Accessing and Managing Avaya Aura® Utility Services

Release 6.3
Issue 3
May 2013

© 2013 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

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 websites referenced within this site or documentation 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 its hardware and Software (“Product(s)”). 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 website: http://support.avaya.com. Please note that if you acquired the Product(s) 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. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

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; 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 you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 you. “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.

License types

- Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order 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.
- Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.
- CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.
- Named User License (NU). You 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). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage

Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product 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 unless expressly authorized by Avaya. 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.

Virtualization

Each virtual appliance has its own ordering code. Note that each instance of a virtual appliance must be ordered separately. If the end-user customer or Business Partner wants to install two of the same type of virtual appliances, then two virtual appliances of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

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 Toll 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 website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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 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.

Avaya and Avaya Aura® are trademarks of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Linux is the registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 7
- Purpose 7
- Intended audience 7
- Document changes since last issue 8
- Related Resources 8
  - Documentation 8
  - Avaya Mentor videos 9
- Support 9
- Warranty 9

Chapter 2: Utility Services overview 11
- Accessing Utility Services applications 12

Chapter 3: Utility Admin 13
- Common 13
  - Viewing the legal notice 13
  - Software Version 13
- Miscellaneous 14
  - Ping Host 14
  - IPv6 Ping Host 14
  - Upload files 15
  - Utility Services Backup and Restore 15
  - Customer Banner Control 16
- Firewall Rules 17
  - Firewall IPv4 17
  - Firewall IPv6 17
  - Viewing firewall rules 17
- IP Phone Tools 18
  - ADVD Settings Editor 18
  - IP Phone Settings Editor 22
  - IP phone backup and restore 27
  - IP Phone Custom File Upload 28
- IP phone firmware manager 29
  - Configure CM Login 29
  - Display stations 30
  - Display firmwareDisplay server firmware 32
  - Manage Phone Firmware 33
  - Schedule Phone File Download 34
- DHCP Manager 36
  - DHCP 36
  - DHCP server status 36
  - Activate or deactivate DHCP 36
  - DHCP IP address pools 37
  - Show DHCP leases 39
  - DHCP server log 40
- IPv6 DHCP Manager 40

IPv6 DHCP Server status ... 40
Activate/Deactivate IPv6 DHCP ... 41
IPv6 DHCP IP Address Pools ... 41
Show IPv6 DHCP Leases ... 42
IPv6 DHCP Sever Log ... 43
Gateway Firmware ... 44
Upload Gateway Firmware ... 44
IP Phone Push Server ... 45
Display Push Database ... 45
Test Push Database ... 45
Application Log View ... 46
File server ... 46
Call Detail Recording ... 47
Messages ... 47
Phone Firmware Manager ... 48
System Database ... 48
MyPhone ... 49
TFTP server ... 49
Application Control ... 50
File server ... 50
Call Detail Recording ... 51
Phone Firmware Manager ... 52
System Database ... 53
MyPhone ... 54
TFTP server ... 55
Call Detail Record Tools ... 56
CDR reports ... 56
CDR backups ... 56
CDR archive ... 57
CDR e-mails ... 57
Chapter 4: Directory application ... 59
General Settings ... 60
Translation Language ... 63
External Numbers ... 64
Appendix A: Accessing the Utility Services database from an external application ... 67
Appendix B: Configuring the Utility Services Standalone Template ... 69
Appendix C: Configuring Call Detail Recording on Communication Manager ... 71
Index ... 73

Chapter 1: Introduction

Purpose

This document provides procedures for managing the features that are part of Utility Services. Features include IP phone settings, ADVD Settings, IP phone firmware management, log viewer, CDR tools, and Enhanced System Directory.

Intended audience

The primary audience for this document is:

- Avaya field technicians
- Avaya partners
- Technical support personnel
- Solution Architects
- Implementation Engineers
- Support Personnel
- Technical support representatives
- Authorized Business Partners

Document changes since last issue

The following change has been made to this document since the last issue:

- Updated the instances of Directory service application to Directory application in the section Directory application on page 59.

Related Resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com/.

Document number	Title	Description	Audience
Administration			
03-603558	*Implementing Avaya Aura® Communication Manager*	This document provides installation, configuration, initial administration, troubleshooting, and basic maintenance checklists and procedures for Avaya Aura® Communication Manager.	Implementation engineers, field technicians, business partners, solution providers, customers
16-300256	*4600 Series IP Telephones Application Programmer Interface (API) Guide*	This document describes how to set up two optional Avaya application interfaces, the Web browser and the Push interface.	Application developers, System administrators who develop or implement Web-based or Push-based applications for Avaya IP Telephones
03-602253	*Avaya Communication Manager Express MyPhone Quick Reference*	This document describes the MyPhone feature and how to administer simple call routing patterns.	Solution architects, Implementation engineers, Support personnel, Technical support representatives, Authorized Business Partners

Document number	Title	Description	Audience
03-602578	*Avaya Communication Manager Express MyPhone Administration Reference*	This document describes the features available to the administrators of Avaya MyPhone for Avaya Communication Manager Express (CME).	Solution architects, Implementation engineers, Support personnel, Technical support representatives, Authorized Business Partners

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: Utility Services overview

Avaya Aura® Utility Services runs a number of utility applications that support or enhance the component applications facilitating a complete single box solution.

With Utility Services Release 6.2 and later, you can connect the Utility Services applications and tools with the duplex Communication Manager or Main Survivable Server template that is running on a separate server. When deployed as a standalone template, the system supports Utility Services for the Communication Manager Duplex deployment solution.

The following sections describe the Utility Services applications.

Utility Admin

Using Utility Admin, you can configure and gain access to the following Utility Services applications:

- Software Version: Displays the software versions of packages, operating system, IP telephone Firmware, media module firmware, and gateway firmware that are installed and active on Utility Services.
- Firewall Rules: Displays the IPv4 and IPv6 firewall rules of Utility Services.
- IP Phone file server: Supports the download of IP telephone firmware and settings files. The server also supports backing up and restoring IP telephone user configuration, for example, speed dial configurations.
- ADVD Settings Editor: Provides a Web-based tool for configuring the Avaya Desktop Video Device (ADVD) settings file. The ADVD Settings Editor significantly simplifies the process of making changes to the ADVD settings file and provides enhanced validation to avoid wrong configurations.
- IP Phone Settings Editor: Provides a Web-based tool for configuring the IP telephone settings file. This significantly simplifies the process of making changes to the IP telephone settings file and provides enhanced validation to avoid wrong configurations.
- IP Phone firmware management: Supports uploading new telephone firmware to the file server.
- DHCP server: Provides basic DHCP server capabilities for supporting IP telephones.
- IPv6 DHCP server: Provides IPv6 DHCP server capabilities for supporting IP telephones.
- IP Phone Push Server: Displays the content from the Push Server Database.
- Log viewer: Supports accessing the log files for all of the Utility Services applications.
- CDR Tools: Provides a Call Detail Records (CDR) collection capability that collects CDR records from Communication Manager and imports the records into the Utility Services database. CDR tool also provides some simple example reports to demonstrate how a system administrator can use the CDR data in the database.

MyPhone Admin

Using MyPhone Admin you can gain access to the following configuration elements of MyPhone and IP telephone operations:

- MyPhone Feature Buttons: You can enable or disable the features available to the users of MyPhone.
- WML Links: The IP Phones can display a default Wireless Markup Language (WML) page. You can use this option to configure the default WML page.
- System Message: You can configure the WML page. This element typically contains a block of text which is relevant to every IP Phone user.

For more information about MyPhone Admin, see *Avaya Communication Manager Express MyPhone Administration Reference*, 03-602578.

MyPhone

Using MyPhone you can configure the IP telephones through a Web interface. You can configure buttons, language settings, EC500, Enhanced Call forwarding, and other features. With MyPhone, you can also change the station security codes and other parameters through the Web interface.

For more information about MyPhone, see *Avaya Communication Manager Express MyPhone Quick Reference*, 03-602253.

MyPhone User Guide

You can download a PDF file and an online HTML file to view the MyPhone documentation.

Accessing Utility Services applications

About this task

Using the Utility Services administration Web pages, you can gain access to various Utility Services applications, administer user settings, and perform other administrative activities.

Procedure

1. Enter the Utility Services 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 Services menu.

Chapter 3: Utility Admin

Common

Viewing the legal notice

Procedure

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

The Legal Notice page displays the copyright and trademarks information.

The system always displays the Legal Notice page after you successfully log on to Utility Services.

Software Version

Use the Software Version page to view the software versions of packages, operating system, IP Telephone Firmware, media module firmware, and gateway firmware that are installed and active on Utility Services.

Viewing the software version

Procedure

Click **Common** > **Software Version**.

The Software Version page displays the packages, operating system, and firmware version information.

Miscellaneous

Ping Host

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

Pinging a host

Procedure

1. Click **Miscellaneous** > **Ping Host**.
2. On the Ping page, enter the Host Name or IP Address of the endpoint.
3. Perform 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. To ping the required endpoint and check the connectivity, click **Execute Ping**.

IPv6 Ping Host

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

Pinging an IPv6 Host

Procedure

1. Click **Miscellaneous** > **IPv6 Ping Host**.
2. On the IPv6 page, enter the Host Name or IPv6 IP Address of the endpoint.
3. Perform 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

Use 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.

Uploading telephone firmware to Utility Services

Procedure

1. Click **Miscellaneous** > **Upload Files**.
2. On the Upload File page, click **Browse** to locate the file.
3. Click **Upload File** to upload the file.

Utility Services Backup and Restore

Use this page to backup and restore Utility Services. Utility Services backup and restore is performed separately from the backup and restore capability of System Platform. Utility Services backup and restore creates exactly the same backup file and uses the same file list. You can use this page to allow the IP telephone and Gateway Firmware to be explicitly included or excluded from all backup that is including from the local page and from System Platform.

Include Firmware in Backup: Use this option to create a complete backup file. Backup files are huge and server takes longer duration to generate the files.

Exclude Firmware in Backup: Use this option to backup the firmware. Excluding the firmware is much faster. If firmware is contained within a backup file, server always restores the firmware.

Note:

Firmware backup setting affects both local and System Platform backups.

Creating a new Utility Services backup file

Procedure

1. In the navigation pane, click **Utility Services Backup and Restore**.
2. On the Utility Services Backup and Restore page, click **Create Backup** to create a new ZIP file of the Utility Services backup files.
   After creating the backup file, the system provides a link to download the newly created Utility Services backup file.
3. Click the **Download the newly create Utility Services Backup File** link to save the ZIP file on the local system.
4. Click **Continue** to return to the Utility Services Backup and Restore page.

Uploading and restoring Utility Services backup file

Procedure

1. Click **Utility Services Backup and Restore**.
2. On the Utility Services Backup and Restore page, click **Browse** to navigate to the file you need to upload.
3. Click **Upload Backup** to upload the backup file.

Customer Banner Control

The Customer Banner Control page displays the current status of the customer banner and a block of text that you can edit. The block of text contains the legal statement about the system that is running on Utility Services. Using the Customer Banner Control page, you can edit, enable, or disable the banner.

Controlling Customer Banner

Procedure

1. Click **Miscellaneous** > **Customer Banner**.
   The Customer Banner Control page displays the customer banner.

2. To enable or disable the customer banner, click **Enable Customer Banner** or **Disable Customer Banner**.
3. To update the customer banner, click **Update Customer Banner**.

Customer Banner Control button descriptions

Name	Description
Enable Customer Banner	Enables the customer banner.
Disable Customer Banner	Disables the customer banner.
Update Customer Banner	Updates the customer banner.

Firewall Rules

Firewall IPv4

The Firewall IPv4 page displays the IPv4 firewall rules of Utility Services. Using the Firewall IPv4 page, you cannot edit or configure the firewall rules.

Firewall IPv6

The Firewall IPv6 page displays the IPv6 Firewall rules of Utility Services. Using the Firewall IPv6 page, you cannot edit or configure the firewall rules.

Viewing firewall rules

Procedure

1. To view the IPv4 firewall rules, click **Firewall Rules** > **Firewall (IPv4)**.
2. To view the IPv6 firewall rules, click **Firewall Rules** > **Firewall (IPv6)**.

IP Phone Tools

ADVD Settings Editor

You can configure settings for an Avaya Desktop Video Device (ADVD) using the ADVD Settings Editor. Most ADVD uses the Axxxsettings.txt file to configure video-related settings such as default Wireless Markup Language (WML) page and the options users can access from the handset. With ADVD settings editor, you can edit this file together with entry checking and help files.

Configuring view of ADVD settings file

Procedure

1. On the left navigation menu, select **ADVD Settings Editor**.
   The system displays the ADVD Settings Editor page.
2. Select the **Display file comments** check box to display the comments located in the Axxxsettings file. If you clear this check box, the comments remain in the Axxxsettings file, but the system does not display the comments.
3. Select the **Display only active options** check box to display only the active settings on the ADVD. Other values remain in the Axxxsettings file as is, but the system does not display the comments.

   Note:

   Comment lines start with double pound keys (##). Active lines start with SET command and contain options that are read by the ADVD. Lines within the file that start with double pound keys (##). 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 the ADVD settings file

Procedure

1. To select a settings file to edit, perform one of the following steps:
   - Download the `Axxxsettings.txt` file from the Utility Services. This method is the default using which you can edit the Axxxsettings file that resides in the

Utility Services. SIP and H.323 videos use the same `Axxxsettings.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 `Axxxsettings.txt` on that server. The application downloads the `Axxxsettings.txt` file for editing.

The application cannot save the file back on the remote server. You must download the edited `Axxxsettings.txt` from the server on the Save page, and then upload the file to the original server.

- To upload a `Axxxsettings.txt` file or `ADVDParameterDefinitions.xml` file from a computer to the server, select **Upload ADVD settings or xml file** and then click **Browse**.

  The `ADVDParameterDefinitions.xml` contains help and entry information for the editor. At present, Utility Services includes the latest version of `ADVDParameterDefinitions.xml` file. This version will be available on the Avaya Support site for later releases. The latest version of the Axxxsettings.txt file is available on the Avaya Support site.

  Note:

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

2. Click **Proceed with selected values** to edit the selected file.
   The system displays the Axxxsettings.txt page with four columns: **Activate**, **Parameter**, **Value**, and **Add Edit Delete**.
3. Perform one of the following steps as required:
   - Performing basic ADVD settings editing on page 19
   - Checking ADVD settings syntax on page 20
   - Performing advanced ADVD settings editing on page 20

Performing basic ADVD settings editing

Procedure

Perform one of the following steps:

- To activate a setting or deactivate a setting in the file, click the check box in the **Activate** column. The system displays the value within the file and ADVD uses 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 ADVD settings syntax

Procedure

Perform one or more of the following steps as required:

- The system displays a setting with orange border if the setting is not found in the xml file in the system and the setting might be invalid. Correctly specify such settings.
- The system displays a setting with red border if the setting is incorrect and the ADVD cannot understand the settings. Click on a settings value to see the detailed information on the problem and correct the value.

Performing advanced ADVD settings editing

Procedure

Perform one or more of the following steps:

- To reload the settings and return to the current line, click **R**. This step is useful if you changed a setting and want to verify if the setting is correct.
- To add a line, click the plus (**+**) sign. The system reloads the page and displays a drop-down menu with all the available ADVD 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 is added below the current line.
- To add a comment, go to statement or raw text and click the plus (**+**) sign. Select the **Comment** option from the bottom of the drop down menu, and click **Add Line**.

- To edit an entire line, click **<**. The system reloads the page and displays the line exactly as 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 the minus (**-**) sign. If you accidentally delete a line, you can reload the original settings file by clicking **ADVD Settings Editor** from the left navigation menu.

Saving ADVD settings

Procedure

1. After finish making the changes, click **Save New Settings File**.
2. On the Output Screen page, perform one of the following steps:
   - To save the file in the Utility Services, click **Save Axxxsettings.txt file to this server**.
   - To download the file to your computer, click either the **Axxxsettings.txt(comments included in file)** link or the **Axxxsettings.txt(no comments)** link.

ADVD Setting Editor field descriptions

Name	Description
Activate	Contains a checkbox. Select the checkbox to signify that the setting is active and ADVD can read the setting. Clear the checkbox to signify that the setting is inactive, displays as commented out in the settings file and the ADVD does not read the settings.
Parameter	Displays comments and settings values. Comments span both the columns, and you can edit the comments using the edit line button in the next column. The system displays the ADVD settings name in the parameter column and the current value in the **Value** column.
Value	Displays comments and settings values. Comments span both the columns, and you can edit the comments using the edit line button in the next column. The system

Name	Description
	displays the ADVD settings name in the parameter column and the current value in the **Value** column
Add **Edit** **Delete** **Reload**	Displays the following buttons: **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 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 the options users can gain access from the handset. With the IP Phone Settings Editor, you can edit this file together with entry checking and help files.

Configuring th edisplay of the IP Phone settings file

Procedure

1. In the left navigation pane, select **IP Phone Settings Editor** from.

   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 you clear this check box, the comments remain in the 46xxsettings file, but the system does not display the comments.
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 the comments.

Note:

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

Editing the IP Phone settings file

Procedure

1. To select a settings file to edit, perform one of the following steps:
   - Download the `46xxsettings.txt` file from the Utility Services. This method is the default using which you can edit the 46xxsettings file that resides in Utility Services. 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 the file back on the remote server. You must download the edited `46xxsettings.txt` from the server on the Save page, and then upload the file back to the original server.

- To upload a `46xxsettings.txt` file or `IpPhoneParameterDefinitions.xml` file from a computer to the server, select **Upload IP phone settings or xml file** and then click **Browse**.

  The `IpPhoneParameterDefinitions.xml` contains help and entry information for the editor. At present, Utility Services includes the latest version of `IpPhoneParameterDefinitions.xml` file. This version 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 to 10 seconds to load the file.

2. To edit the selected file, click **Proceed with selected values**.
   The system displays the 46xxsettings.txt page with four columns:
   - **Activate**
   - **Parameter**
   - **Value**
   - **Add Edit Delete**

   See IP Phone Setting Editor field descriptions on page 26.
3. Perform one of the following steps as required:
   - Performing basic IP Phone settings editing on page 24
   - Checking IP Phone settings syntax on page 25
   - Performing advanced IP Phone settings editing on page 25

Performing basic IP Phone settings editing

Procedure

Perform one of the following steps:

- To activate a setting or deactivate a setting in the file, click the check box in the **Activate** column. The system displays the value within the file and IP Phone uses 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

Procedure

Perform one or more of the following steps as required:

- The system displays a setting with orange border if the setting is not found in the xml file in the system and the setting might be invalid. Correctly specify such settings.
- The system displays a setting with red border if the setting is incorrect and the IP Phones cannot understand the settings. Click on a settings value to see the detailed information on the problem and correct the value.

Performing advanced IP Phone settings editing

Procedure

Perform one or more of the following steps:

- To reload the settings and return to the current line, click **R**. This step is useful if you changed a setting and want to verify if the setting is correct.
- To add a line, click the plus sign (**+**). The system reloads the page and displays a drop-down menu with all the available IP phone options listed in alphabetical order. The existing 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 is added below the current line.
- To add a comment, go to statement or raw text and click the plus sign (**+**). Select the **Comment** option from the bottom of the drop-down menu, and click **Add Line**.
- To edit an entire line, click the less than (**<**) sign. The system reloads the page and displays the line exactly as the line 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 the plus sign (**+**). If you accidentally delete a line, you can reload the original settings file by clicking **IP Phone Settings**

Editor from the left navigation menu. Changes are not saved to the file until the system displays the final page and you select a save option.

Saving IP Phone settings

Procedure

1. After finish making the changes, click **Save New Settings File**.
2. On the Output Screen page, perform one of the following steps:
   - To save the file in the Utility Services, click **Save 46xxsettings.txt file to this server**.
   - To download the file to your computer, click either the **46xxsettings.txt(comments included in file)** link or the **46xxsettings.txt(no comments)** link.

IP Phone Setting Editor field descriptions

Name	Description
Activate	Contains a checkbox. Select the checkbox to signify that the setting is active and IP Phones can read the setting. Clear the checkbox to signify that the setting is inactive, displays as commented out in the settings file and the IP Phones does not read the settings.
Parameter	Displays comments and settings values. Comments span both the columns, and you can edit the comments using the edit line button in the next column. The system displays the IP phone settings name in the parameter column and the current value in the **Value** column.
Value	Displays comments and settings values. Comments span both the columns and you can edit the comments using the edit line button in the next column. The system displays the IP phone settings name in the parameter column and the current value in the **Value** column.

Name	Description
Add **Edit** **Delete** **Reload**	Displays the following buttons: **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.
- Compress the backup files into a ZIP file and store it locally.
- Restore an existing backup file to the Utility Services repository of IP phone backup files.

Note:

The SIP Phones store their configuration information on the SIP Enablement Server. The System Platform master backup also backs up this data.

Backing up an IP Phone settings file

Procedure

1. In the navigation pane, select **IP Phone 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 a link to download the newly created zip file.

Restoring an IP Phone settings file

Procedure

1. In the left navigation pane, click **IP Phone Tools** > **IP Phone Backup and Restore**.
2. To locate an existing ZIP file of the IP Phone backup files, click **Browse**.

3. To upload the backup files to restore later, click **Upload Backup**.

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 Custom File Upload

You can upload the custom files to Utility Services. You can also use the IP Phone Custom File Upload page to install-site specific files such as Custom Screen Saver images. Currently, you can upload a single file or a ZIP file. The files are immediately available and the system overwrites any existing files.

Displaying a custom file

Procedure

1. Click **IP Phone Tools** > **IP Phone Custom File Upload**.
2. On the IP Phone Custom File Upload page, click **Display Custom Directory** to see the custom files.

Uploading and activating custom file

Procedure

1. Click **IP Phone Tools** > **IP Phone Custom File Upload**.
2. To navigate to the file you need to upload, on the IP Phone Custom File Upload page, click **Browse**.

3. To upload a custom file, click **Upload Custom Files and Activate**.

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.

Configure CM Login

The Configure CM Login page contains the login for Communication Manager. Using the Configure CM Login page, you can configure the login that Utility Services will use to communicate with Communication Manager.

Configuring the Communication Manager login

About this task

Use this procedure to configure the login that Utility Services will use to communicate with Communication Manager. Utility Services requires communication with Communication Manager to:

- Display the stations that are registered and the version of firmware that the stations are running
- Schedule the IP telephones to load new firmware and perform the required reset

Procedure

1. Log in to the Utility Services Utility Admin interface.
2. In the navigation pane, under **IP Phone Firmware Manager**, click **Configure CM Login**.
3. Enter the IP address of Communication Manager.
4. Enter the user name.

Important:

The user name and password that you enter must already be configured in Communication Manager.

5. Enter the password.
6. Click **Save Callserver Settings**.
7. To test that Utility Services can communicate with Communication Manager, click **Test Connection**.

Configure CM Login field descriptions

Name	Description
CM Address	Enter the Communication Manager IP Address.
User Name	Enter the user name. **Important:** The user name and password must be configured in Communication Manager. The user name must be bash shell privileged or non Access Secure Gateway (non ASG). If you enter the `dadmin` user name, which does not have the bash shell privileges, and click the **Test Connection** button, the system displays the `Connection to Call Server failed!`.
Password	Enter the password.

Configure CM Login button descriptions

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

Display stations

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

Viewing stations and firmware versions

Before you begin

Configure the Communication Manager login. See Configuring the Communication Manager login on page 29.

About this task

Use this procedure to view a list of configured IP telephone stations that have been administered on Communication Manager. The list also displays the version of firmware that is installed on each telephone.

Procedure

1. Log in to the Utility Services Utility Admin interface.
2. In the navigation pane, under **IP Phone Firmware Manager**, click **Display Stations**.

Note:

The telephone information might take some time to display the first time that you perform this procedure. Results for larger systems will take more time to display than results for smaller systems. Subsequent displays take less time.

Display Stations field descriptions

Name	Description
Extension	The 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 Services.

Display Stations button descriptions

Name	Description
Update Table	Forces the IP Phone Firmware Manager application to log in to Communication Manager and update the Phone Firmware Manager database with the station information.
Refresh Page	Refreshes the current Web page with the current information in the Phone Firmware Manager database.

Display firmwareDisplay server firmware

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

Viewing available firmware

About this task

Use this procedure to view the firmware that is stored locally on Utility Services. If you set an IP telephone to use Utility Services, the system upgrades the IP telephone to the release listed on this page after a reset.

Procedure

1. Log in to the Utility Services Utility Admin interface.
2. In the navigation pane, under **IP Phone Firmware Manager**, click **Display Server Firmware**.
   The Phone Firmware Manager - Display Latest Firmware page lists the latest firmware versions available on Utility Services.

Manage Phone Firmware

Managing firmware

About this task

Use this procedure to view, unpack, activate, deactivate, or remove endpoint firmware from Utility Services.

Procedure

1. Log in to the Utility Services Utility Admin interface.
2. In the navigation pane, under **IP Phone Firmware Manager**, click **Upload Phone Firmware**.
3. Select the firmware package to view, unpack, activate, deactivate, or remove.
4. Click the appropriate button:
   - **View**
   - **Unpack**
   - **Activate**
   - **Deactivate**
   - **Remove**

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 firmware available to the Utility Server.
Deactivate	Deactivates the selected firmware package and remove firmware from the web server.
Remove	Deletes the extracted files as well as the ZIP archive.

Schedule Phone File Download

With the Schedule Phone File Download page, you can 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 specify the date and time to reset the IP phones.

Scheduling endpoint reset to load firmware

Before you begin

Configure the Communication Manager login. See Configuring the Communication Manager login on page 29.

About this task

Use this procedure 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.

Procedure

1. Log in to the Utility Services Utility Admin interface.
2. In the navigation pane, under **IP Phone Firmware Manager**, click **Schedule Phone File Download**.
3. Select options on the Phone Firmware Manager – Schedule Control page, and enter the appropriate information when required.
4. Click **Schedule Phone Firmware Update**.

Schedule Phone File Download field descriptions

Name	Description
Select Phones	The list of IP phones from which you select one or more IP Phone to reset based on the phone type and firmware.
Select Start Time	The time when the reset operation starts. You can choose to reset a phone

Name	Description
	immediately, or you can set a date and time to reset later.
Select Stop Time	The time when the system stops the reset or reboot operation. You can specify the date and time for the reset operation.
Select whether a phone may be updated while being active	An option to enable the system to reset the phones that are currently active on a call. You can set the option to No or Yes.
Select whether a phone running the latest firmware should be reset	An option to enable the system to reset only those phones that do not run the same version of firmware as on Utility Services. Set this option to Yes if you made 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 the system fails to upgrade the phone to the firmware on Utility Services. The number of retries is limited by the stop time specified in 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	The option to schedule 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 Phone File Download button descriptions

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

DHCP Manager

DHCP

Dynamic Host Configuration Protocol (DHCP) 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 Services 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

Procedure

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

Activate or deactivate DHCP

Use the **Activate/Deactivate DHCP** feature to activate or deactivate the DHCP server. When you activate the server, the system displays a status message. A DHCP server in a running state indicates that the `dhcpd.conf` file is correctly created and the DHCP server has started. A DHCP server that does not start indicates a problem in the `dhcpd.conf` file, and the system displays an error message to indicate the likely cause of the problem.

Activating and deactivating a DHCP server

Procedure

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

DHCP Service Control button descriptions

Name	Description
Activate DHCP Server	Activates the DHCP server. On the DHCP Service Control page, you can see **RUNNING** to indicate the active state.
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

Procedure

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 system displays the raw details of the file.

Adding a DHCP subnet

Procedure

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

Procedure

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

Procedure

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 subnets from the DHCP network.
4. In the confirm message window, click **OK**.

Show DHCP leases

On the DHCP Leases Display page, you can view the DHCP lease information, the percentage of IP addresses in use, and the addresses of the current endpoints. This information is useful for knowing when pools are nearly all used.

Viewing DHCP lease information

Procedure

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, the last usage duration of the IP ports, and the binding states of the IP ports.

DHCP Leases Display field descriptions

Name	Description
Range Start	The start of the range of IP addresses that you can use in DHCP.
Range End	The end of the range of IP addresses that you can use in DHCP.
Range Size	The total number of IP addresses available in the range for DHCP.
IP addresses in use	The total number of IP addresses that are currently in use within the range of IP addresses.
Percentage in use	The percentage for the number of IP addresses in use within the range of IP addresses.
Binding State	The current status of 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.

Name	Description
MAC Address	The 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 and use the information to troubleshoot DHCP-related problems.

Viewing DHCP log files

Procedure

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

Procedure

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

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

Activate/Deactivate IPv6 DHCP

Use the Activate/Deactivate IPv6 DHCP page to activate or deactivate the IPv6 DHCP server using the utility server. When you activate the server, the system displays a status message from the utility service. An IPv6 DHCP server in a running state indicates that the `dhcpd.conf` file is correctly created and the IPv6 DHCP server has started. An IPv6 DHCP server that does not start indicates a problem in the `dhcpd.conf` file, and the system displays an error message to indicate the likely cause of the problem.

DHCP Service Control button descriptions

Name	Description
Activate DHCP Server	Activates the DHCP server. On the IPv6 DHCP Service Control page, you can see RUNNING to indicate the active state.
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 an IPv6 DHCP server

Procedure

1. Click **IPv6 DHCP Manager** > **Activate/Deactivate IPv6 DHCP**.
   The IPv6 DHCP Service Control page displays the status of the IPv6 DHCP server.
2. To activate or deactivate the DHCP server based on the current status of the DHCP server, click **Activate DHCP Server** or **Deactivate DHCP Sever**.
3. To load the last working DHCP configuration file, click **Load last woring DHCPD conf file**.

IPv6 DHCP IP Address Pools

You can use the IPv6 DHCP IP Address Pools option to configure IPv6 DHCP IP addresses. You can update a DHCP address to the 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 that is identical to the start and stop addresses.

Updating DHCP IPv6 values

Procedure

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

On the IPv6 DHCP Leases Display page, you can view the IPv6 DHCP lease information, the percentage of IP addresses in use, and the addresses of the current endpoints. This information is useful for knowing when pools are nearly all used.

IPv6 DHCP Leases Display field descriptions

Name	Description
Range Start	The start of the range of IPv6 addresses that you can use in DHCP.
Range End	The end of the range of IPv6 addresses that you can use in DHCP
Range Size	The total number of IPv6 addresses available in the range for DHCP.
IP addresses in use	The total number of IPv6 addresses that are currently in use within the range of IP addresses.
Percentage in use	The percentage of the number of IPv6 addresses in use within the range of IP addresses.
Binding State	The current status of 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

Name	Description
MAC Address	IPv6 addresses of a particular computer or laptop. This address is used for physical identification of a particular Ethernet code.

Viewing DHCP lease information

Procedure

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

The IPv6 DHCP Leases Display page shows two pieces of information:

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

IPv6 DHCP Sever Log

You can view the server logs and use the information to troubleshoot IPv6 DHCP-related problems.

Viewing IPv6 DHCP log files

Procedure

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.

Gateway Firmware

Upload Gateway Firmware

This feature enables Utility Server to support Trivial File Transfer Protocol (TFTP) access for Media Module and Gateway Firmware. Using Upload Gateway Firmware, you can view the firmware and also upload a new firmware file on Utility Server.

Viewing Gateway firmware

Procedure

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

Procedure

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.

IP Phone Push Server

Display Push Database

Avaya IP telephones support the Push mechanism. The IP telephones use the Push functionality to display emergency information, appointment reminders, or general internal communications to your screen from a trusted server.

Utility Services provides a Push Database and a registered trusted push server. The Push Database contains a list of extensions and names. Use this page to display the content from the Push Server Database. All IP telephones must be registered with the Utility Services.

For more information on Push interface and administration, see *4600 Series IP Telephones Application Programmer Interface (API) Guide*.

With the administrator login credentials, you can access the Postgres table and write your own applications.

The IP telephones register to receive Push messages, you must register the IP telephones. However, IP telephones remain registered even after logoff. Therefore, you must age the registrations and set a resubscription process at required intervals.

Button	Description
Refresh Page	Refreshes the IP telephone Push Server - Display Push Database page.
Re-Subscribe Extensions	Marks all registration entries as expired. The button also requests that each device reregisters. On successful reregistration, the system updates and validates the records.
Purge Database	Deletes all expired records.

Test Push Database

Use this page to diagnose and to test the Push capability of Utility Services. You can push content from the applications to the registered telephones. Use this page to allow each mode and type of Push message to be sent to a single device, several devices, or all devices simultaneously.

Sending Push messages

Procedure

1. Click **IP Phone Push Server** > **Test Push Server**.
2. On the IP Phone Push Server - Test Push Server page:
   a. To select all the extensions, click **Select All Extensions**.
   b. To deselect the extension, click **Select No Extensions**.
3. Select the type of PUSH message: Topline and Display.
4. Select the number of alert tones: Silent, One Beep, Two Beeps, and Three Beeps.
5. Select the priority of PUSH message. Available values are Normal and Barge.
6. In the **PUSH Message to be sent** text field, enter the message.
7. Click **PUSH Message** to send the message.

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 files, and the history log files. The system maintains the secure and nonsecure access logs separately and also provides separate log files for 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 Services. The Watchdog tests the file server on a regular basis and restarts the server if the file 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 when rebooted. 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 to make the changes to the log levels effective.

Note:

Error logs do not support filtering.

Viewing file server log files

Procedure

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 handle Call Detail Records (CDR) that Communication Manager generates. At present, five separate daemons perform the following five functions: Collect data from Communication Manager. Import data to Utility Services. Export history data. Back up data. Generate automated e-mail reports.

Viewing CDR log files

Procedure

1. Click **Application Log View** > **Call Detail Recording**.
2. Click **View Log** to view a particular log file, for example, CDR Collectors Activity log and CDR Importers Activity log.
3. To download the log file, click **Download Log**.

Messages

Use the View Linux Messages Log Files page to view and download the Linux Messages log files.

You can:

- view the log files, such as Messages Server Access Log and View Archive Log Files.
- zip the archived log files, download, and save the log files on your local drive.
- download the historic data to diagnose the system.

Viewing Linux Messages log files

Procedure

1. Click **Application Log View** > **Messages**.
   The system displays the View Linux Messages Log Files page.
2. Click **View Log** to view a particular log file, for example, Messages Server Access Log and View Archive Log Files.
3. To download the log file, click **Download Messages Log**.

Phone Firmware Manager

The Phone Firmware Manager (PFM) server updates the firmware of Avaya IP Phones. Use the View Phone Firmware Manager Server Log Files page to view and download the Phone Firmware Manager Server Access log files.

Viewing Phone Firmware Manager Server log files

Procedure

1. Click **Application Log View** > **Phone Firmware Manager**.
   The system displays the View Phone Firmware Manager Server Log Files page.
2. Click **View Log** to view a particular log file, for example, PFM Server Access Log.
3. To download the logs, click **Download PFM Server Access Log**.

System Database

The Utility Services 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

Procedure

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

MyPhone

With the MyPhone application, you can change the station security code and station buttons. The application includes an administrator interface to control the buttons that 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. The MyPhone server includes 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 the MyPhone application.

Note:

Avaya recommends that you keep the MyPhone option turned off so that users cannot modify the settings on the phone, for example, the security code.

Viewing MyPhone server log files

Procedure

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. On the respective log file page, click **Download Log**.

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

Procedure

1. Click **Application Log View** > **TFTP Server**.
2. To view the TFTP sever access log, click **View Log**.
   The system displays View TFTP Server Log Files page.

Viewing archive log files

Procedure

1. Click **Application Log View** > **TFTP Server**.
2. To view the archive log files, click **View Log**.
   The system displays View Archive Log Files page.

Application Control

File server

The Control Web Server 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 the changes to the log levels effective.

Note:

You cannot change the operation of the File Server when a server reboots or stop the File Server when a server reboots.

Viewing file server status

Procedure

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. Perform one of the following steps as appropriate:
   - 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

Procedure

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 Importer** 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.

Control CDR Servers field descriptions

Name	Description
CM Username	Enter the Communication Manager user name.
CM Password	Enter the password.

Phone Firmware Manager

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

You can use the Phone Firmware Manager option to check whether the PFM server is running or not. On the Control Phone Firmware Manager (PFM) Server page, you can see **RUNNING** to indicate the active state of the PFM server.

Controlling Phone Firmware Manager server

Procedure

1. Click **Application Control** > **Phone Firmware Manager**.

The Control Phone Firmware Manager (PFM) Server page displays the current status of the PFM server.

2. To start or stop the PFM Server, click **Start the PFM Server** or **Stop the PFM Server**.
3. To enable or disable autostart of the PFM Server after a reboot, click **Enable Autostart of the PFM Server** or **Disable Autostart of the PFM Server**.

Control Phone Firmware Manager Server button descriptions

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

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 the operation of the system database after a reboot.

Controlling System Database

Procedure

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

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 the MyPhone operation after a reboot.

Controlling MyPhone server

Procedure

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.

Name	Description
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.

TFTP server

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

Controlling TFTP server

Procedure

1. Click **Application Control** > **TFTP Server**.
   The Control TFTP Server page displays the current status of the TFTP server.
2. To start or stop the TSTP server, click **Start the TFTP Server** or **Stop the TFTP Server**.
3. To enable or disable autostart of the TFTP server after a reboot, click **Enable Autostart of the TFTP Server** or **Disable Autostart of the TFTP Server**.

Control TFTP Server button descriptions

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

Call Detail Record Tools

CDR reports

You can use the CDR Reports option to view the CDR Reports currently available. The system collects the CDR records from Communication Manager and imports the records to the Utility Services database.

Viewing CDR reports

Procedure

1. Click **CDR Tools** > **CDR Reports**.
2. Click **View CDR Report** to view a CDR report from the available options, for example, the 10 longest calls, the 10 most active extensions, the 10 most dialed numbers, and the raw CDR data.

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

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 Comma Separated Values (CSV) file. You can use the CDR Backups option to download the data and store the data 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. At any given time, you can gain access to a maximum of 12 months of online data and 12 months of previous offline data in Utility Services.

Gaining access to CDR backup files

Procedure

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

CDR archive

The CDR Compress daemon compresses the raw CDR files collected from Communication Manager as ZIP files, and stores the files in a directory named by month or year. You can use the CDR Archive option to download these compressed zip files.

Accessing the CDR archive

Procedure

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 e-mails

By using the Control CDR E-Mails page, you can configure and control the operation of each of the three regular e-mail daemons: daily, weekly, and monthly. You can enable or disable each daemon separately. You can configure each daemon to generate up to three separate reports and send the reports to a configurable list of recipients.

CDR E-Mails field descriptions

Name	Description
E-Mail Daemon	Enable or disable e-mail daemon for each of the three regular daemons: daily, weekly, and monthly.

Name	Description
Longest Calls	Generate a report for the longest calls you have made over a period of time.
Most Active	Generate a report for the most active extensions that you have called.
Most Dialed	Generate a report of the most dialed numbers when you make calls.
Distribution List	Send the reports to a list of recipients by e-mail. You can separate each e-mail address in the distribution list with a semicolon.

CDR E-Mails button descriptions

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

Chapter 4: Directory application

Using the Directory application, you can search an LDAP database using browsers that are compatible with your 46xx and 96xx telephones. You can use the Web pages to configure the Directory application to connect to an LDAP database and to customize the user search experience. Directory application supports 250 instances of the Directory configuration and provides multi-language support for each of these instances. For a more detailed description of the Directory application feature and the required configuration, see *Directory Application Job Aid* on the Avaya Support website at https://support.avaya.com.

Configuring the Directory application

About this task

You must configure the Directory application correctly for the Wireless Markup Language (WML) Browsers to perform search operations.

Procedure

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

Configuring the telephones

Procedure

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

Utility Server includes a `46xxsettings.txt` file. The WMLHOME parameter is automatically set up to point to a landing page that 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 application.

General Administration

Directory number

Select any number between one and 250 and the system configures Directory 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 the search screen of the telephone browsers can display.

HTTP

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

Warning:

When you enable the Directory application on the HTTP port or unsecured port 80, you allow any browser to gain access to the Directory application without authentication or encryption mechanisms. Unauthorized users can gain access to directory information that is stored on your LDAP server using the Directory interface.

HTTPS

Select Enable to enable HTTPS traffic. If you enable HTTPS, the Directory 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 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. You should open the port only for outbound traffic.

Base DN (Search Root)

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

Base DN (External Search Root)

Specify an LDAP Base Distinguished Name where the external numbers are stored. With the Manage External Numbers screen, you can use this root to list, add, or delete entries in the external directory. This distinguished name must be under the Search Root to enable the Directory 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.

User ID

Specify a User ID to connect to the LDAP server. If you do not provide a User ID, the Directory application uses an 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 specified for the LDAP server.

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.

Secure Connection (TLS support)

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

Test Connection

Click **Test Connection** to ensure that the Directory application can connect to the LDAP server using the connection parameters you specified in Secure Connection (TLS support) section.

Search Screen settings

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

Search Attribute

Select from the list of available LDAP attributes or choose a new attribute. Enter the LDAP attribute name in the space provided. For example, the LDAP attribute for Name can be cn or cn;lang-en. A second attribute can be a telephone number or any attribute associated with the telephone number.

Note:

A valid LDAP attribute name can be an alphabetic character, a number, and the minus (-) and colon (;) symbols. 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 telephone search screen.

Minimum Search String

Enter the minimum number of characters with values between one and nine required for user entered Search strings. The directory application denies a search with a search string containing less than the minimum number of characters required.

Detail Screen settings

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

Detail Attribute

Select from the list of available LDAP attributes or choose a new attribute. Enter the attribute name in the space provided. For example, the LDAP attribute for Name can be cn or cn;lang-en. A second attribute can be a telephone number or any attribute associated with the telephone number.

Note:

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

Associated Label

Enter the label that the system displays before the actual value on the detail screen.

LDAP Filter Settings

You can customize the LDAP Filter settings of the Directory 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. The system has 11 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 11 predefined languages, the system displays English text mapping English translations. In either of these scenarios, you can edit the English text in the translation mapping column.

The following list includes the 11 predefined language translations:

- Brazilian-Portuguese
- English
- French
- German
- Italian
- Japanese
- Korean
- Lat-Spanish
- Russian
- Simplified Chinese
- Traditional Chinese

Using the translation language settings, the user can edit the translation string in the right column of 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.

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

Procedure

1. Enter the Utility Services URL on your Web browser.
2. Click **Administration** > **Directory Application**.

3. On the Directory Application Administration page, click **External Numbers**.
4. On the External Numbers Administration page, click **Add**.
5. In **Native Name** field, specify a Unicode name.
6. In the **Name** field, specify an ASCII name.
7. In the **Phone Number** field, enter a telephone number.
8. In the **E-mail** field, specify an e-mail address.

   Note:

   The **Native Name** and **Phone Number** fields are mandatory.
9. To add the external number to the LDAP database and go back to the External Numbers screen, click **Save**.
10. To view your changes, click **Refresh**.

Editing an external number in the LDAP database

Procedure

1. On the Directory Application Administration page, click **External Numbers**.
2. Select an entry in the List page.
3. Click **Edit**.
4. 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.
5. To save your changes to the LDAP database and go back to the External Numbers screen, click **Save**.
6. To view your changes, click **Refresh**.

Deleting an external number from LDAP database

Procedure

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.

Appendix A: Accessing the Utility Services database from an external application

To gain access to the Postgres database, use Utility Services. To gain access to the Postgres databases, use the administrator credentials. You gain read-only access.

The Utility Services database contains the Call Detail Records (CDR) as the database CDR and the Push Registration Database as PUSH. You can access the CDR and the Push Registration Database from an external application as standard Postgres database. To access the database, use the base IP Address of Utility Services on port 5432.

The database schemas are as follows:

Call Detail Record

```
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)
)
```

Push

```
TABLE subscription
(
  macaddr varchar(25) NOT NULL DEFAULT 'UNKNOWN'::bpchar,
  extn varchar(12) NOT NULL DEFAULT '0'::bpchar,
  ipaddr varchar(15) NOT NULL DEFAULT '0'::bpchar,
  setid varchar(10) NOT NULL DEFAULT 'UNKNOWN'::bpchar,
  lastupdate date DEFAULT '2011-07-27'::date,
  extnvalid bool DEFAULT true,
  CONSTRAINT subscription_pk PRIMARY KEY (extn)
)
```

Appendix B: Configuring the Utility Services Standalone Template

Configuring MyPhone

You can configure the MyPhone application using the MyPhoneAdmin application on Utility Services. These applications have their own help files that Utility Services has provided in both HTML and PDF formats. You can access the MyPhoneAdmin application by performing the following steps:

1. Browse to the IP address of Utility Services.
2. From the **Utilities** menu, select **MyPhone Admin** option.
3. Log in using the default administrative account.

Use the **MyPhone AES, CM, and SES Access** to gain access to Communication Manager to be administered. The default account is called MyPhone and installation that use Post-Install wizards configures this account automatically with minimal require permissions. Use the **test connection** option to verify connectivity prior to saving this configuration.

Configuring the Phone Firmware Manager

The Phone Firmware Manager (PFM) requires access to Communication Manager to perform status enquiries and schedule firmware upgrades. This account can be any user account that has SAT access and can also be the same as the account used for MyPhone. You can gain access to Phone Firmware Manager using from the **Configure CM Login** option of the **IP Phone Firmware Manager** menu of the Utility Services Administration pages. Using this option you can configure: IP address of Communication Manager, user account, and user password. Use the **test connection** option to verify connectivity prior to saving this configuration.

Important elements of the 46xxsettings.txt file

Post-Install Wizard configures the 46xxsettings.txt file when the template is first installed, but you can edit or replace the file after installation. You can configure several elements to link up to Utility Services for various features. While configuring the following elements, you must replace <IP> with the Utility Services IP address:

- **IP Phone Backup and Restore**: By default, Utility Services can act as an IP Phone Backup and Restore server. You can configure either HTTP or HTTPS and the subdirectory “PhoneBackup” is important. Utility Services only allows Avaya IP Phones to read and write to this directory. You can configure the element typing the following command in the configuration file: **`SET BRURI http://<IP>/PhoneBackup or https://<IP>/PhoneBackup`**.
- **PUSH**: By default, Utility Services can act as both a Push Registration server and as a Trusted Push server. You can configure the element by performing the following steps in the configuration file:
    a. Type the **`SET TPSLIST <IP>`** command.
    b. Type the **`SET SUBSCRIBELIST http://<IP>/push/subscribe.php`** command.

- **WML Home Page**: By default, Utility Services provides a default WML Home Page. You can configure the element typing the following command in the configuration file: **`SET WMLHOME http://<IP>/landing.wml`**.
- **ESD Landing Pages**: By default, Utility Services provides access to the Enterprise System Directory application. However, you must add the following command at the end of the configuration file to gain access to the full configuration: **`GET ESD_Landing.txt`**.

Appendix C: Configuring Call Detail Recording on Communication Manager

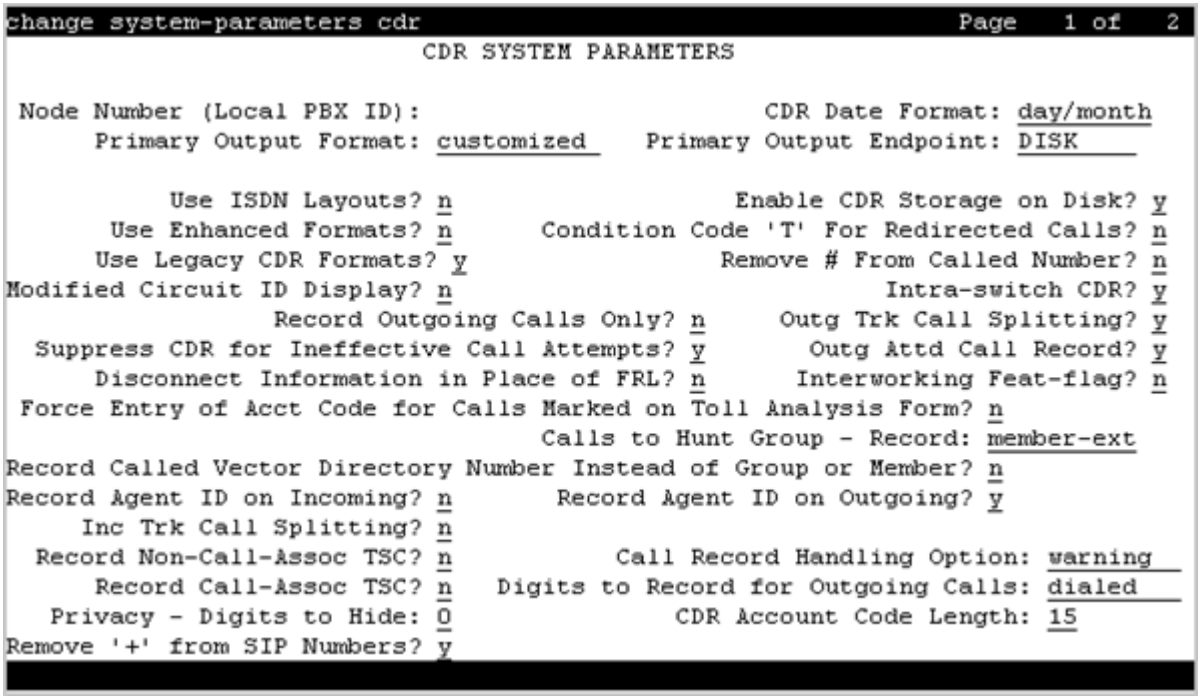
About this task

The Call Detail Record (CDR) capability of Utility Services requires a very specific configuration of Communication Manager to operate successfully. Most of the Post-Install Wizards configure Communication Manager automatically for operation with Utility Services, but this is not possible when Utility Services is collecting CDR data from an existing system.

For CDR collection to operate correctly, perform the following steps:

Procedure

1. Create a new user of the CDR_User type on Communication Manager and administer the new username and password on Utility Services in step 3. The CDR_User type has the required privilege to gain access to the CDR data.
2. Configure the CDR format to ensure that the correct data elements are passed to Utility Services. Refer to the following figures.



```
change system-parameters cdr                                    Page   1 of   2
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID):                          CDR Date Format: day/month
      Primary Output Format: customized   Primary Output Endpoint: DISK

           Use ISDN Layouts? n                    Enable CDR Storage on Disk? y
       Use Enhanced Formats? n       Condition Code 'T' For Redirected Calls? n
      Use Legacy CDR Formats? y                  Remove # From Called Number? n
Modified Circuit ID Display? n                               Intra-switch CDR? y
                 Record Outgoing Calls Only? n     Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? y       Outg Attd Call Record? y
      Disconnect Information in Place of FRL? n      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                  Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? n
  Record Non-Call-Assoc TSC? n           Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0              CDR Account Code Length: 15
Remove '+' from SIP Numbers? y
```

```
change system-parameters cdr                                    Page   2 of   2
                              CDR SYSTEM PARAMETERS

     Data Item - Length          Data Item - Length          Data Item - Length
 1: date              - 6    17: attd-console     - 2    33:                  -
 2: time              - 4    18: auth-code        - 13   34:                  -
 3: sec-dur           - 5    19: return           - 1    35:                  -
 4: cond-code         - 1    20: line-feed        - 1    36:                  -
 5: code-dial         - 4    21:                  -      37:                  -
 6: code-used         - 4    22:                  -      38:                  -
 7: dialed-num        - 23   23:                  -      39:                  -
 8: clg-num/in-tac    - 15   24:                  -      40:                  -
 9: acct-code         - 15   25:                  -      41:                  -
10: ppm               - 5    26:                  -      42:                  -
11: in-crt-id         - 3    27:                  -      43:                  -
12: out-crt-id        - 3    28:                  -      44:                  -
13: isdn-cc           - 11   29:                  -      45:                  -
14: feat-flag         - 1    30:                  -      46:                  -
15: frl               - 1    31:                  -      47:                  -
16: clg-pty-cat       - 2    32:                  -      48:                  -

                              Record length = 120
```

3. Open an Administrative Web session on Utility Services.
4. Click **Application Control** option from the **Call Detail Recording** menu.
5. Enter the username and password administered in the earlier step.
6. Click **Enable Password Mode** to update the configuration.

Note:

By default, the CDR Daemons are disabled and you must enable CDR Daemons as required. CDR Collector must be stopped and started for any changes in configuration to be applied. If the Communication Manager details are updated prior to enabling the CDR daemon, then the CDR Collector must only be started for the changes to be effective.

Index

Numerics

46xxsettings.txt 22, 23

A

accessing CDR backup files 57
accessing utility server 12
accessing utility server applications 12
Activate/Deactivate IPv6 DHCP 41
    activating and deactivating IPv6 DHCP server 41
activating and deactivating DHCP server 37
add a subnet 38
adding a new external number 64
ADVD Setting Editor field descriptions 21
ADVD settings 18–20
    advanced editing 20
    basic editing 19
    checking syntax 20
    configuring view of settings file 18
ADVD settings editor 18
ADVD Settings Editor 21
    saving ADVD settings 21
Application Control 52, 53, 55
    control phone firmware manager server button descriptions 53
    control TFTP server button descriptions 55
    controlling phone firmware manager server 52
    controlling system database 53
    controlling TFTP server 55
    phone firmware manager 52
    TFTP server 55
Application Log View 47, 48
    Messages 47
    Phone Firmware Manager 48
    Viewing PFM Server log files 48
Audience 7
Avaya Mentor videos 9
Axxxsettings.txt 18

B

back up and restore 27

C

Call Detail Record 47
    CDR log files 47
call detail recording 47, 51
Call Detail Recording 52
Call Detail Records Collector 47
catalina.out 49
CDR 47, 51, 52
CDR archive 57
CDR backup 56
CDR backup files 57
CDR e-mail 57
CDR e-mail button descriptions 58
CDR e-mail field descriptions 57
CDR export daemon 56
CDR report 56
CDR reports 56
CDR Tools 11
CM login button descriptions 30
Communication Manager 29, 47, 56, 57
Communication Manager login 29
    configuring in Utility Services 29
Configure CM login 29
Configure CM Login field descriptions 30
Configuring Call Detail Recording on Communication Manager 71
configuring DHCP IP address pools 38
Configuring the Directory application 59
Configuring the telephones 60
Configuring the Utility Services Standalone Template 69
Control CDR Servers 52
    field descriptions 52
control MyPhone server button descriptions 54
control system database button descriptions 54
Control Web Server button descriptions 51
controlling CDR Servers 52
controlling customer banner. 16
controlling MyPhone server 54
CSV file 56
Customer banner control 16
Customer Banner Control button descriptions 17

D

deleting an external number from LDAP database 65
Detail Screen 63
DHCP 36
    activate 36

deactivate 36
DHCP IP address 37
DHCP lease 39
DHCP leases display field descriptions 39
DHCP server 11
DHCP server log 40
DHCP server status 36
DHCP service control button descriptions 37
Directory application 59
display firmware 32
Display server firmware 32
display stations 30
display stations field descriptions 31, 32
document changes 8
Dynamic Host Configuration Protocol 36

E

e-mail daemon 57
editing an external number in the LDAP database 65
editing DHCP subnets 38
External Numbers 64

F

file server log 46
file server log files 47
file server status 50, 51
Firewall 17
IPv4 17
IPv6 17
firmware 15, 32, 33
managing 33
uploading to Utility Services 15
viewing on Utility Services 32

G

General Administration 60
General Settings 60

I

IP Phone 27
backup 27
restore 27
IP phone back up and restore 28
IP Phone file server 11
IP Phone firmware management 11
IP phone firmware manager 29
IP Phone Setting Editor field descriptions 26
IP phone settings 22, 24, 26
basic editing 24
configuring view of settings file 22
saving 26
IP Phone settings 25
advanced editing 25
checking syntax 25
IP phone settings editor 22
IP Phone Settings Editor 11
IP Phone Tools 28
displaying custom file 28
IP Phone Custom File Upload 28
uploading and activating custom file 28
IP telephone Push Server 45, 46
display push database 45
sending push messages 46
test push database 45
IPv6 DHCP IP address pools 41
IPv6 DHCP IP Address Pools 42
Updating DHCP IPv6 values 42
IPv6 DHCP Server status 40, 41
activate/deactivate IPv6 DHCP 41
IPv6 DHCP Server Status 40
viewing IPv6 DHCP Server status 40
IPv6 DHCP Sever Log 43
viewing IPv6 DHCP log files 43
IPv6 Ping Host 14
pinging an IPv6 host 14

L

LDAP Administration 61
LDAP Filter Settings 63
legal notice 2
Log viewer 11

M

managing ADVD settings 18
managing IP phone settings 23
MyPhone 11, 49, 54
MyPhone Server 49, 54
MyPhone server log files 49
MyPhoneAdmin 49

P

ping 14
IP host 14
TCP host 14
pinging a host 14

R

related resources 9
Avaya Mentor videos 9
removing DHCP subnets 38

S

Schedule Phone File Download 34
schedule control 34
schedule phone file download button descriptions 35
schedule phone file download field descriptions 34
Search Screen Settings 62
Show IPv6 DHCP Leases 42
showing DHCP lease 39
SIP Enablement Server 27
SIP Phone 27
SQL import server 51
stations 31
viewing in Utility Services 31
subnet 37
support 9
contact 9
system database 48, 49
system database status 53

T

TFTP server 49
TFTP Server 50
viewing archive log files 50
viewing TFTP server access log 50
Translation Language 63

U

Upload files 15
Upload Gateway Firmware 44
uploading Gateway firmware 44
viewing Gateway firmware 44
Upload phone firmware 33
Utility Server 27, 47, 56
Utility services 11
Utility Services 13, 15, 29, 31–33, 46, 56, 67
configuring login for Communication Manager 29
database schema 67
managing firmware 33
software version 13
uploading telephone firmware 15
viewing available firmware 32
viewing stations 31
viewing the legal notice 13
viewing the software version 13
Utility Services Backup and Restore 15, 16
creating a new Utility Services backup file 16
uploading and restoring Utility Services backup file 16

V

videos 9
Avaya Mentor 9
Viewing DHCP lease information 43
viewing DHCP log files 40
viewing DHCP server status 36
viewing DHCP subnets 37
Viewing firewall rules 17
IPv4 and IPv6 17
Viewing Linux Messages log files 48

W

Warranty 9
Watchdog file 46
Watchdog test 46