by Communication Manager. At present, there are five separate daemons to collect the data from Communication Manager, import the data to the Utility Server,

export history data, backup data, and generate automated e-mail reports. You can also download the history log files.

Viewing CDR log files

1. Click **Application Log View** > **Call Detail Recording**.
2. Click **View Log** to view a particular log file, for example, CDR Collector's Activity log and CDR Importer's Activity log.
3. Click **Download Log** on the respective log file page to download the log file.

System database

The Utility Server uses a local database to store and retrieve data for a variety of applications. These applications include the Call Detail Recording system, the MyPhone System Administrator, and other diagnostic tools. You can use the System Database option to view and download the log files for the system database.

Viewing system database log files

1. Click **Application Log View** > **System Database**.
2. Click **View Log** to view log file for a particular day of the week, for example, Monday and Tuesday.
3. Click **Download Log** on the respective log file page to download the log file.

MyPhone

The MyPhone application allows users to change their station security code and station buttons. There is also an administrator interface to control which buttons users can select, phone WML page, and LDAP directory control. You can use the MyPhone option to view and download all the log files relevant to the MyPhone Server. This includes the MyPhone, the MyPhone Administrator log files, and the raw output from Tomcat - catalina.out. You must use the catalina.out file only for diagnostic analysis, as this file contains entries which are unrelated to MyPhone application.

Note:
It is best practice to keep the MyPhone option turned off so that users do not have access to any settings on a phone and cannot modify the settings (for example, the security code) in the phone.

Viewing MyPhone server log files

1. Click **Application Log View** > **MyPhone**.
2. Click **View Log** to view a particular log file, for example, MyPhone server log file and MyPhoneAdmin error log file.
3. Click **Download Log** on the respective log file page to download the log file.

Application Control

File server

This page displays the current status of the File Server and also provides information on whether the server will automatically restart after a reboot. You can conduct a configuration file test and request a restart of the File Server. You can change the level of logging for the File Server independently for Insecure (HTTP) and Secure (HTTPS) access. You must restart the file server to make any changes to the log levels effective.

Note:
You cannot change the operation of the File Server on a server reboot or stop the File Server during reboot.

Viewing file server status

1. Click **Application Control** > **File Server**.
   The Control Web Server page displays the current status of the File Server.
2. Click **File Server Configuration Test** to start a configuration test for the File Server.
3. Click **Restart File Server** to restart the File Server.

Note:

The system can take up to five minutes to activate the request to restart the File Server.

4. Do one of the following steps:
   - Choose the required option from the drop-down menu, and click **Set Logging Level for Insecure Access (HTTP)**.
   - Choose the required option from the drop-down menu, and click **Set Logging Level for Secure Access (HTTPS)**.

Control Web Server button descriptions

Name	Description
FIle Server Configuration Test	Starts a configuration file test.
Restart File Server	Restarts the file server.
Set Logging Levels for Insecure Access (HTTP)	Sets logging level for the file server for HTTP, or changes the existing log level settings based on your selection.
Set Logging Levels for Secure Access (HTTPS)	Sets logging level for the file server for HTTPS, or changes the existing log level settings based on your selection.

Call detail recording

You can view the current status of the Call Detail Recording (CDR) Collector applications and also control these applications (for example, starting or stopping the CDR applications) and the SQL Import Servers using the Call Detail Recording option. The changes you make are effective immediately and the system preserves the settings when you restart the server.

Controlling CDR Servers

1. Click **Application Control** > **Call Detail Recording**.
2. Click **Enable the CDR Collector** or **Disable the CDR Collector** to enable or disable the CDR Collector application respectively.
3. Click **Enable the CDR Importerr** or **Disable the CDR Importer** to enable or disable the CDR Importer application respectively.

4. Click **Enable the CDR Exporter** or **Disable the CDR Exporter** to enable or disable the CDR Exporter application respectively.
5. Click **Enable the CDR Compressor** or **Disable the CDR Compressor** to enable or disable the CDR Compressor application respectively.

System database

You can use the System Database option to view the current status of the system database and check whether the server restarts automatically on a reboot. You can also start or stop the server immediately or configure its operation after a reboot.

Controlling system database

1. Click **Application Control** > **System Database**.
   The Control System Database page displays the current status of the system database.
2. Click **Start System Database** or **Stop System Database** to start or stop the system database respectively.
3. Click **Enable Autostart of System Database** or **Disable Autostart of System Database** to enable or disable autostart of the system database after a reboot.

Control System Database button descriptions

Name	Description
Start System Database	Starts the system database server.
Stop System Database	Stops the system database server.
Enable Autostart of System Database	Enables auto start of the system database server after a reboot.
Disable Autostart of System Database	Disables auto start of the system database server after a reboot.

MyPhone

You can use the MyPhone option to view the current status of the MyPhone Server and check whether the server restarts automatically on a reboot. You can also start or stop the server immediately or configure its operation after a reboot.

Controlling MyPhone server

1. Click **Application Control** > **MyPhone**.
   The Control MyPhone server page displays the current status of the MyPhone server and the status of the option to restart the server automatically after a reboot.
2. Click **Start the MyPhone Server** or **Stop the MyPhone Server** to start or stop the MyPhone server respectively.
3. Click **Enable Autostart of the MyPhone Server** or **Disable Autostart of the MyPhone Server** to enable or disable autostart of the MyPhone server after a reboot.

Control MyPhone Server button descriptions

Name	Description
Start MyPhone Server	Starts the MyPhone Server.
Stop MyPhone Server	Stops the MyPhone Server.
Enable Autostart of the MyPhone Server	Enables auto start of the MyPhone Server after a reboot.
Disable Autostart of the MyPhone Server	Disables auto start of the MyPhone Server after a reboot.

Call Detail Record Tools

CDR database external access

This feature allows almost any Postgres—compliant report writing tool to generate reports on the CDR data collected by Utility Server.

Note:

pgAdmin is one such Postgres—compliant tool and is freely available for a variety of platforms.

Access to the CDR database is provided on the standard port 5432 on the IP address of Utility Server. Use the `admin` user ID to open the connection.

Note:

The access to CDR data is read—only. That is, it is not possible to change or remove any data in the database.

Currently, the only table on Utility Server is called “raw” and is part of the CDR database. The table name may change in the future releases of Utility Server. The “raw” table is defined as follows:

```
CREATE TABLE raw

(

pbxid varchar(25) NOT NULL DEFAULT 'PBX'::bpchar,

cdrdate date NOT NULL DEFAULT '2005-01-01'::date,

cdrtime time NOT NULL DEFAULT '00:00:00'::time without time zone,

duration int4 NOT NULL,

acctcode varchar(15),

attdconsole varchar(4),

authcode varchar(13),

bandwidth varchar(2),

bcc char(1),

callingnum varchar(15) NOT NULL,

calltype char(1),

clgnum varchar(15),
```

```
clgpty varchar(2),
codedial varchar(4),
codeused varchar(4),
condcode char(1),
contacturi varchar(20),
countryfrom varchar(3),
countryto varchar(3),
dialednum varchar(23),
enddate date,
endtime time,
featflag char(1),
frl char(1),
fromuri varchar(20),
incrtid varchar(3),
intrkcode varchar(4),
ins varchar(5),
internalcodec varchar(2),
isdncc varchar(11),
isdnccppm varchar(11),
ixccode varchar(4),
locationfrom varchar(3),
locationto varchar(3),
mauui char(1),
nodenum char(2),
outcrtid char(3),
ppm varchar(5),
requesturi varchar(20),
resflag char(1),
secdur varchar(5),
seqnum varchar(10),
startdate date,
```

```
starttime time,
timezonefrom varchar(6),
timezoneto varchar(6),
touri varchar(20),
tscct varchar(4),
tscflag char(1),
trunkcode varchar(2),
ucid varchar(20),
vdn varchar(3),
CONSTRAINT raw_pk PRIMARY KEY (pbxid, cdrdate, cdrtime, duration,
callingnum)
)
WITHOUT OIDS;
```

CDR reports

You can use the CDR Reports option to view the Call Detail Record Reports currently available. The system collects the CDR records from Communication Manager and imports them into the Utility Server database.

Viewing CDR reports

1. Click **CDR Tools** > **CDR Reports**.
2. Click **View CDR Report** to view a CDR report from the available options, for example, the ten longest calls, the ten most active extensions, the ten most dialled numbers, and the raw CDR data.

   The system displays each report in both a numeric and graphical form.

CDR archive

The CDR Compress daemon compresses the raw CDR files collected from Communication Manager as ZIP files after they are successfully imported, and stores them in a directory for each month or year. You can use the CDR Archive option to download these compressed zip files.

Accessing the CDR archive

1. Click **CDR Tools** > **CDR Archive**.
   The system displays a list of ZIP files that you can download.
2. Click **Download** to download a particular archive file.

CDR backups

The CDR Export daemon ensures that the active CDR database contains only 12 months of data. Once per month, the system deletes any data that is older than 12 months. However, before deleting the data, the system stores the data in a CSV (Comma Separated Values) file. You can use the CDR Backups option to download the data and store it remotely or import the data to another database. To provide ease of import, the system stores database headings as the first line in the CSV file.

Note:
The system automatically deletes the files that are older than 12 months. This means that the Utility Server has a maximum of 12 months of on-line data and 12 months of previous off-line data at any time.

Accessing CDR backup files

1. Click **CDR Tools** > **CDR Backups**.
   The system displays a list of backup files that you can download.
2. Click **Download** to download a particular backup file.

CDR e-mails

You can configure and control the operation of each of the three regular e-mail daemons (daily, weekly and monthly) by using this page. You can enable or disable each daemon separately. You can configure each daemon to generate up to three separate reports and send them to a configurable list of recipients.

CDR E-Mails field descriptions

Name	Description
E-Mail Daemon	Lets you enable or disable e-mail daemon for each of the three regular daemons, that are, daily, weekly, and monthly.
Longest Calls	Lets you generate a report for the longest calls you have made over a period of time.
Most Active	Lets you generate a report for the most active extensions that you have called.
Most Dialled	Lets you generate a report of the most dialled numbers when you make calls.
Distribution List	Lets you send the reports to a list of recipients by e-mail. You can separate each e-mail address in the distribution list with a semi-colon.

CDR E-Mail button descriptions

Name	Description
Update CDR E-Mailer Configuration	Saves and updates the CDR E-mail settings based on the settings on the CDR E-Mail page.

Chapter 3: Directory Service Application

The Directory Service application enables you to search an LDAP database using browsers on your compatible 46xx and 96xx phones. You can use these web pages to configure the Directory Service application to connect to an LDAP database and to customize the user search experience. Directory Service application supports 250 instances of the Directory Service configuration and provides multi language for each of these instances. See the Directory Application Job Aid available at Avaya Support Site https://support.avaya.com for a more detailed description of this feature and required configuration.

Configuring the Directory Service

You must configure the Directory Service application correctly for the WML Browsers to perform search operations.

1. Specify the LDAP connection settings on the General Settings screen.
2. Click **Test Connection** to ensure that the Directory Service application is connecting to the LDAP database.
3. Enable the Directory Service application for HTTP or HTTPS traffic.
4. (Optional) Use the Search Screen Settings screen to customize the Search screen on the phone browser.
5. (Optional) Use the Details Screen Settings screen to customize the Details screen on the phone browser.
6. (Optional) Use the Ldap Filter Settings screen to customize the Ldap filter attributes while searching.

Configuring the phones

Set the HTTP (or HTTPS) to point to the Utility Server through DHCP or in the `46xxsettings.txt` file.

The Utility Server comes with a `46xxsettings.txt` file and the WMLHOME parameter is automatically set up to point to a landing page which includes three WML applications: Directory Application, User entered URL, and Message Application.

General Settings

Use this screen to administer general settings and LDAP connection settings for the Directory Service application.

General Administration

Directory Number

Select any number between one and 250 and the system configures Directory Service application for the particular directory number. The system configures and applies the particular directory number to the General Settings page, the Translation Language page, and the External Numbers page.

Application Title

Enter an application title that would be displayed on the search screen of the phone browsers.

HTTP

Select Enable to enable HTTP traffic. If you enable HTTP, the Directory Service application can accept traffic from WML Browsers using the HTTP protocol.

Warning:

Enabling the Directory Service application on the HTTP port (unsecured port 80) will allow any browser to access the Directory Service application without authentication or encryption mechanisms. This may allow unauthorized users to access directory information stored on your LDAP server using the Directory Service interface.

HTTPS

Select Enable to enable HTTPS traffic. If you enable HTTPS, the Directory Service application can accept traffic from WML Browsers using the HTTPS protocol.

Select a language file

Select a language file from the drop-down menu where you can write your translation.

Select language for your translation

Select a language for your translation from the drop-down menu to write to the language file you selected in the previous step.

LDAP Administration

Host Name

Enter the hostname or IP address of the LDAP server. The Directory Service application connects to this server for searching.

Port

Enter a port number. The default LDAP port is 389. If the LDAP server is using a different port, enter the port number.

Note:

Ensure that this port is enabled in the firewall. Avaya recommends that you open the port only for outbound traffic.

Base DN (Search Root)

Specify an LDAP distinguished name from where the Directory Search application can begin searching.

Base DN (External Search Root)

Specify an LDAP Base Distinguished Name where the external numbers are stored. The Manage External Numbers screen uses this root to list/add/delete entries in the external directory. This distinguished name must be under the Search Root specified above to enable the Directory Service application to include external names in its search. For example, if the Search Root is o=avaya.com, then the External Search Root can be ou=external numbers, o=avaya.com.

Max number of hits

Enter the maximum number of results that must be returned for a particular search. The default value is 96.

Note:

A higher number can degrade the system performance. The system stops the search operation when the search reaches the maximum number.

Search Time

Enter the maximum number of seconds the search can take before returning the results. The system stops the search operation when the search exceeds the time. The default value is 10 seconds.

User ID

Specify a User ID to connect to the LDAP server. If you do not provide any User Id, the Directory Service application uses anonymous LDAP connection. To ensure that you can modify the LDAP database using the Manage External Numbers screen, you must give write access to the specified user for the database.

Password

Specify a Password for the User ID you have specified for the LDAP server.

Secure Connection (TLS support)

Select On or Off. The Directory Service application can connect to an LDAP server on TCP or TLS. If you select TLS as the connection type, additional configuration is required. See the TLS Configuration topic for more details.

Test Connection

Click Test Connection to ensure that the Directory Service application can connect to the LDAP server using the connection parameters you have specified above.

Search Screen Settings

You can customize the search or home page of the Directory Service application to enable users to search against particular LDAP attributes. You can specify total six search attributes, out of which you can customize four. Each search attribute is displayed on a separate line on the phone. You can configure the settings for each line as follows:

Search Attribute

Select from the list of available LDAP attributes that can be searched, or choose others and enter the attribute name in the space provided. The LDAP attribute for Name can be either cn or cn;lang-en; and for the second attribute it can be a telephone number or any attribute which must be associated with the phone number.

Note:

A valid LDAP attribute name can be an alphabetic character, a number, and the symbols - and ;. But the attribute name must begin with an alphabetic character.

Associated Label

Enter the label for each search attribute that is activated. This label supports Unicode and is displayed on the phone search screen.

Minimum Search String

For Item #7 enter the minimum number of characters (value between one and nine) required for user entered Search strings. The directory application denies any search when the search string contains less than the minimum number of characters required.

Detail Screen Settings

You can customize the details screen of the Directory Service application to display attributes of a particular LDAP entry. A total of six attributes can be displayed on the phone browser. The first attribute must be a name and the second attribute must be a phone number. You can customize the other four attributes.

Detail Attribute

Select from the list of available LDAP attributes that can be displayed, or choose other and enter the attribute name in the space provided.

The LDAP attribute for Name can be cn, or cn;lang-en, or displayName and for the second attribute it can be a telephone number or any attribute which must be associated with a phone number.

Note:

A valid LDAP attribute name can be an alphabetic character, a number, and the symbols - and ;. But the attribute name must begin with an alphabetic character.

Detail Attribute Label

Enter the label which would be displayed before the actual value on the detail screen.

LDAP Filter Settings

You can customize the LDAP Filter settings of the Directory Service application to add filters to the LDAP search. The system sends the results if the filter text is part of a DN that matches the search string. You can configure a total of six attributes for the ldap search filter.

Filter Attribute

Select from the list of available LDAP attributes that can be used in search filter, or select the other option and enter the attribute name in the text box.

Note:

A valid LDAP attribute name can be an alphabetic character, a number, or the symbols - and ;. But the attribute name must begin with an alphabetic character.

Filter Text

Enter the label which would be used in the ldap search filter for the associated filter attribute.

Translation Language

Use the Translation Language screen for the translation language you selected in the General Administration screen for the selected Directory Number. There are eleven predefined translation languages. When you select a language, the system writes the language translation to the file and the system displays the details in the translation column. If you select a language other than the eleven pre-defined languages, the system displays English text mapping with English translations. In either of these scenarios, you can edit the English text in the translation mapping column.

The list of eleven predefined language translations are as follows:

- Brazilian-Portuguese
- English
- French

- German
- Italian
- Japanese
- Korean
- Lat-Spanish
- Russian
- Simplified Chinese
- Traditional Chinese

The translation language settings allows the user to edit the translation string on the right column for each English string.

External Numbers

You can use this screen to view entries under the External Number search root in the LDAP database based on your specification in the General Settings screen. You can also add new external numbers, and edit or delete existing external numbers using this screen.

Note:
To ensure that you can modify the LDAP database using the Manage External Numbers screen, you must give write access to the specified user for the database.

Adding a new external number in the LDAP database

1. Click **Add**.
2. In **Native Name** field, specify a Unicode name.
3. In the **Name** field, specify an ASCII name.
4. In the **Phone Number** field, enter a phone number.
5. In the **E-mail** field, specify an e-mail address.

Note:
The **Native Name** and **Phone Number** fields are mandatory.

6. Click **Save** to add the external number to the LDAP database and go back to the External Numbers screen.
7. Click **Refresh** to view your changes.

Editing an external number in the LDAP database

1. Select an entry in the List page.
2. Click **Edit**.
3. Edit the details of the selected entry as required.

   Note:
   You can edit only one entry at a time. You cannot modify the details in the **Native Name** field.
4. Click **Save** to save your changes to the LDAP database and go back to the External Numbers screen.
5. Click **Refresh** to view your changes.

Deleting an external number from LDAP database

1. Select an entry in the List page.
   You can select multiple entries at a time.
2. Click **Delete**.
3. Click **Delete** in the next screen to confirm your action and go back to the External Numbers screen.
4. Click **Refresh** to view your changes.

Index

Numerics

46xxsettings.txt 11

A

accessing CDR backup files 38
accessing utility server 8
accessing utility server applications 8
Activate/Deactivate IPv6 DHCP
    activating and deactivating IPv6 DHCP server 24
activating and deactivating DHCP server 20
add a subnet 21
adding a new external number 46

B

back up and restore 15

C

Call Detail Record 30
call detail recording 29, 32
Call Detail Recording 32
Call Detail Records Collector 30
catalina.out 31
CDR 29, 32
CDR archive 37
CDR backup 38
CDR backup files 38
CDR database external access 35
CDR e-mail 38
CDR email button descriptions 39
CDR email field descriptions 39
CDR export daemon 38
CDR log files 30
CDR report 37
CDR reports 37
CDR Tools 7
CM login 17
CM login button descriptions 17
Communication Manager 17, 29, 37
configuring DHCP IP address pools 21
Configuring the Directory Service 41
Configuring the phones 41
control MyPhone server button descriptions 34
control system database button descriptions 33
Control Web Server button descriptions 32
controlling CDR Servers 32
controlling MyPhone server 34
controlling system database 33
CSV file 38

D

deleting an external number from LDAP database 47
Detail Screen 44
DHCP 19
    activate 19
    deactivate 19
DHCP IP address 20
DHCP lease 22
DHCP leases display field descriptions 22
DHCP server 7
DHCP server log 22
DHCP server status 19
DHCP service control button descriptions 20
Directory Service Application 41
Display server firmware 16
display stations 16
display stations field descriptions 16
Dynamic Host Configuration Protocol 19

E

e-mail daemon 38
editing an external number in the LDAP database 47
editing DHCP subnets 21
External Numbers 46

F

file server log 29
file server log files 29
file server status 31

G

General Administration 42
General Settings 42

I

IP Phone
- backup 14
- restore 14

IP phone back up and restore 15
IP Phone file server 7
IP Phone firmware management 7
IP phone firmware manager 15
IP Phone Setting Editor field descriptions 14
IP phone settings
- basic editing 12
- configuring view of settings file 11
- saving 13

IP Phone settings
- advanced editing 13
- checking syntax 12

IP phone settings editor 10
IP Phone Settings Editor 7
IPv6 DHCP IP Address Pools
- Updating DHCP IPv6 values 25

IPv6 DHCP Server status 23
- activate/deactivate IPv6 DHCP 23

IPv6 DHCP Server Status
- viewing IPv6 DHCP Server status 23

IPv6 DHCP Sever Log 26
- viewing IPv6 DHCP log files 26

IPv6 Ping Host 10
- pinging an IPv6 host 10

L

LDAP Administration 43
LDAP Filter Settings 45
legal notice 2, 9
Log viewer 7
logging 31

M

managing IP phone settings 11
MyPhone 7, 30, 34
MyPhone Server 30, 34
MyPhone server log files 31
MyPhoneAdmin 30

P

ping 9
- IP host 9
- TCP host 9

pinging a host 9

R

removing DHCP subnets 21

S

schedule control 17
schedule control button descriptions 18
schedule control field descriptions 18
Search Screen Settings 44
Show IPv6 DHCP Leases 25
showing DHCP lease 22
SIP Enablement Server 14
SIP Phone 14
SQL import server 32
subnet 20
system database 30
system database status 33

T

TFTP server 27, 28
TFTP Server
- viewing archive log files 28
- viewing TFTP server access log 27

Translation Language 45

U

Upload files 10
Upload Gateway Firmware 26, 27
- uploading Gateway firmware 27
- viewing Gateway firmware 27

Upload phone firmware 17
utility server 7
Utility Server 14, 29, 37, 38

V

Viewing DHCP lease information 25
viewing DHCP log files 23
viewing DHCP server status 19
viewing DHCP subnets 20

W

Watchdog file 29
Watchdog test 29