Administering Avaya Flare® Experience for iPad Devices

Release 1.2
18-604079
Issue 02.01
January 2014

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED 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 AUTHORIZED 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, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

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

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

Copyright

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

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

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

Avaya is a registered trademark 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.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

About this guide

This guide describes server administration for Avaya Flare® Experience. In release 1.2, this document only contains iPad administration information. In future releases, Windows information will also be added to this document.

Product documentation

The following documents are available for Avaya Flare® Experience:

- *Administering Avaya Flare® Experience*, document number 18-604079 (for administrators). This document contains server administration information for Avaya Flare® Experience for iPad Devices. Administration information for other Avaya Flare® Experience products will be consolidated into this document in future releases.
- *Using Avaya Flare® Experience for iPad Devices*, document number 18-603943 (for end users). This document contains overview, installation, and feature usage information.
- *Using Avaya Flare® Experience for Windows*, document number 18–604158 (for end users). This document contains overview, installation, and feature usage information.

Avaya Mentor videos

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

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

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

Support

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

Chapter 2: Requirements

Server requirements

The Avaya Aura® server elements required to support Avaya Flare® Experience are listed below. For more information about products that interwork with Avaya Flare® Experience, see http://support.avaya.com/CompatibilityMatrix/Index.aspx.

- Avaya Aura® Session Manager Release 6.2 or 6.3.

  You can configure more than one Session Manager server. If the primary server fails, Avaya Flare® Experience automatically fails over to the secondary Session Manager server to ensure service continuity for users.

- One of the following Avaya Aura® Communication Manager servers:

  - Avaya Aura® Communication Manager Feature or Evolution Server Release 6.3.1 (FP 2, SP 1) for encrypted audio and unencrypted video.
  - Avaya Aura® Communication Manager Feature or Evolution Server Release 6.3.2 (FP 3) for encrypted audio and encrypted video.

- Avaya Aura® System Manager Release 6.2 or 6.3.
- Avaya Aura® Conferencing Release 7.0 Service Pack 2 or later if you want to use the Conference (audio and video) and Web Collaboration features.
- Avaya Aura® Presence Services Release 6.1 Service Pack 2 or later if you want to use the presence and instant messaging features. To use the single sign-on feature, you must have Avaya Aura® Presence Services Release 6.2.2 Feature Pack 3 with SASL authentication configured.

  Note:

  Avaya Flare® Experience users can send and receive instant messages with Microsoft Office Communicator 2007 R2 users and Microsoft Lync users. For more information about using Presence and IM with users of these Microsoft clients, see *Integrating Avaya Aura® Presence Services with Microsoft OCS*.

You can optionally use the Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.2 or higher to provide a secure connection for the following Avaya Flare® Experience settings when users are working remotely and are not connected to the enterprise network.

- SIP-TLS to Avaya Aura® Session Manager and Avaya Aura® Presence Services for Presence functionality
- XMPP to Avaya Aura® Presence services for instant messaging functionality
- PPM over HTTPS to Avaya Aura® Session Manager
- LDAPS to LDAP server

If the Avaya Flare® Experience client is communicating with the Avaya SBCE, you should provision DNS entries for the Avaya Aura® Session Manager, Presence Server, and Enterprise Search (LDAP) server that resolve to the internal service IP addresses for internal DNS clients and resolve to the Avaya SBCE IP address for external DNS clients. By doing this, no configuration change is required for users that use the client both inside and outside your corporate network.

For information about installing the Avaya Avaya SBCE, see *Installing Avaya Session Border Controller for Enterprise*. For information about configuring the Avaya SBCE, see *Administering Avaya Session Border Controller for Enterprise*.

Related topics:

Multiple Device Access requirements for Avaya Flare Experience for iPad Devices on page 10
Security on page 10

Multiple Device Access requirements for Avaya Flare® Experience for iPad Devices

Avaya Flare® Experience for iPad Devices supports Multiple Device Access (MDA). This feature allows users to log in to multiple devices with the same extension, as well as answer and join point-to-point calls from multiple devices.

MDA requires the use of TLS endpoints. Users can log in to their extension with a TCP device, but a new incoming call will not ring on the TCP device and the user will not be able to join the call from that device.

For details on other MDA user limitations, see *Using Avaya Flare® Experience for iPad Devices* (18-603943).

Security

To provide a secure communication channel for voice and instant messaging sessions, Avaya Flare® Experience requires Transport Layer Security (TLS). Avaya Flare® Experience also supports SRTP for both video and audio with Avaya Aura® dependencies.

Note:

- Avaya Flare® Experience does not currently support audio or video on Polycom SRTP devices.
- In Avaya Aura® Conferencing, you must ensure the Encrypt RTCP parameter is not selected to maintain SRTP on a conference call. When this parameter is selected, the SRTP call becomes an RTP call when the moderator adds participants into the conference.

The following table shows the ports that must be enabled for secure signalling on the Avaya Flare® Experience client.

Network firewall port matrix	
Destination	**Port**
Avaya Aura® Session Manager	5060 (SIP/TCP) or 5061 (SIP/TLS)
Avaya Aura® Presence Services (XMPP/TLS)	5223
Avaya Aura® Session Manager (PPM traffic)	80 and 443 (HTTP/SOAP)
Media Gateway	RTP/UDP port range (depends on ip-network-region)
Directory Server	389 (LDAP) or 636 (LDAPS)

Related topics:

Server requirements on page 9

Supported codecs

Avaya Flare® Experience supports the following audio codecs:

- G.711 A-law (PCM-A)
- G.711 U-law (PCM-U)
- G.722
- G.729a
- iSAC

Avaya Flare® Experience supports the following video codecs:

- H.264

For information on bandwidth requirement for different codecs, see the section **Codec Selection** in *Avaya IP Voice Quality Network Requirements* on the Avaya Web site at http://www.avaya.com/support.

DSCP values

The Avaya Flare® Experience client uses the following default DSCP values to mark packets to support network quality of service mechanisms:

- Audio: 46
- Video: 26

Related topics:

Configuring the audio and video quality of service settings on page 19

Supported LDAP directories for Avaya Flare® Experience for iPad Devices

Avaya Flare® Experience for iPad Devices supports LDAPv3 (both LDAP and secure LDAP) with Microsoft® Active Directory 2003 and 2008.

During an LDAP search, Avaya Flare® Experience for iPad Devices searches the following attributes:

- sn (surname/family name)
- givenName
- cn (common name)

After the search, the name is constructed using the sn and givenName.

If a user adds the contact to the Aura Contacts, and that contact is already an enterprise contact, the name will be overwritten by the localized display name in Avaya Aura® System Manager. When a user adds the contact from an enterprise search, the mail and telephone number attributes are used for determining whether the contact is added to Enterprise or Private in Aura Contacts. The homephone, mobile, and mail attributes for the added contact are displayed in the Contacts fan in the Avaya Flare® Experience for iPad Devices client.

Chapter 3: Network diagnostics and system configuration

Media quality on a consumer device like the Apple iPad is influenced heavily by the network in which the device is deployed as well as the deployed Avaya Aura® system configuration. The way in which the device is connected to the wireless network (for example, a cellular data connection with a virtual private network) can also influence media quality.

Network diagnostics

Avaya Flare® Experience for iPad Devices provides a call quality indicator to help you diagnose some of the issues that arise in wireless networks. By tapping and holding the Call Timer box for an active call in Avaya Flare® Experience for iPad Devices, you can view the audio and video statistics for the current session. You can use these statistics to determine the network conditions that may be affecting this session.

Packet loss

As you approach 1% packet loss, you may start to see visual artifacts (for example, see broken images) or hear audible artifacts. As you approach 2 to 3% packet loss, there will be consistent visual artifacts and audible artifacts.

Note:

Packet loss characteristics influence the occurrence of visual and audible artifacts. For example, a burst of lost packets will affect the media quality differently than an even distribution of lost packets.

Jitter

Jitter is caused when the packets that make up a media stream are not delivered at regular intervals to the endpoint. The effects of jitter are cancelled by buffering for the most part, but buffering causes delay. Delay, or latency, has a noticeable effect on lip synchronization between the audio and video feed for the user. Lip synchronization issues will occur when the delay exceeds 100 ms.

Generally speaking, the statistics described above are strongly influenced by network and network engineering issues. If you find the values of the impairments exceeding the limits listed above, you may need to contact your network administrator for more diagnostic information to solve any network implementation issues.

Avaya Aura® Configuration

The Avaya Aura® solution enables the administrator to configure the maximum bandwidth permitted on a per-user basis. The Avaya Flare® Experience client video encoders will adjust to fit within the bandwidth “envelope” provided by the network, but the resulting video quality is influenced heavily by the amount of bandwidth available. If there is more bandwidth available, the resulting video quality for the user will be better. Network engineers should also confirm that the appropriate classes of service for the network have been defined and that the correct DSCP mark is set for media in the Avaya Aura® configuration.

For Avaya Aura® Conferencing 7.0 Service Pack 2 or later, each user is assigned a specific profile for video, which enables different classes of resolution. These profiles can be provisioned to be 180p or 360p, but the profiles can be provisioned only at the conferencing server – not at the client device.

If you have good quality video, but you are dissatisfied with the resolution, you should check the provisioning at your endpoint to confirm that adequate bandwidth and the correct profile have been assigned to your endpoint. To determine the resolution you are receiving on the Avaya Flare® Experience client, check the call statistics for the resolution as well as the frames per second provided.

Virtual Private Networks (VPNs)

Virtual private networks provide a significant challenge to high-quality video because as a security measure the VPN assigns video packets the same priority it does all other packets. This method prevents malicious users from differentiating certain classes of traffic that could lead to targeted attacks on clients. VPNs effectively negate network engineering for differentiated service and also introduce additional delay, which can be problematic for media packets that depend on timely receipt of all video packets for subjectively good quality.

To ensure a better overall experience, the Avaya Flare® Experience client will drop to a lower frame rate of 15 frames per second (fps) from 30 fps when a VPN is detected, enabling the video encoder to create a more robust bit stream and making calls over the VPN more reliable. This reduction of the frame rate allows users to remotely connect through the network and maintain a quality media experience. Note that this detection and optimization does not apply when connecting through a network element like a Session Border Controller (SBC).

Troubleshooting Logs

When troubleshooting issues, it may become necessary to report logs to your support organization. Logging for the Avaya Flare® Experience client includes media quality statistics that record information about network performance for analysis by support teams. To enable these logs, you must enable the **Verbose Logging** option in the Settings dialog box. These logs can assist support teams in diagnosing media issues due to network performance.

To send log files, under **Settings**, select **Support Information** > **Send Logs**.

Chapter 4: Configuring Avaya Aura® Communication Manager settings

Use the Avaya Aura® System Manager administration interface to modify the Avaya Aura® Communication Manager settings. For information about configuring Avaya Aura® Communication Manager, see *Administering Avaya Aura® Communication Manager* (03-300509).

Perform the following steps:

- For the Communication Manager signaling group associated with Avaya Session Manager, under IP network regions, set:
  - **Transport Method** to **tls**.
  - **Enforce SIPS URI for SRTP** to **y**.
  - **Initial IP-IP Direct Media** to **y**.
- For trunk signaling with the PRI line, under Trunk Parameters, set **Disconnect Supervision - Out** to **y**. If this field is not set, some point-to-point call transfers will not work properly.
- On page 19 of System Parameters – Features, set **SIP Endpoint Managed Transfer** to **y**.
- To support secure calls, set the following additional parameters:
  - Under System Parameters – Features, set **Initial INVITE with SDP for secure calls?** to **y**.
  - Under System Parameters — Customer Options, set **Media Encryption Over IP?** to **y**.
  - Under IP Codec Set, in the Media Encryption section, set 1 to **1-srtp-aescm128-hmac80**, 2 to **2-srtp-aescm128-hmac32**, and 3 to **none**.

You must also configure Avaya Aura® endpoints for Avaya Flare® Experience. The following list describes the minimum configuration you must perform on the Endpoints page to use Avaya Flare® Experience features.

- Enable **IP SoftPhone**.
- Enable **IP Video SoftPhone**. For video calls, Avaya Flare® Experience for iPad Devices supports a maximum resolution and frame rate of 352 x 288 pixels @ 30 fps.
- If a bridged line appearance is configured for the extension, enable **Bridged Call Alerting** to alert the Avaya Flare® Experience client when a call arrives at the main extension to which the Avaya Flare® Experience client is bridged.
- Configure eight call appearances to provide support for merging active calls.

Depending on your system configuration, you may need to perform additional configuration steps on the Avaya Aura® Communication Manager Endpoints page.

Chapter 5: Configuring user accounts in Avaya Aura® Session Manager

Use the Avaya Aura® System Manager administration interface to access Avaya Aura® Session Manager. You can add or modify user profiles through Avaya Aura® Session Manager. For detailed information about user profiles, see *Administering Avaya Aura® Session Manager*.

Avaya Flare® Experience supports only SIP endpoints. H.323 endpoints are not supported. For each Avaya Flare® Experience extension, set the following settings on the User Profile page:

- Set an **Avaya SIP** communication address. If you have E.164 numbers in your enterprise directory, you may also set an **Avaya E.164** communication address for the extension.
- Set **Origination Application Sequence** to the Communication Manager server.
- Set **Termination Application Sequence** to the Communication Manager server.
- Set Template to any 96x1 SIP template.
- In the **Max. Simultaneous Devices** and **Block New Registration When Maximum Registrations Active?** fields, specify the requirement for simultaneous device registrations. Avaya Flare® Experience for iPad Devices currently supports Multiple Device Acess (MDA).
- Enable **Conferencing Profile** and configure the settings for the user's Avaya Aura® Conferencing profile. See *Deploying Avaya Aura® Conferencing* for information about configuring Avaya Aura® conferencing. You must configure Avaya Aura® conferencing to use the conferencing feature in Avaya Flare® Experience.

Chapter 6: Configuring the audio and video quality of service settings

About this task

Use the Avaya Aura® System Manager administration interface to configure the audio and video quality of server (QoS) settings. For more information, see *Installing and Configuring Avaya Aura® Session Manager* on the Avaya Web site at http://www.avaya.com/support.

Procedure

1. Log in to Avaya Aura® System Manager.
2. Select **Elements > Session Manager**.
3. In the navigation pane, select **Device and Location Configuration > Device Settings Groups**.
4. On the Device Settings Groups page, select the appropriate group (for example, default group, a terminal group, or a location group), and click **Edit**.
5. On the Device Settings Group page, click the right-arrow for **DIFFSERV/QOS Parameters**.
6. Configure the PHB values.
7. Click **Save**.
8. In the navigation pane, select **Device and Location Configuration > Location Settings**.
9. On the Location Settings page, select the device settings group you modified in Steps 4 through 6 from the Device Setting Group drop-down list box for each appropriate location.
10. When finished, click **Save**.

Chapter 7: Configuring automatic service discovery for Avaya Flare® Experience

You can configure automatic service discovery on the iPad client so users do not have to configure the client Settings manually. Users will simply have to enter a URL or email address and the client settings will automatically be configured.

The following checklist describes the tasks you must perform to configure automatic service discovery for the enterprise.

Task	Notes	✔
Create a Settings Configuration file with the settings information for the enterprise.	Save your Settings Configuration file to an enterprise web server. If the web server for your enterprise uses a secure `https` connection, make sure there is a security certificate available for users to install on their iPad.	
Configure your DNS server with three DNS records	Set up of the DNS server varies for each enterprise. However, three standard DNS records must be created to link the enterprise's DNS server to the Settings Configuration file. **Note:** DNS set up is only required if an email address will be used for automatic service discovery. DNS is not required if a standard web address will be used.	

Creating the Settings Configuration file

Create a Settings Configuration file in the JSON or Avaya settings text file (46xxsettings.txt) formats with the Avaya Flare® Experience client Settings for the enterprise.

Description of elements

The following table describes the main element strings for the file.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>userid (JSON name)
SSOUSERID (Avaya settings text file name)</td><td>Account user ID.
There are no other values associated with this element.</td></tr>
<tr><td>sso</td><td>Single sign-on or unified log in configuration that allows users to log in to the Avaya Flare® Experience client and access all features with the same login.
The following values are associated with this element.

<table>
<tr><th>JSON value name</th><th>Avaya settings text file value name</th><th>Description of value</th></tr>
<tr><td>enabled</td><td>SSOENABLED</td><td>Indicates whether single sign-on (SSO) is enabled.
Enter 1 to indicate that SSO is enabled, and 0 to indicate that SSO is disabled.</td></tr>
<tr><td>realm-mapper</td><td>SSOREALMMAPPERADDRESS</td><td>Link to the Realm Mapper service.</td></tr>
</table></td></tr>
<tr><td>signaling</td><td>Voice over IP (VoIP) server configuration.
The following values are associated with this element:

<table>
<tr><th>JSON value name</th><th>Avaya settings text file value name</th><th>Description of value</th></tr>
<tr><td>use-sso</td><td>SIPSSO</td><td>Indicates whether SSO is being used.
Enter 1 to indicate that SSO is enabled, and 0 to indicate that SSO is disabled.</td></tr>
<tr><td>address</td><td>SIPPROXYSRVR</td><td>IP address or fully qualified domain name (FQDN) of the VoIP server. An example is <code>135.20.246.20</code> (IP address) or <code>sip.gsc.avaya.com</code> (FQDN).</td></tr>
<tr><td>port</td><td>SIPPORT</td><td>VoIP server port. The default port numbers are 5060 for TCP and 5061 for TLS.</td></tr>
<tr><td>domain</td><td>SIPDOMAIN</td><td>Domain for transmitting VoIP data. An example is <code>example.com</code>.</td></tr>
<tr><td>use-ssl</td><td>SIPSECURE</td><td>Indicates whether TLS is enabled for SIP signalling. Enter 1 to indicate that TLS is enabled, and 0 to indicate that TLS is disabled.</td></tr>
</table></td></tr>
<tr><td>conference</td><td>Conference configuration.</td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td></td><td>The following values are associated with this element:

<table><tr><th>JSON value name</th><th>Avaya settings text file value name</th><th>Description of value</th></tr><tr><td>enabled</td><td>CONFERENCEENABLED</td><td>Indicates whether Conferencing is enabled.
Enter 1 for enabled, and 0 for disabled.</td></tr><tr><td>address</td><td>CONFERENCE_FACTORY_URI</td><td>Adhoc conference URL (for example, 60397@example.com)</td></tr></table></td></tr>
<tr><td>support</td><td>E-mail support configuration.
The following values are associated with this element:

<table><tr><th>JSON value name</th><th>Avaya settings text file value name</th><th>Description of value</th></tr><tr><td>email</td><td>SUPPORTEMAIL</td><td>Defines the default e-mail address for sending diagnostic logs.</td></tr></table></td></tr>
<tr><td>presence</td><td>Presence server configuration
The following values are associated with this element:

<table><tr><th>JSON value name</th><th>Avaya settings text file value name</th><th>Description of value</th></tr><tr><td>enabled</td><td>PRESENCEENABLED</td><td>Indicates whether Presence is enabled.
Enter 1 for enabled, and 0 for disabled.</td></tr><tr><td>address</td><td>PRESENCE_SERVER</td><td>Address for presence server (for example, 135.20.246.11 or presence.gsc.avaya.com)</td></tr></table></td></tr>
<tr><td>video</td><td>Video server configuration
The following values are associated with this element:

<table><tr><th>JSON value name</th><th>Avaya settings text file value name</th><th>Description of value</th></tr><tr><td>enabled</td><td>VIDEOENABLED</td><td>Indicates whether video is enabled.
Enter 1 for enabled, and 0 for disabled.</td></tr></table></td></tr>
<tr><td>dialing-rules</td><td>Dialing rules configuration
The following values are associated with this element:</td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>JSON value name</th><th>Avaya settings text file value name</th><th>Description of value</th></tr>
<tr><td>enabled</td><td>ENHDIALSTAT</td><td>Indicates whether dialing rules are enabled.
Enter 1 for enabled, and 0 for disabled.</td></tr>
<tr><td>outside-line</td><td>PHNOL</td><td>Number to dial to access an external line. This value is generally set to 9 or is empty.</td></tr>
<tr><td>country</td><td>PHNCC</td><td>Country code.</td></tr>
<tr><td>area</td><td>SP_AC</td><td>Area code</td></tr>
<tr><td>pbx-main-prefix</td><td>PHNPBXMAINPREFIX</td><td>The PBX main prefix for your telephone number. An example is 538.</td></tr>
<tr><td>long-distance</td><td>PHNLD</td><td>Number to dial when making a long distance call within the same country.</td></tr>
<tr><td>international-call</td><td>PHNIC</td><td>Number to dial when making an international call.</td></tr>
<tr><td>internal-extension-length</td><td>PHNDPLENGTH</td><td>Length of internal extensions.</td></tr>
<tr><td>national-number-length</td><td>PHNLDLENGTH</td><td>Length of phone numbers within the country (national phone numbers).</td></tr>
<tr><td>remove-area-code</td><td>PHNREMOVEAREACODE</td><td>Indicates whether the area code should be removed for local calls.
Enter 1 for true, and 0 for false.</td></tr>
</table>
</td></tr>
<tr><td>ldap</td><td>Enterprise search or LDAP configuration
The following values are associated with this element:

<table>
<tr><th>JSON value name</th><th>Avaya settings text file value name</th><th>Description of value</th></tr>
<tr><td>use-sso</td><td>DIRSSO</td><td>Indicates whether SSO is being used.
Enter 1 to indicate that SSO is enabled, and 0 to indicate that SSO is disabled.</td></tr>
<tr><td>enabled</td><td>DIRENABLED</td><td>Indicates whether LDAP is enabled.
Enter 1 for enabled, and 0 for disabled.</td></tr>
<tr><td>server</td><td>DIRSRVR</td><td>IP address or fully qualified domain name (FQDN) of the LDAP server. An example</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>JSON value name</th><th>Avaya settings text file value name</th><th>Description of value</th></tr>
<tr><td></td><td></td><td>is <code>135.20.246.111</code> (IP address) or <code>ldap.gsc.avaya.com</code> (FQDN).</td></tr>
<tr><td>username</td><td>DIRUSERNAME</td><td>LDAP authentication user name.</td></tr>
<tr><td>password</td><td>DIRPASSWORD</td><td>LDAP authentication password.</td></tr>
<tr><td>search-root</td><td>DIRTOPDN</td><td>LDAP search root. An example is <code>ou=global users,dc=global,dc=example,dc=com</code>.</td></tr>
<tr><td>use-ssl</td><td>DIRSECURE</td><td>Indicates whether TLS is enabled. Enter 1 to indicate that TLS is enabled, and 0 to indicate that TLS is disabled and TCP is used.</td></tr>
</table>
</td></tr>
</table>

Examples of the Settings Configuration file

JSON format example

The following example shows the Settings Configuration file in the JSON format and the types of values that can be used for each string and sub-string.

```
{ "accounts":
       "userid": "",
     "sso": {
                "enabled": "1",
              "realm-mapper": "ide.example.com/getCredentials"          },
     "signaling": {
        "address": "sipserver.example.com",
        "port": "5061",
        "use-ssl": "1",
        "domain": "example.com",
        "use-sso": "1",
        "username": ""
       },
      "conference": {
         "enabled": "1",
         "address": "22111@example.com"
       },
      "presence": {
         "enabled": "1",
         "address": "server.presence.example.com",
                 },
      "video": {
         "enabled": "1"
       },
      "ldap": {
         "enabled":"1",
```

```
        "server": "ldapserver.example.com",
        "use-sso":"1",
        "username": "",
        "password": "",
        "search-root":"dc=global,dc=example,dc=com",
        "use-ssl":"1"
      },
     "dialing-rules": {
        "enabled": "0",
        "outside-line": "9",
        "country": "1",
        "area": "613",
        "long-distance": "1",
        "international-call": "011",
        "internal-extension-length": "7",
        "national-number-length": "10"
         "remove-area-code": "1"
       },
     "support": {
           "email": "support@example.com"
           }
```

Avaya settings text file format

The following example shows the Settings Configuration file in the Avaya settings text file (46xxsettings.txt) format and the types of values that can be used for each string and sub-string.

```
## SSO
SET SSOUSERID ""
SET SSOENABLED "1"
SET SSOREALMMAPPERADDRESS "ide.example.com/getCredentials"

## Signaling
SET SIPSSO "1"
SET SIPUSERNAME ""
SET SIPPROXYSRVR "sipserver.example.com "
SET SIPPORT ""
SET SIPDOMAIN "example.com "
SET SIPSECURE "1"

## Conference
SET CONFERENCEENABLED "1"
SET CONFERENCE_FACTORY_URI "22111@example.com"

## Presence
SET PRESENCEENABLED "1"
SET PRESENCE_SERVER "server.presence.example.com"

## Video
SET VIDEOENABLED "1"

## LDAP
SET DIRENABLED "1"
SET DIRSRVR "ldapserver.example.com "
SET DIRSSO "1"
SET DIRUSERNAME ""
SET DIRPASSWORD ""
SET DIRTOPDN "dc=global,dc=example,dc=com"
SET DIRSECURE "1"

## Dialing Rules
SET ENHDIALSTAT "1"
SET PHNOL "9"
```

```
SET PHNCC "1"
SET SP_AC "613"
SET PHNPBXMAINPREFIX ""
SET PHNLD "1"
SET PHNIC "011"
SET PHNDPLENGTH "7"
SET PHNLDLENGTH "10"
SET PHNREMOVEAREACODE "1"

## Support
SET SUPPORTEMAIL "support@example.com"
```

Setting up the DNS server

For users to use automatic service discovery, you must create records on your enterprise's DNS server to link your DNS server to the Settings Configuration file.

Note:

DNS set up is only required if an email address will be used for automatic service discovery. DNS is not required if a standard web address will be used.

Before you begin

- You must create the Settings Configuration file. For more information, see Creating the Settings Configuration file on page 21.
- Configure a web server and save the Settings Configuration file to that web server. You will need to know the URL to the file on the web server for this procedure.
- If your web server uses a secure `https` connection, create a security certificate for users to install on their iPad.
- Select a descriptive name for your settings file that will work with the limits of your enterprise's DNS server. Some DNS servers have restrictions on the characters that can be used in names.
- Set the following information based on your DNS server policy:
  - SRV and TXT record time-to-live period in seconds (for example, 300).

    During this time, client or intermediate servers may cache the retrieved record. Generally, the SRV and TXT record time-to-live periods share the same value.
  - Web server port number (for example, 0).
  - SRV record priority (for example, 0).
  - SRV record weight (for example, 0).

Procedure

1. Create a PTR record linking the descriptive name of your Settings Configuration file to your enterprise's domain.

a. Make sure the PTR record is named `_avaya-ep-config._tcp.<domain>`.
b. Use the descriptive name for the Settings Configuration file as the target of the PTR record: `<Descriptive name>.avaya-ep-config._tcp.<domain>`.

The following is an example of a PTR record:

```
_avaya-ep-config._tcp.example.com. PTR Production._avaya-ep-config._tcp.example.com
```

2. Create an SRV record linking the descriptive name of your Settings Configuration file to the web server where the file resides.

   If the URL to the Settings Configuration file is `https://server.example.com/settings.json`, then the server name is `server.example.com`.

   An SRV record also includes the following information:

   • SRV "time to live" period in seconds during which the client or intermediate servers may cache the retrieved record.

   The following is an example of an SRV record:

   ```
   Production._avaya-ep-config._tcp.example.com. 300 IN SRV 0 0 0 server.example.com
   ```

   In this example:

   • 300 is the time-to-live period

   • The three zeros are the priority, weight, and port number.

3. Create a TXT record linking the descriptive name of your Settings Configuration file to the remaining URL information.

   TXT records are provisioned differently depending on the DNS server. However, all TXT records must have the three parameters described in the following table.

Key	Description	Value
txtvers	The text version of the TXT record. This value indicates the structure version of the record.	The value must always be set to 1.
path	The path to the Settings Configuration file.	An example value is: `/settings.json`.
proto	Web server access scheme	This value is generally `http` or `https`

   The following is an example of a TXT record:

   ```
   Production._avaya-ep-config._tcp.example.com. 300 IN TXT "txtvers=1" "proto=https" "path=/settings.json"
   ```

In this example, 300 is the time-to-live period

Index