Accessing and Managing Avaya Aura® Utility Services

Release 7.0.1
Issue 3
March 2018

© 2012-2018, 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 may generally make available to users of its products and Hosted Services. 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 Avaya hardware and software. 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "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. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance 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, Instance, 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 or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance 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 one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance 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 each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of 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 is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. 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 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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service 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"). As required, 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 products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(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, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

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

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 8
- Purpose 8
- Change History 8
- Warranty 9

Chapter 2: Utility Services overview 10
- Out of Band Management 10
- Utility Admin 11
- MyPhone Admin 12
- MyPhone 12
- MyPhone User Guide 13
- Deploying Utility Services 13
- Audit Account Addition 13
- IP Phone Firmware Removal 13

Chapter 3: Utility Admin 14
- Common 14
  - Viewing the legal notice 14
  - Software Version 14
- Miscellaneous 15
  - Ping Host 15
  - IPv6 Ping Host 15
  - Upload files 16
  - Utility Services backup and restore 16
  - Customer Banner Control 17
  - NTP Status 18
  - RFA License Activation 18
- Firewall Rules 18
  - Firewall IPv4 18
  - Firewall IPv6 18
  - Viewing firewall rules 18
- IP Phone Tools 19
  - ADVD Settings Editor 19
  - IP Phone Settings Editor 23
  - IP phone backup and restore 26
  - IP Phone Custom File Upload 27
- IP phone firmware manager 28
  - Configure CM Login 28
  - Display stations 29
  - Display server firmware 31
  - Manage Phone Firmware 31

Schedule Phone File Download.......... 32
DHCP Manager.......... 34
DHCP.......... 34
DHCP server status.......... 34
Activate or deactivate DHCP.......... 34
DHCP IP address pools.......... 35
Show DHCP leases.......... 36
DHCP server log.......... 37
IPv6 DHCP Manager.......... 37
IPv6 DHCP Server status.......... 37
Activate/Deactivate IPv6 DHCP.......... 38
IPv6 DHCP IP Address Pools.......... 39
Show IPv6 DHCP Leases.......... 39
IPv6 DHCP Sever Log.......... 40
Gateway Firmware.......... 41
Upload Gateway Firmware.......... 41
IP Phone Push Server.......... 42
Display Push Database.......... 42
Test Push Database.......... 42
Application Log View.......... 43
File server.......... 43
Call Detail Recording.......... 44
Messages.......... 44
Phone Firmware Manager.......... 44
System Database.......... 45
MyPhone.......... 45
TFTP server.......... 46
Application Control.......... 46
File server.......... 46
Call Detail Recording.......... 47
IP Phone Firmware Manager.......... 48
System Database.......... 49
MyPhone.......... 50
TFTP server.......... 50
Call Detail Record Tools.......... 51
CDR reports.......... 51
CDR backups.......... 52
CDR archive.......... 52
CDR e-mails.......... 52
Chapter 4: Directory Application.......... 54
General Settings.......... 55
Administering the General Administration section.......... 55
Administering the LDAP Administration section.......... 56

Administering the Search Screen settings section........ 57
Administering the Detail Screen settings section........ 58
Administering the LDAP Filter Settings section........ 58
Translation Language........ 59
External Numbers........ 59
Chapter 5: Resources........ 62
Documentation........ 62
Finding documents on the Avaya Support website........ 63
Training........ 63
Viewing Avaya Mentor videos........ 64
Support........ 65
Appendix A: Configuring the Standalone Utility Services template........ 66
Adding a new account to Communication Manager........ 66
Configuring MyPhone........ 67
Configuring Phone Firmware Manager........ 67
Important elements of the 46xxsettings.txt file........ 68
Appendix B: Configuring Call Detail Recording on Communication Manager........ 69

Chapter 1: Introduction

Purpose

This document provides procedures for managing the features that are part of Avaya Aura® Utility Services. These features include: IP Phone Settings, Avaya Desktop Video Device (ADVD) Settings, IP Phone Firmware Management, Log Viewer, Call Detail Recording Tools, and Enhanced System Directory. The content of this document is applicable to Utility Services deployed in Full Functionality and Utility Services Only modes. For Utility Services deployed in Services Port Only mode, this document is not applicable.

The primary audience for this document is:

- Avaya field technicians
- Avaya partners
- Technical support personnel
- Solution architects
- Implementation engineers
- Support personnel
- Technical support representatives

Change History

Issue	Date	Summary of changes
3.0	March 2018	Updated the “Utility Services backup and restore” section.
2.0	May 2015	• Updated the “Purpose” section of this document. • Added section “Out of Band Management”. • Updated information about wep page access in the section “Utility Admin”. • Updated information about Utility Services MyPhone Administration web pages in the section “MyPhone Admin”.

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

Utility Services runs a number of applications that provide a complete single box solution.

From Utility Services Release 7.0, you can deploy Utility Services as a standalone OVA.

Out of Band Management

Out of Band Management is a physically and logically separate network connection. It connects to a customer's private IT management network and provides for secure management and administration of Avaya products.

From Utility Services Release 7.0.1, you can activate out-of-band management even after deployment.

Utility Services Release 7.0.1 and later support a full out of band management configuration. Therefore, you can deploy Utility Services with two IP addresses and split the user and management traffic to different Ethernet interfaces on different IP networks.

When Utility Services is set for out of band management, the following services are allocated for full or Utility Services-only mode:

Application	Interfaces for traffic
Phone firmware download	Public
Phone settings file	Public
Gateway firmware download	Public
DHCP Server	Public
Myphone User	Public
SSH	Out of Band Management / Services
Myphone Admin	Out of Band Management
CDR connection to CM	Out of Band Management
Main admin web pages	Out of Band Management / Services
Alarm source	Out of Band Management
SAL connection (SSH, HTTP)	Out of Band Management

When Utility Services is set for out of band management, the following services are allocated for services port-only mode:

Application	Interfaces for traffic
SSH	Out of Band Management / Services
Alarm source	Out of Band Management
SAL connection (SSH, HTTP)	Out of Band Management
Main admin web pages	Disabled
Phone firmware download	Disabled
Gateway firmware download	Disabled
Phone settings	Disabled
Gateway firmware download	Disabled
DHCP Server	Disabled
Myphone Server	Disabled
CDR connection to CM	Disabled
Myphone admin	Disabled

Note:

If a network is not mentioned for service when Out of Band Management is enabled, the service must be disabled on that interface.

Utility Admin

With Utility Services 7.0.1, the Utility Services Administration Web Pages are accessible on port 543.

The URL is https:// <Utility Services IP> :543/admin.html.

‘Utility Services IP’ is the Public IP address of Utility Services when OOBM is disabled. This is the OOBM IP address of Utility Services when OOBM is enabled.

With the Utility Admin page, you can configure and gain access to the following elements:

- Software Version: Displays the software versions of packages, operating system, IP telephone firmware, media module firmware, and gateway firmware that are active on Utility Services.
- Firewall Rules: Displays the IPv4 and IPv6 firewall rules of Utility Services.
- IP Phone file server: Supports the download of the IP telephone firmware and the settings files. The server also supports backing up and restoring of 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. ADVD Settings Editor provides enhanced validation to avoid wrong configurations.

- IP Phone Settings Editor: Provides a Web-based tool for configuring the IP telephone settings file. IP Phone Settings Editor provides enhanced validation to avoid wrong configurations.
- IP Phone firmware management: Supports the upload of the 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 Push Server Database.
- Log viewer: Provides access of the log files for the Utility Services applications.
- CDR tools: Provides a Call Detail Record (CDR) collection capability. The CDR tool collects the CDR records from Communication Manager and imports the records into the Utility Services database. The CDR tool also provides simple examples on using the CDR data in the database.

MyPhone Admin

With Utility Services 7.0.1, the Utility Services MyPhone Administration Web Pages are accessible on port 9443.

The URL is `https://<Utility Services IP>:9443/MyPhoneAdmin`.

‘Utility Services IP’ is the Public IP address of Utility Services when OOBM is disabled. This is the OOBM IP address of Utility Services when OOBM is enabled.

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

- MyPhone Feature Buttons: Enable or disables the features available to the MyPhone users.
- WML Links: Displays the default Wireless Markup Language (WML) page on the IP telephones. You can use this element to configure the default WML page.
- System Message: Configures the WML page. This element contains a block of text that is relevant to every IP telephone user.

MyPhone

With the MyPhone page, you can:

- Configure the IP telephones.
- Configure buttons, language settings, EC500, Enhanced Call forwarding, and other features.

- Configure the security codes and other parameters.

MyPhone User Guide

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

Deploying Utility Services

You can deploy Utility Services on the following:

- VMware

  For more information, see *Deploying Avaya Aura® Utility Services* guide.
- Appliance Virtualization Platform through Solution Deployment Manager (SDM)

  For more information, see *Deploying Avaya Aura® applications from System Manager*.

Audit Account Addition

Utility Services supports an auditor account. You can use the auditor account to view the configuration and log files on Utility Services. However, you cannot alter any configuration. During the time of installation, the default password for the auditor account is `audit01`. You can change the default password at any given instance by starting an SSH session to Utility Services.

IP Phone Firmware Removal

Utility Services no longer bundles the IP Phone firmware within the build. To ensure that Utility Services has the correct IP Phone firmware for the installation, you must download the latest version of the firmware from PLDS. You can download the latest IP Phone firmware to store on Utility Services at any time. The IP Phone firmware management features remain unchanged from the previous versions.

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 the following elements that are installed and are active on Utility Services:

- Packages
- Operating System
- IP telephone firmware
- Media module firmware
- Gateway firmware

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. **(Optional)** To send a ping without looking up symbolic names for host address, select the **Do not look up symbolic names for host addresses** check box.
4. **(Optional)** To send a ping directly to the host, select the **Bypass normal routing tables and send directly to a host** check box.
5. To ping the required endpoint and check the connectivity, and click **Execute Ping**.

IPv6 Ping Host

On the IPv6 Ping page, you can check the network connectivity between Utility Services and IPv6 hosts.

Pinging an IPv6 Host

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.
2. In the navigation pane, in the **Miscellaneous** section, click **IPv6 Ping Host**.

   The system displays the IPv6 page.
3. In the **Host Name Or IPv6 IP address** field, type the host name or the IPv6 IP address of the endpoint.
4. **(Optional)** To send a ping without looking up symbolic names for host address, select the **Do not look up symbolic names for host addresses** check box.
5. **(Optional)** To send a ping directly to the host, select the **Bypass normal routing tables and send directly to a host** check box.
6. Click **Execute Ping6** to ping the required endpoint, and check the connectivity.

Upload files

Use a web browser to upload a file to Utility Services. You can upload a single file or a zipped file. In both cases, the system transfers the file from the web browser session to the `/tmp` directory on Utility Services. Other applications can use this directory as a temporary store for files.

Uploading telephone firmware to Utility Services

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.
2. In the navigation pane, in the **Miscellaneous** section, click **Upload Files**.

   The system displays the Upload File page.
3. Click **Browse**, and select the file that you want to upload.
4. Click **Upload File**.

Utility Services backup and restore

Use the Utility Services backup and restore functionality to back up and restore Utility Services. You must perform the Utility Services backup and restore separately from the backup and restore capability of System Platform.

Ensure that the type of Utility Services virtual machine deployment on which the restore is executed must be similar to the type of Utility Services virtual machine deployment on which the backup was taken.

You can include or exclude the IP telephone and gateway firmware in the backup file.

- **Include Firmware in Backup**: Use this option to create a complete backup file. As these backup files are large, the server takes longer duration to generate the files.
- **Exclude Firmware in Backup**: Use this option to create a backup file excluding the firmware. If you exclude the firmware, the backup process is faster. If you include the firmware in a backup file, the server always restores the firmware.

Note:

The firmware backup setting affects both the local and System Platform backups.

Creating a new Utility Services backup file

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **Miscellaneous** section, click **Utility Services Backup and Restore**.

   The system displays the Utility Services Backup and Restore page.

3. 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 Utility Services backup file.

4. Click the **Download the newly create Utility Services Backup File** link to save the ZIP file on the local system.

5. Click **Continue**.

Uploading and restoring the Utility Services backup file

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **Miscellaneous** section, click **Utility Services Backup and Restore**.

   The system displays the Utility Services Backup and Restore page.

3. Click **Browse** to navigate to the file you must upload.

4. 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 runs Utility Services. With the Customer Banner Control page, you can edit, enable, or disable the banner.

Controlling Customer Banner

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **Miscellaneous** section, click **Customer Banner**.

   The system displays the Customer Banner Control page.

3. Click one of the following:

   - **Enable Customer Banner**
   - **Disable Customer Banner**

- **Update Customer Banner**

Customer Banner Control button descriptions

Name	Description
Enable Customer Banner	Use this button to activate the customer banner.
Disable Customer Banner	Use this button to deactivate the customer banner.
Update Customer Banner	Use this button to make changes to the customer banner.

NTP Status

The **NTP Status** displays the status of the Network Time Protocol Infrastructure page including Daemon Status, Synchronization Status, and NTP System Status.

RFA License Activation

RFA License Activation enables a previously uploaded Avaya Authentication File to be activated on Utility Services.

Firewall Rules

Firewall IPv4

The system displays the IPv4 firewall rules of Utility Services on the Firewall IPv4 page. You cannot edit or configure the firewall rules.

Firewall IPv6

The system displays the IPv6 Firewall rules of Utility Services on the Firewall IPv6 page. You cannot edit or configure the firewall rules.

Viewing firewall rules

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

The system displays the Utility Server Administration page.

2. In the navigation pane, in the **Firewall Rules** section, click one of the following:
   - **Firewall (IPv4)**
   - **Firewall (IPv6)**

IP Phone Tools

ADVD Settings Editor

Use ADVD Settings Editor to configure the settings for Avaya A175 Desktop Video Device (ADVD). ADVD uses the Axxxsettings.txt file to configure video-related settings such as the default Wireless Markup Language (WML) page and the options that users can gain access to from the handset. With ADVD Settings Editor, you can edit the file along with the entry-checking and help files.

Configuring the view of the ADVD settings file

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **IP Phone Tools** section, click **ADVD Settings Editor**.

   The system displays the ADVD Settings Editor page.

3. Select the **Display file comments** check box to display the comments 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.

4. Select the **Display only active options** check box to display only the active settings on ADVD.

   The other options remain in the Axxxsettings file, but the system does not display the options.

   Note:

   Comment lines begin with two pound keys (##). Active lines begin with SET command. Lines within the file that start with two pound keys (##) or SET are inactive. As ADVD Settings Editor processes only the values in uppercase, you must use uppercase for SET and parameter names in the file.

Editing the ADVD settings file

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **IP Phone Tools** section, click **ADVD Settings Editor**.

   The system displays the ADVD Settings Editor page.

3. Perform one of the following steps to select a settings file to edit:

   - Download the `Axxxsettings.txt` file from the Utility Services. SIP and H.323 videos use the same `Axxxsettings.txt` file.

     Note:

     You can edit the URL address to download the file from a different HTTP source. If you have a different file server in the network, then enter the URL for the `Axxxsettings.txt` on that server. The system downloads the `Axxxsettings.txt` file for editing. However, the system cannot save the file on the remote server. You must download the edited `Axxxsettings.txt` file from the server, 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 click **Browse**.

     The `ADVDParameterDefinitions.xml` file contains help and entry information for the editor. Utility Services includes the latest version of the `ADVDParameterDefinitions.xml` file. The latest version of the Axxxsettings.txt file is available on the Avaya Support website.

     Note:

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

4. 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**.

5. Perform one of the following steps as required:

   - Performing basic ADVD settings editing on page 21
   - Checking the ADVD settings syntax on page 21
   - Performing advanced ADVD settings editing on page 21

Performing basic ADVD settings editing

Procedure

1. On the ADVD Settings Editor page, perform one of the following steps:
    - Select the check box in the **Activate** column to activate a setting in the file.

      The system displays the value within the file and ADVD uses that value.

      When you clear a check box in the **Activate** column, the system deactivates the setting in the file.
    - Modify the value of the setting in the text box.
2. Click **Commit** to save the changes.

Checking the ADVD settings syntax

Procedure

On the ADVD Settings Editor page, perform one or more of the following steps:

- Correctly specify the settings with orange border.

  The system displays a setting with orange border if the setting is not found in the xml file in the system and if the setting is invalid.
- Click a settings value to see the detailed information about the problem and correct the value.

  The system displays a setting with red border if the setting is incorrect and the ADVD cannot process the settings.

Performing advanced ADVD settings editing

Procedure

On the ADVD Settings Editor page, 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 have 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 available ADVD options in alphabetical order. The system displays the existing lines in the file above and below **Add Line**. Select the required option and enter an appropriate value in the text box. Click **Add Line**. The system adds the line below the current line.
- To add a comment, go to the statement, 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 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 minus (**-**) sign.

  If you accidentally delete a line, you can reload the original settings file by clicking **ADVD Settings Editor** in the navigation pane.

Saving ADVD settings

Procedure

1. After making the changes to the ADVD settings file, click **Save New Settings File**.

   The system displays the Output Screen page.

2. Perform one of the following steps:

   - Click **Save Axxxsettings.txt file to this server** to save the file in Utility Services.
   - Click the **Axxxsettings.txt(comments included in file)** link or the **Axxxsettings.txt(no comments)** link to download the file to your computer.

ADVD Setting Editor field descriptions

Name	Description
Activate	Displays whether the setting is active or inactive. Select the check box to show that the setting is active and ADVD can read the setting. Clear the check box to signify that the setting is inactive and the ADVD does not read the settings. The system displays the inactive setting as commented out in the settings file.
Parameter	Displays comments and settings values. Comments span both the columns, and you can edit the comments by 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 by 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.
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.

Button	Description
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 the display of the IP Phone settings file

Procedure

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

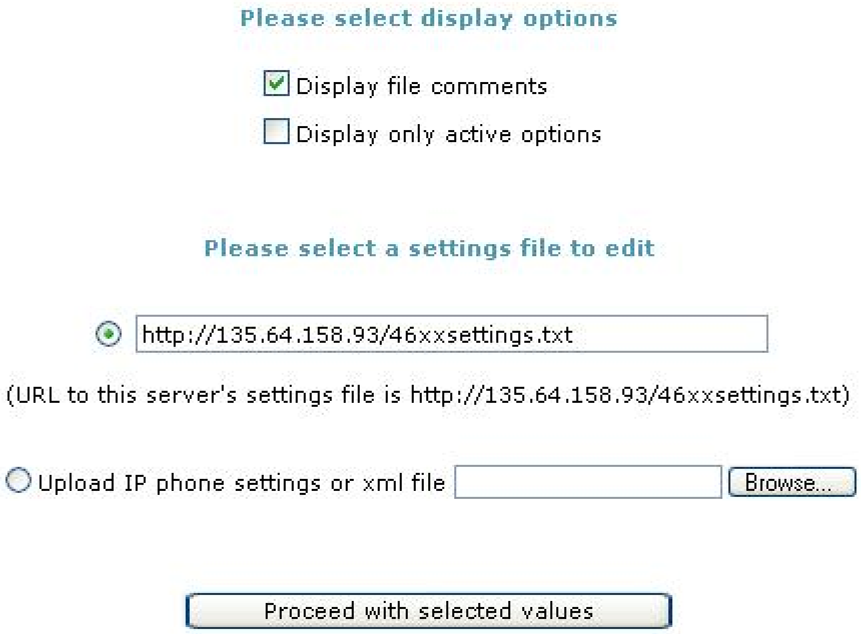
   The system displays the IP Phone Settings Editor page.

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.



Please select display options

☑ Display file comments

□ Display only active options

Please select a settings file to edit

● http://135.64.158.93/46xxsettings.txt

(URL to this server's settings file is http://135.64.158.93/46xxsettings.txt)

○ Upload IP phone settings or xml 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 25
    - 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 minus 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.
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, click **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 including site-specific files such as Custom Screen Saver images to Utility Services by using the IP Phone Custom File Upload page. You can upload a single file or a ZIP file. The files are immediately available, and the system overwrites the existing files.

Viewing a custom file

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.
2. In the navigation pane, in the **IP Phone Tools** section, click **IP Phone Custom File Upload**.

   The system displays the IP Phone Custom File Upload page.

3. Click **Display Custom Directory**.

   The system displays the custom files.

Uploading and activating the custom file

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.
2. In the navigation pane, in the **IP Phone Tools** section, click **IP Phone Custom File Upload**.

   The system displays the IP Phone Custom File Upload page.
3. Click **Browse**, and select the file that you must upload.
4. 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	The Communication Manager IP address.
User Name	The user name. ❗ **Important:** You must configure the user name and the password in Communication Manager. The user name must have bash shell privilege. For the `dadmin` user who does not have the bash shell privileges, the system displays the `Connection to Call Server failed!` message.
Password	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 28.

About this task

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

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **IP Phone Firmware Manager** section, click **Display Stations**.

   Note:

   The system might take some time to display the telephone information the first time that you perform the procedure but takes less time for subsequent displays. The system takes more time to display the results for larger systems than results for smaller systems.

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

Table continues…

Name	Description
	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 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 the 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 the Phone Firmware Manager - Display Latest Firmware page after a reset.

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **IP Phone Firmware Manager** section, click **Display Server Firmware**.

   On the Phone Firmware Manager - Display Latest Firmware page, the system displays 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 the endpoint firmware from Utility Services.

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **IP Phone Firmware Manager** section, click **Manage Phone Firmware**.

   The system displays the Manage Firmware page.

3. Select the firmware package.
4. Click one of the following:
   - **View**
   - **Unpack**
   - **Activate**
   - **Deactivate**
   - **Remove**
   - **Forcibly Unpack**

Manage Firmware button descriptions

Name	Description
View	Displays the information of the selected firmware package.
Unpack	Unpacks each package of the phone firmware separately and extracts files from the ZIP archive.
Activate	Activates the selected firmware package, and makes the firmware package available to Utility Services.
Deactivate	Deactivates the selected firmware package and removes the firmware from the Web server.
Remove	Deletes the extracted files and the ZIP archive.
Forcibly Unpack	When the **Unpack** option does not function, use the **Forcibly Unpack** option to forcibly unpack each package of the phone firmware separately and extract files from 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 28.

About this task

Use this procedure to select an IP telephone to reset and specify the period for reset. You can also configure the system to reset the telephone if the telephone fails to upgrade or if you do not want to reset the telephone that is active on a call.

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.
2. In the navigation pane, in the **IP Phone Firmware Manager** section, click **Schedule Phone File Download**.

   The system displays the Phone Firmware Manager – Schedule Control page.
3. Select the options, 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 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.

Note:

A DHCP scope must be defined for the subnet of the public interface of Avaya Aura® Utility Services. Otherwise, activation of DHCP will fail.

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.
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. In the left navigation pane, click **DHCP Server Log**.
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 **DHCP Server Status** option to check whether the IPv6 DHCP server is running.

Viewing the IPv6 DHCP Server status

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **IPv6 DHCP Manager** section, click **IPv6 DHCP Server Status**.

   The system displays the status of the IPv6 DHCP service.

Activate/Deactivate IPv6 DHCP

Use the **Activate/Deactivate DHCP** option to start or stop the IPv6 DHCP server that uses Utility Services. When you start the server, the system displays a status message from Utility Services. An IPv6 DHCP server in a running state indicates that the `dhcpd.conf` file is correctly created. An IPv6 DHCP server that is not in the running state indicates a problem in the `dhcpd.conf` file, and the system displays an error message about the problem.

DHCP Service Control button descriptions

Name	Description
Activate DHCP Server	Starts the DHCP server. The system displays **RUNNING** to indicate the active state.
Deactivate DHCP Server	Stops IPv6 DHCP server. The system displays **STOPPED** to indicate the deactivated state.
Load last working DHCPD conf file	Loads the DHCPD file containing the settings that you used to run the DHCP server the last time.

Activating and deactivating an IPv6 DHCP server

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **IPv6 DHCP Manager** section, click **Activate/Deactivate IPv6 DHCP**.

   The system displays the status of the IPv6 DHCP server on the IPv6 DHCP Service Control page.

3. Click one of the following:

   - **Activate DHCP Server**
   - **Deactivate DHCP Sever**
   - **Load last working 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	Type a valid IPv6 address without prefix.
DHCP v6 Stop Address	Type a valid IPv6 address without prefix.
DHCP v6 Prefix Address	Type the prefix address that is identical to the start and stop addresses.

Updating DHCP IPv6 values

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **IPv6 DHCP Manager** section, click **IPv6 DHCP IP Address Pools**.

   The system displays the IPv6 DHCP Server IP Address Pools page.

3. 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 when pools are used.

IPv6 DHCP Leases Display field descriptions

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

Table continues…

Name	Description
Binding State	The status of an IPv6 address. The available options are: • **Active**: The endpoint is using the IPv6 address. • **Free**: The endpoint has returned the IPv6 address to the pool.
MAC Address	IPv6 addresses of a particular computer or a laptop. MAC address is used for physical identification of a particular Ethernet code.

Viewing DHCP lease information

Procedure

1. On the Utility Services Web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **IPv6 DHCP Manager** section, click **Show IPv6 DHCP Lease**.

   The system displays the following information on the IPv6 DHCP Leases Display page:

   - The range of IP ports available.
   - The number of IP ports in use.
   - The percentage of IP ports in use.
   - The last usage duration of the IP ports.
   - The binding states of the IP ports.

IPv6 DHCP Sever Log

Use the IPv6 DHCP Sever Log page to view the server logs. You can use the information to troubleshoot DHCP-related problems.

Viewing the IPv6 DHCP log files

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **IPv6 DHCP Manager** section, click **IPv6 DHCP Server Log**.

   The system displays the View IPv6 DHCP Log Files page.

3. Click **View Log**.

   The system displays the DHCP log files.

Gateway Firmware

Upload Gateway Firmware

The Upload Gateway Firmware page enables Utility Services to support Trivial File Transfer Protocol (TFTP) access for Media Module and Gateway Firmware. Use the Upload Gateway Firmware page to view the firmware file and upload a new firmware file on Utility Services.

Viewing Gateway Firmware

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **Gateway Firmware** section, click **Upload Gateway Firmware**.

   The system displays the Upload Gateway Firmware page.

3. Click **Display Firmware Directory**.

   The system displays the information about the gateway firmware.

Uploading Gateway Firmware

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **Gateway Firmware** section, click **Upload Gateway Firmware**.

   The system displays the Upload Gateway Firmware page.

3. Click **Browse**, and navigate to the file you must upload.

4. Click **Upload Gateway Firmware and Activate**.

IP Phone Push Server

Display Push Database

Avaya IP deskphones support the Push mechanism. The deskphones 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. The Display Push Database page displays the content from the Push server and database. To use the Push functionality, all deskphones must be registered with Utility Services.

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

You must register the deskphones to receive Push messages. As deskphones remain registered even after logoff, you must age the registrations and set a resubscription process at required intervals.

Table 1: Display Push Database button descriptions

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

Test Push Database

Use the Test Push Database page to:

- Diagnose and test the Push capability of Utility Services. You can push the content from the applications to the registered deskphones.
- Allow each mode and type of the Push message to be sent to a single device, several devices, or all devices simultaneously.

Sending Push messages

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **IP Phone Push Server** section, click **Test Push Server**.

The system displays the IP Phone Push Server - Test Push Server page.

3. Perform one of the following steps:
   a. Click **Select All Extensions** to select all the extensions.
   b. Click **Select No Extensions** to deselect all the extensions.
4. Select the type of PUSH message: **Topline** or **Display**.
5. Select the number of alert tones: **Silent**, **One Beep**, **Two Beeps**, or **Three Beeps**.
6. Select the priority of PUSH message: **Normal** or **Barge**.
7. In the **PUSH Message to be sent** field, type the message.
8. 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 and the log files, such as Messages Server Access Log and View Archive Log.
- Zip the archived log files, download, and save the log files on your local drive.
- Download the historical data to diagnose the system.

Viewing Linux Messages log files

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.
2. In the navigation pane, in the **Application Log View** section, click **Messages**.

   The system displays the View Linux Messages Log Files page.
3. Click **View Log** to view a log file.
4. Click **Download Messages Log** to download the log file.

Phone Firmware Manager

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

Viewing the Phone Firmware Manager Server log files

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **Application Log View** section, click **Phone Firmware Manager**.

   The system displays the View Phone Firmware Manager Server Log Files page.

3. Click **View Log** to view a log file.
4. Click **Download PFM Server Access Log** to download the log file.

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 archived log files.

Viewing the TFTP server access log

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.
2. In the navigation pane, in the **Application Log View** section, click **TFTP Server**.
3. Click **View Log**.

   The system displays the View TFTP Server Log Files page.

Viewing the archived log files

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.
2. In the navigation pane, in the **Application Log View** section, click **TFTP Server**.
3. Click **View Log**.

   The system displays the 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	The user name of Communication Manager.
CM Password	The password of Communication Manager.

IP Phone Firmware Manager

You can use the IP Phone Firmware Manager option to:

- View the current status of the Phone Firmware Manager (PFM) server.
- Check whether the PFM server restarts automatically on a restart.
- Start or stop the server immediately or configure the operation of the PFM server after a restart.
- Check whether the PFM server is running or not. To indicate the active state of the PFM server, the system displays **RUNNING** on the Control Phone Firmware Manager (PFM) Server page.

Controlling the Phone Firmware Manager server

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **Application Control** section, click **Phone Firmware Manager**.

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

3. Click one of the following:
    - **Start the PFM Server**
    - **Stop the PFM Server**
4. Click one of the following:
    - **Enable Autostart of the PFM Server**
    - **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 restart.
Disable Autostart of the PFM Server	Disables auto start of the PFM server after a restart.

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.
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 use the Control TFTP Server page to:

- View the current status of the TFTP server and whether the server will automatically restart.
- Start or stop the server.
- Configure the operation of the server after a restart.

Controlling the TFTP server

Procedure

1. On the Utility Services web interface, click **Utilities** > **Utility Admin**.

   The system displays the Utility Server Administration page.

2. In the navigation pane, in the **Application Control** section, click **TFTP Server**.

On the Control TFTP Server page, the system displays the current status of the TFTP server.

3. Click one of the following:
    - **Start the TFTP Server**
    - **Stop the TFTP Server**
4. Click one of the following:
    - **Enable Autostart of the TFTP Server**
    - **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 restart.
Disable Autostart of the TFTP Server	Disables auto start of the TFTP server after a restart.

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.
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

With the Directory Application feature, you can search an LDAP database by using browsers that are compatible with the 46xx and the 96xx deskphones. You can use the Web pages to configure the Directory Application feature to connect to the LDAP database and to customize user search. The Directory Application feature supports 250 instances of the directory configuration and provides multilingual support for the instances.

For a more information about 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 feature

About this task

To enable the Wireless Markup Language (WML) browsers to perform search operations, you must configure the Directory Application feature.

Procedure

1. On the Utility Services web interface, click **Administration** > **Directory Application**.

   The system displays the Directory Application Administration page.
2. In the navigation pane, click **General Settings**.
3. Specify the LDAP connection settings.
4. Click **Test Connection** to ensure that the Directory application connects to the LDAP database.
5. In the General Administration section, select **Enable** on the **HTTP** or the **HTTPS** field.
6. **(Optional)** Use the Search Screen Settings screen to customize the Search screen of the deskphone.
7. **(Optional)** Use the Details Screen Settings screen to customize the Details screen of the deskphone.
8. **(Optional)** Use the Ldap Filter Settings screen to customize the LDAP filter attributes.

Configuring the deskphones

Procedure

On the deskphone, set the **HTTP** or the **HTTPS** field to connect Utility Services through DHCP or the `46xxsettings.txt` file.

Utility Services includes a `46xxsettings.txt` file. The WMLHOME parameter in the file is set to display a landing page that includes three WML applications: Directory Application, User entered URL, and Message Application.

General Settings

Use the General Settings page to administer the general settings and the LDAP connection settings of the Directory Application feature.

Administering the General Administration section

Procedure

1. On the Utility Services web interface, click **Administration** > **Directory Application**.

   The system displays the Directory Application Administration page.

2. In the navigation pane, click **General Settings**.
3. In the **Directory number** field, select a directory number from **1** to **250**.

   The system configures the Directory Application feature for the particular directory number and applies the directory number to the General Settings page, the Translation Language page, and the External Numbers page.

4. In the **Application title** field, type an application title that the Search screen of the deskphone browser must display.
5. In the **HTTP** field, select **Enable** to enable the HTTP traffic.

   The directory application can accept traffic from the WML browsers that use the HTTP protocol.

   ⚠ **Warning:**

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

6. In the **HTTPS** field, select **Enable** to enable the HTTPS traffic.

The Directory application can accept traffic from the WML browsers that use the HTTPS protocol.

7. In the **Select a language file** field, select a language file where you can write the translation.
8. In the **Select language for your translation** field, select a language for the translation.

Administering the LDAP Administration section

Procedure

1. On the Utility Services web interface, click **Administration** > **Directory Application**.

   The system displays the Directory Application Administration page.
2. In the navigation pane, click **General Settings**.
3. In the **Host Name** field, type the host name or IP address of the LDAP server.

   The directory application connects to the LDAP server for searching the database.
4. In the **Port** field, type the port number of the LDAP server.

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

   Note:

   Ensure that firewall is enabled for the port. You must open the port only for outbound traffic.
5. In the **Base DN (Search Root)** field, type an LDAP name from where the Directory application can begin searching.
6. In the **Base DN (External Search Root)** field, type an LDAP base name where the external numbers are stored.

   You can use the root to list, add, or delete entries in the external directory on the Manage External Numbers screen. For the directory application to include external names in the search, the name must be under Search Root. For example, if Search Root is o=avaya.com, then External Search Root can be ou=external numbers, o=avaya.com.
7. In the **Max number of hits** field, type the maximum number of results that the system must return 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.
8. In the **User ID** field, type 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 by using the Manage External Numbers screen, you must give write access to the specified user.

9. In the **Password** field, type a password for the User ID that you specified for the LDAP server.
10. In the **Search Time** field, type the maximum number of seconds for the search operation before returning the results.

    The system stops the search operation when the operation exceeds the time.

    The default value is **10**.
11. In the **Secure Connection (TLS support)** field, select **On** or **Off**.

    The directory application can connect to an LDAP server on TCP or TLS. If you select TLS, you must perform additional configuration. For more information, see *TLS Configuration*.
12. Click **Test Connection** to ensure that the directory application can connect to the LDAP server by using the connection parameters you have specified.

Administering the Search Screen settings section

About this task

You can customize the search or the home page of the Directory application to allow users to search for particular LDAP attributes. The telephone displays each search attribute on a separate line. You can configure the settings for each line.

Procedure

1. On the Utility Services web interface, click **Administration** > **Directory Application**.

   The system displays the Directory Application Administration page.
2. In the navigation pane, click **General Settings**.
3. In the **Search Attribute** field, you can select from the list of available LDAP attributes or choose a new attribute.

   For example, the LDAP attribute for Name can be cn or cn;lang-en. The second attribute must be a telephone number or any attribute associated with the telephone number.

   Note:

   A valid LDAP attribute name can contain an alphabetic character, a number, and the minus sign (-) and colon (;). However, the attribute name must begin with a letter.
4. In the **Associated Label** field, type a label for each search attribute that is activated.

   The label supports Unicode and the telephone Search screen displays the label.
5. In the **Minimum Search String** field, type the minimum number of characters required for a search string.

The directory application denies a search operation with a search string containing less than the minimum number of characters required.

Administering the Detail Screen settings section

Procedure

1. On the Utility Services web interface, click **Administration** > **Directory Application**.

   The system displays the Directory Application Administration page.

2. In the navigation pane, click **General Settings**.
3. In the **Search Attribute** field, you can select from the list of available LDAP attributes or choose a new attribute.

   For example, the LDAP attribute for Name can be cn or cn;lang-en. A second attribute must be a telephone number or any attribute associated with the telephone number.

   Note:

   A valid LDAP attribute name can contain an alphabetic character, a number, and the minus sign (-) and colon (;). However, the attribute name must begin with a letter.

4. In the **Associated Label** field, type a label that the system must display before the actual value on the Detail screen.

Administering the LDAP Filter Settings section

Procedure

1. On the Utility Services web interface, click **Administration** > **Directory Application**.

   The system displays the Directory Application Administration page.

2. In the navigation pane, click **General Settings**.
3. In the **Filter Attribute** field, you can select from the list of available LDAP attributes or choose a new attribute.

   For example, the LDAP attribute for Name can be cn or cn;lang-en. A second attribute must be a telephone number or any attribute associated with the telephone number.

   Note:

   A valid LDAP attribute name can be an alphabet, a number, and the minus sign (-) and colon (;). However, the attribute name must begin with an alphabet.

4. In the **Filter Text** field, type the label that the system must use in the LDAP search filter for the associated filter attribute.

Translation Language

Use the Language Translation Settings screen for the translation language that you selected on 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 the English text mapping with English translations. In either of the 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

The user can edit the value in the **Translation** column of each English string.

External Numbers

Use the External Numbers Administration screen to view entries in the External Number search root of the LDAP database, based on the specification in the General Settings screen. You can also perform the following operations:

- Add external numbers.
- Edit external numbers.
- Delete external numbers.

Adding a new external number in the LDAP database

Procedure

1. On the Utility Services web interface, click **Administration** > **Directory Application**.

   The system displays the Directory Application Administration page.
2. In the navigation pane, click **External Numbers**.

   The system displays the External Numbers Administration page.
3. Click **Add**.
4. In the **Native Name** field, type a Unicode name.
5. In the **Name** field, type an ASCII name.
6. In the **Phone Number** field, type a deskphone number.
7. In the **E-mail** field, type an email address.
8. Click **Save** to add the external number to the LDAP database.
9. Click **Refresh** to view your changes.

Editing an external number in the LDAP database

Procedure

1. On the Utility Services web interface, click **Administration** > **Directory Application**.

   The system displays the Directory Application Administration page.
2. In the navigation pane, click **External Numbers**.
3. Select an entry.
4. Click **Edit**.
5. Modify the details of the selected entry.

   Note:

   You can modify only one entry at a time. You cannot modify the value of the **Native Name** field.
6. Click **Save** to save your changes to the LDAP database.
7. Click **Refresh** to view your changes.

Deleting an external number from the LDAP database

Procedure

1. On the Utility Services web interface, click **Administration** > **Directory Application**.

   The system displays the Directory Application Administration page.

2. In the navigation pane, click **External Numbers**.

   The system displays the External Numbers Administration page.

3. Select an entry.

   You can select multiple entries at a time.

4. Click **Delete**.
5. Click **Delete** to confirm your action.
6. Click **Refresh** to view your changes.

Chapter 5: 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	*Deploying 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
03-602578	*Avaya Communication Manager Express MyPhone Administration Reference*	This document describes the features available to the administrators of the MyPhone feature for Avaya Communication Manager Express (CME).	Solution architects, Implementation engineers, Support personnel, Technical support representatives, Authorized Business Partners

Related links

Finding documents on the Avaya Support website on page 63

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

Related links

Documentation on page 62

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
Understanding	
1A00234E	Avaya Aura® Fundamental Technology
AVA00383WEN	Avaya Aura® Communication Manager Overview
ATI01672VEN, AVA00832WEN, AVA00832VEN	Avaya Aura® Communication Manager Fundamentals
2007V	What is New in Avaya Aura® 7.0
2009V	What is New in Avaya Aura® Communication Manager 7.0

Table continues…

Course code	Course title
2011V	What is New in Avaya Aura® System Manager & Avaya Aura® Session Manager 7.0
2009T	What is New in Avaya Aura® Communication Manager 7.0 Online Test
2013V	Avaya Aura® 7.0 Solution Management
5U00060E	Knowledge Access: ACSS - Avaya Aura® Communication Manager and CM Messaging Embedded Support (6 months)
Implementation and Upgrading	
4U00030E	Avaya Aura® Communication Manager and CM Messaging Implementation
ATC00838VEN	Avaya Media Servers and Implementation Workshop Labs
AVA00838H00	Avaya Media Servers and Media Gateways Implementation Workshop
ATC00838VEN	Avaya Media Servers and Gateways Implementation Workshop Labs
2012V	Migrating and Upgrading to Avaya Aura® 7.0
Administration	
AVA00279WEN	Communication Manager - Configuring Basic Features
AVA00836H00	Communication Manager Basic Administration
AVA00835WEN	Avaya Communication Manager Trunk and Routing Administration
5U0041I	Avaya Aura® Communication Manager Administration
AVA00833WEN	Avaya Communication Manager - Call Permissions
AVA00834WEN	Avaya Communication Manager - System Features and Administration
5U00051E	Knowledge Access: Avaya Aura® Communication Manager Administration

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to 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 website.

  ✱ **Note:**

  Videos are not available for all products.

Support

Go to 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.

Appendix A: Configuring the Standalone Utility Services template

Adding a new account to Communication Manager

About this task

Use the following procedure to manually add a new account to Communication Manager for installations that use a Post-Install wizard and automatic addition of a MyPhone account on the server SMI.

Procedure

1. Open a web session to Communication Manager (SMI) and select **Administration** > **Server (Maintenance)**.
2. In the left navigation pane, select **Security** > **Administrator Accounts**.
3. On the Administrator Accounts page, select **Add Login** with an account type **Unprivileged Administrator** and click **Submit**.
4. On the Administrator Accounts -- Add Login: Unprivileged Administrator page, complete the following:
    a. Enter the **Login name**.

       By default the **Login name** is `MyPhone`.

    b. For **Additional groups (profile)**, ensure **prof26** is selected.

    c. For **Select type of authentication**, ensure **Password** is selected.

    d. Enter your password in the **Enter password or key** field.

    e. Re enter your password in the **Re-enter password or key** field.

    f. For **Force password/key change on next login**, ensure **No** is selected.

    g. Click **Submit**.

Configuring MyPhone

About this task

You can configure MyPhone by using the MyPhone Admin application on Utility Services. The MyPhone Admin application has the help files that Utility Services provides in both HTML and PDF formats.

Procedure

1. Type the IP address of Utility Services in the web browser, and press `Enter`.
2. Click **Utilities** > **MyPhone Admin**.
3. Log on the Utility Services web interface by using the administrator credentials.
4. Click **MyPhone AES, CM, and SES Access** to gain access to Communication Manager.

   MyPhone is the default account. Installations that use the Post-Install wizards configure the Communication Manager account with minimal permissions.
5. Click **Test** to verify connectivity before you save the configuration.

Configuring Phone Firmware Manager

About this task

Phone Firmware Manager (PFM) requires access to Communication Manager to perform status inquiries and to schedule firmware upgrades. The Communication Manager account must have SAT access, and you can use the same account that you used for MyPhone.

Procedure

1. Log on to the Utility Services web interface.
2. Click **Utilities** > **Utility Admin**.
3. In the navigation pane, in the **IP Phone Firmware Manager** section, click **Configure CM Login**.

   The system displays the Phone Firmware Manager - Config CM Login page.
4. You can configure the following parameters:
   - IP address of Communication Manager
   - User name
   - Password
5. Click **Test** to verify connectivity before you save the configuration.

Important elements of the 46xxsettings.txt file

The Post-Install wizard configures the 46xxsettings.txt file when you install the template, but you can edit or replace the file after the installation is complete. You can configure the following elements: **IP Phone Backup and Restore**, **PUSH**, and **WML Home Page**.

Note:

While configuring the elements, replace < IP > in the command with the Utility Services IP address.

- **IP Phone Backup and Restore**: Utility Services functions as an IP Phone Backup and Restore server. You can configure HTTP or HTTPS and the PhoneBackup subdirectory. Utility Services allows only Avaya IP deskphones to read and write to the directory. To configure the **IP Phone Backup and Restore** element, type the following command in the configuration file: **`SET BRURI http://<IP>/PhoneBackup or https://<IP>/PhoneBackup`**.
- **PUSH**: By default, Utility Services functions both as a Push Registration server and a Trusted Push server. To configure the **PUSH** element, type the following commands in the configuration file:
    1. **`SET TPSLIST <IP>`**
    2. **`SET SUBSCRIBELIST http://<IP>/push/subscribe.php`**
- **WML Home Page**: Utility Services provides a default WML home page. To configure the **WML Home Page** element, type the following command in the configuration file: **`SET WMLHOME http://<IP>/landing.wml`**.
- **ESD Landing Pages**: Utility Services provides access to the Enterprise System Directory application. To gain the full configuration access, type the following command at the end of the configuration file: **`GET ESD_Landing.txt`**.

Appendix B: Configuring Call Detail Recording on Communication Manager

About this task

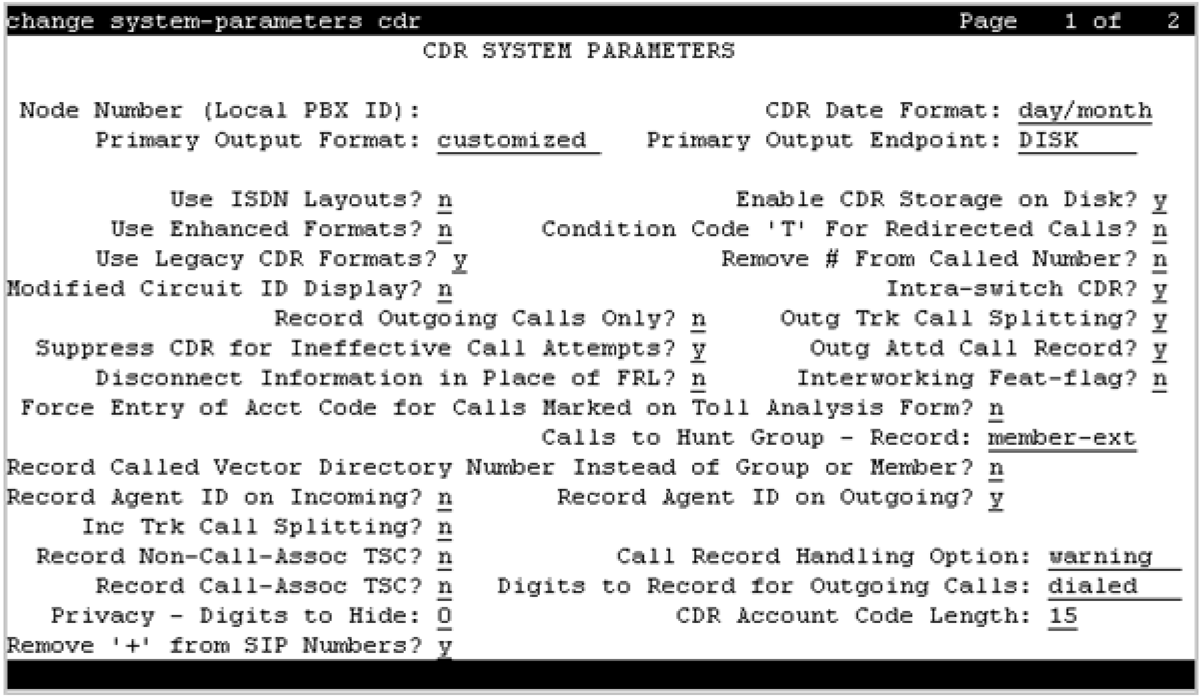
To operate correctly, Call Detail Recording requires a specific configuration on Communication Manager. Most of the Post-Install wizards configure Communication Manager automatically for operation with Utility Services, but this is not possible when Utility Services is collecting Call Detail Record (CDR) data from an existing system. For Call Detail Recording to operate correctly, perform the following procedure.

Procedure

1. Create a new user of the CDR_User type on Communication Manager.

   The CDR_User type has the required privileges to gain access to the CDR data.

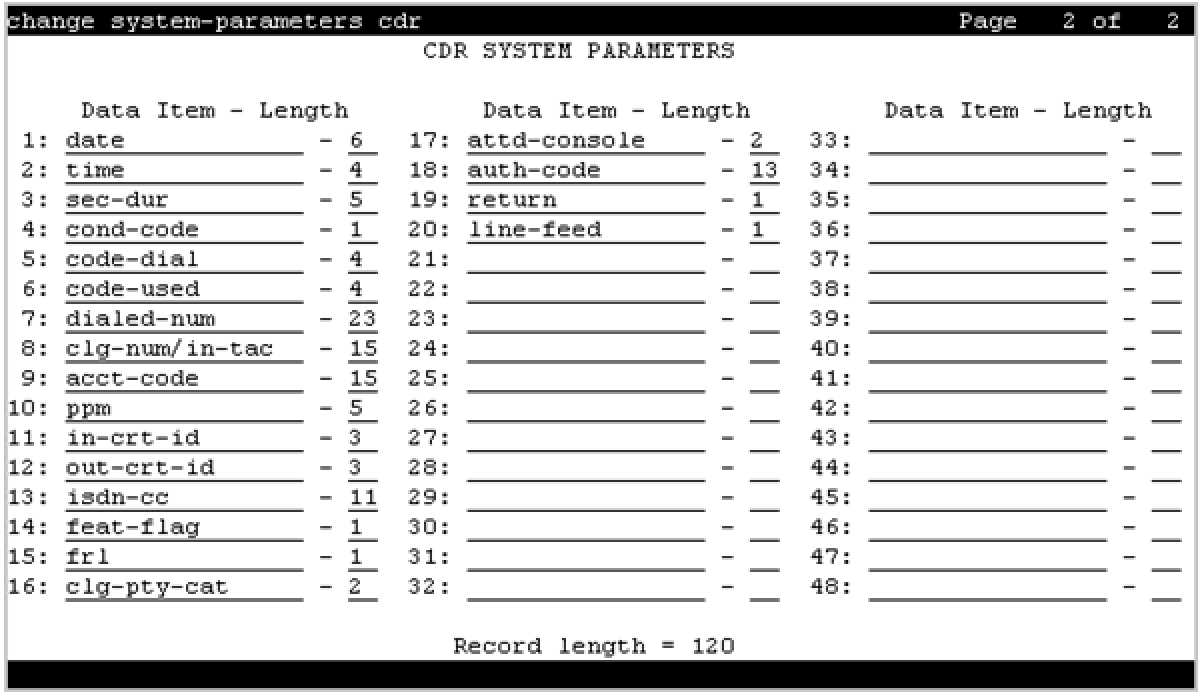
2. Configure the CDR format.



```
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 **Call Detail Recording** > **Application Control**.
5. Type the user name and the password that you administered earlier.
6. Click **Enable Password Mode** to update the configuration.

Note:

By default, the system disables the CDR daemons. You must enable the CDR daemons as required. You must start and stop the CDR collector to apply any changes in configuration. If you update the details of Communication Manager before you enable the CDR daemon, you must only start the CDR collector to apply the changes.

Index

Numerics

46xxsettings.txt 23, 24, 55

A

accessing CDR backup files 52
activate IPv6 DHCP 38
activating and deactivating DHCP server 35
add a subnet 35
Adding a new account 66
advanced ADVD settings editing 21
ADVD 19
ADVD Setting Editor
    field descriptions 22
ADVD settings
    configuring view of settings file 19
ADVD Settings Editor 11, 19
    advanced ADVD settings editing 21
    basic editing 21
    checking syntax 21
    configuring view 19
    editing ADVD settings file 20
    saving ADVD settings 22
ADVD settings file 20
    editing 20
ADVD settings syntax 21
Application Control
    controlling phone firmware manager server 48
    controlling system database 49
    controlling TFTP server 50
    control phone firmware manager server button descriptions 49
    control TFTP server button descriptions 51
    phone firmware manager 48
    TFTP server 50
Application Log View
    Messages 44
    Phone Firmware Manager 44
    Viewing PFM Server log files 45
archive log files 46
Audit Account Addition 13
Avaya courses 63
Avaya Desktop Video Device 19
Axxxsettings.txt 19, 20

B

backup 16
back up and restore 27
backup file 16
basic ADVD settings editing 21
button descriptions
    control phone firmware manager server 49
    Control TFTP Server 51

C

Call Detail Record
    CDR log files 44
call detail recording 44, 47
Call Detail Recording 48, 69
Call Detail Records Collector 44
catalina.out 46
CDR 44, 47, 48, 69
CDR archive 52
CDR backup 52
CDR backup files 52
CDR e-mail 52
CDR e-mail button descriptions 53
CDR e-mail field descriptions 53
CDR export daemon 52
CDR report 51
CDR reports 51
CDR tools 11
Change History 8
CM login button descriptions 29
Common
    software version 14
Communication Manager 28, 44, 51, 52
Communication Manager login
    configuring in Utility Services 28
Configure CM login 28
Configure CM Login
    field descriptions 29
configuring DHCP IP address pools 35
configuring the telephones 55
Control CDR Servers
    field descriptions 48
controlling CDR Servers 48
controlling customer banner 17
controlling MyPhone server 50
controlling phone firmware manager server 48
controlling TFTP server 50
control MyPhone server button descriptions 50
control phone firmware manager server button descriptions 49
control system database button descriptions 49
control TFTP server button descriptions 51
Control Web Server button descriptions 47
CSV file 52
customer banner 17
Customer Banner Control 17
    button descriptions 18

D

deactivate IPv6 DHCP 38
deploying utility services
  SDM 13
  VMware 13
Detail Screen settings 58
DHCP 34
DHCP:activate 34
DHCP:deactivate 34
DHCP IP address 35
DHCP lease 36
DHCP leases display field descriptions 37
DHCP server 11
DHCP server log 37
DHCP server status 34
DHCP service control button descriptions 35
DHCP v6 Prefix Address 39
DHCP v6 Start Address 39
DHCP v6 Stop Address 39
Directory Application 54
  configuring 54
  External Numbers 59
  General Settings 55
  Translation Language 59
Directory Application Administration 54
Disable Customer Banner 17
Display Push Database 42
Display server firmware 31
display stations 29
display stations field descriptions 30
Dynamic Host Configuration Protocol 34

E

editing DHCP subnets 36
e-mail daemon 52
Enable Customer Banner 17
Exclude Firmware in Backup 16
External Numbers
  adding external number 60
  deleting external number 61
  editing external number 60

F

field descriptions
  ADVD Setting Editor 22
  Configure CM Login 29
file server log 43
file server log files 43
file server status 46, 47
firewall
  IPv4 18
  IPv6 18
firewall rules 18
Firewall Rules 11
firmware
  managing 31
  uploading to Utility Services 16
  viewing on Utility Services 31
firmware backup setting 16

G

Gateway Firmware
  Upload Gateway Firmware 41
General Administration 55
General Settings
  Detail Screen settings 58
  General Administration 55
  LDAP Administration 56
  LDAP Filter Settings 58
  Search Screen settings 57

I

Include Firmware in Backup 16
IP Phone 13
IP Phone:backup 26
IP Phone:restore 26
IP phone back up and restore 27
IP Phone custom file 27
  uploading and activating custom file 28
  viewing custom file 27
IP Phone file server 11
IP Phone firmware management 11
IP phone firmware manager 28
IP Phone Firmware Removal 13
IP Phone Push Server 11
IP Phone Setting Editor field descriptions 26
IP Phone settings:advanced editing 25
IP phone settings:basic editing 25
IP Phone settings:checking syntax 25
IP phone settings:configuring view of settings file 23
IP phone settings:saving 26
IP phone settings editor 23
IP Phone Settings Editor 11
IP Phone Tools
  IP Phone custom file 27
IP telephone Push Server
  Display Push Database 42
  sending push messages 42
  Test Push Database 42
IPv6 15
IPv6 DHCP IP address pools 39
IPv6 DHCP IP Address Pools
  updating DHCP IPv6 values 39
IPv6 DHCP Leases Display 39, 40
IPv6 DHCP Manager
  IPv6 DHCP Sever Log 40
IPv6 DHCP server 11
  status 37
IPv6 DHCP Server status

IPv6 DHCP Server status *(continued)*
  activate/deactivate IPv6 DHCP 38
IPv6 DHCP Server Status
  viewing IPv6 DHCP Server status 38
IPv6 DHCP Sever Log
  viewing IPv6 DHCP log files 40
IPv6 Ping Host 15

L

LDAP Administration 56
LDAP connection settings 54
LDAP database 54
LDAP Filter Settings 58
legal notice ....
Linux Messages log files 44
load last working DHCPD conf file 38
Log viewer 11

M

managing IP phone settings 24
Miscellaneous
  IPv6 Ping Host 15
  Upload files 16
MyPhone 12, 45, 50
MyPhoneAdmin 45
MyPhone Admin 12
MyPhone Feature Buttons 12
MyPhone Server 45, 50
MyPhone server log files 46
MyPhone User Guide 13

N

NTP Status 18
NTP Synchronization Status 18

O

out of band management 10

P

phone firmware
  upload 32
phone firmware manager 48
Phone Firmware Manager 44
ping 15
ping: IP host 15
ping:TCP host 15
pinging a host 15

R

removing DHCP subnets 36
restore 16, 17
RFA License Activation 18

S

saving ADVD settings 22
Schedule Phone File Download
  schedule control 32
schedule phone file download button descriptions 34
schedule phone file download field descriptions 33
scheduling endpoint reset 32
Search Screen settings 57
showing DHCP lease 36
Show IPv6 DHCP Lease 40
SIP Enablement Server 26
SIP Phone 26
software version 14
Software Version 11
SQL import server 47
stations
  viewing in Utility Services 30
subnet 35
support 65
system database 45
system database status 49
System Message 12

T

Test Push Database 42
TFTP server 46, 50
TFTP Server
  TFTP server access log 46
  View Archive Log Files 46
TFTP server access log 46
training 63

U

Update Customer Banner 17
Upload files 16
Upload Gateway Firmware 41
  uploading Gateway firmware 41
  viewing Gateway firmware 41
uploading and activating custom file 28
uploading Gateway firmware 41
upload phone firmware 32
Utility Admin 11
Utility Server 26, 44, 52
Utility Server backup 16
Utility services
  overview 10
Utility Services 43, 51
  backup 16
  configuring login for Communication Manager 28
  managing firmware 31

Utility Services *(continued)*
restore 16
uploading telephone firmware 16
viewing available firmware 31
viewing stations 30
viewing the legal notice 14
viewing the software version 14
Utility Services applications
MyPhone 12
MyPhone Admin 12
Utility Admin 11
Utility Services backup file 16
Utility Services restore 17
Utility Services Standalone template
elements of the 46xxsettings.txt file 68
MyPhone 67
Phone Firmware Manager 67

V

videos 64
viewing custom file 27
viewing DHCP lease information 40
viewing DHCP log files 37
viewing DHCP server status 34
viewing DHCP subnets 35
viewing IPv6 DHCP log files 40
Viewing Linux Messages log files 44
Viewing PFM Server log files 45
View Linux Messages Log Files 44
View Phone Firmware Manager Server Log Files 44

W

Warranty 9
Watchdog file 43
Watchdog test 43
WML Links 12