Avaya Identity Engines Release Notes
Software Release 9.0.3

1. Release Summary

Document Version: 05.04
Document Date: March 2015
Purpose: Identity Engines (IDE) software service pack release to introduce Enhancements, and to address customer found software issues.

Release Notes Revisions	Description	Comments
05.01	Initial release of Release Notes for IDE 9.0.3	
05.02	Correction of the 9.0.3 GA build number	
05.03	For clarity, added a note to the corrected 9.0.3 GA build number and also added this Release Notes Revisions table	
05.04	Updated • Minimum AOS version for AP9100 • Dashboard supported OSs • Add SSO issue(wi01211922) to Outstanding Issues section	

2. Important General Notes

- Avaya provides the Identity Engines Ignition Server as a complete Virtual Appliance.
  - Do not install or uninstall any software components on this Virtual Appliance unless Avaya specifically provides the software and/or instructs you to do so.
  - Do not modify the configuration or the properties of any software components of the Ignition Server VM (including VMware Tools) unless Avaya documentation and/or personnel specifically instruct you to do so.
  - Avaya does not support any deviation from these guidelines.

- Avaya does not support upgrading the VMware Tools in the Ignition Server VMware VM. If you have already updated the VMware tools or unsure, stop the process and follow the procedure given below:
  - Take a backup of Ignition Server configuration from your existing VM.
  - Deploy a fresh new Ignition Server using the OVA supplied by Avaya.
  - Install the necessary licenses. You may need to obtain new licenses in case you have created a new instance of the Ignition Server(s).
  - Restore the configuration.

- **Avaya WLAN 9100 users MUST read and follow the instructions provided in this Releases Notes to ensure proper upgrade to Identity Engines Release 9.0.3**

3. Important Notes about this Release

- This Identity Engines Service Pack 9.0.3 is an update only for the following Identity Engines components:
  - Ignition Server
  - Ignition Dashboard

- Upgrade from release 8.0.x to 9.0.x is not available as the hardware system requirements for release 9.0.x have changed compared to previous release(s).Customers who are on release 8.0.x should take a configuration back from 8.0.x, install the 9.0.3 OVA and then restore the 8.0.x configuration into 9.0.3 instance. Follow the upgrade procedure in "***Chapter 9. Upgrade Procedure"*** of this document.

- If you are running release 9.0.1 or 9.0.2 and would like to migrate to 9.0.3, you have two options:
  - Take a configuration backup from 9.0.1 or 9.0.2, deploy a new 9.0.3 VM and perform a configuration restore on the 9.0.3 VM. New licenses will be required. Follow the upgrade procedure in "***Chapter 9. Upgrade Procedure"*** of this document.
  - Perform an upgrade directly from 9.0.1 or 9.0.2 to 9.0.3 using the pkg (Package) file. Follow the upgrade procedure in "***Chapter 9. Upgrade Procedure"*** this document.

- Please be reminded that whenever you deploy fresh new OVA, you will have to obtain new licenses.

4. Platforms Supported

The following VMware ESXi platforms are supported with Identity Engines release 9.0.3:
VMware vSphere version 5.0
VMware vSphere version 5.1
VMware vSphere version 5.5

Please be aware that a VMware ESXi platform upgrade may be necessary as previous release 8.0.x also supported VMware ESXi 4.0, 4.1 and 5.0. VMware ESXi 4.x is no longer supported in Identity Engines release 9.0 and above.

IMPORTANT NOTE:
Note that VMware vMotion, VMware Player and VMware Workstation are not supported and cannot be used in conjunction with the Ignition Server.

5. Installation

File Names for Identity Engines release 9.0.3

File Name	Module or File Type	Comments
AIEIS_RHEL_6_3_LINUX-VM_09_00_03_027725_x86_64.ova (1)	Ignition Server OVA files for vSphere 5.x environment	Ignition Server release 9.0.3. This file is used if fresh VM install option is desired.
LINUX-VM_09_00_03_027725_server_complete.pkg (1)	Ignition Server upgrade package files for vSphere 5.x environment	Ignition Server release 9.0.3. These files are used if upgrade option is desired.
DashboardInstaller-9.0.3.27725.exe (1)	Dashboard Installer	Dashboard Installer release 9.0.3 compatible with Ignition Server release 9.0.3

(1) Revision 05.01 of this IDE 9.0.3 Release Notes indicated an incorrect build number of the GA software

Identity Engines software file names of Release 8.x and 9.x that are compatible for deployment in conjunction with Identity Engines Release 9.0.3

File Name	Module or File Type	Comments
AdminConsoleInstaller-1.0.0.22931.exe	CASE Manager Installer	CASE Manager release 1.0 is compatible with Ignition Server release 9.0.3
AccessPortal_01.00.00_022931_x86_32.mf AccessPortal_01.00.00_022931_x86_32.ovf AccessPortal_01.00.00_022931_x86_32.vmdk	Access Portal OVF files for vSphere 4.x and 5.x	Access Portal Release 1.0 is compatible with Ignition Server release 9.0.3
GuestManagerInstaller-9.0.0.25816.exe	Guest Manager installer	Bug Fixes and compatibility with Ignition server release 9.0.3
SSOServiceProviderAgent-9.0.0-25816.zip SSOServiceProviderAgent-9.0.0-25816.tar.gz	Service Provider Agent Package	Service Provider application and configuration utility for Identity Engines Web-based SSO

6. Compatibility

Identity Engines Ignition Server release 9.0.3 software can only be managed with Avaya Ignition Dashboard release 9.0.3.

See "***Chapter 5. Installation"*** for other Identity Engines software components compatibility matrix

Software	Software Compatibility	Comments
Ignition Server Release 9.0.3	• VMware ESXi versions 5.0 or 5.1 or 5.5 • Installation on a VMware ESXi server is done using an OVA file which already incorporates the OS Red Hat Enterprise Linux.	• The VM requires a x86_64 capable environment • Minimum 4 CPUs • Minimum 4 GB of memory • Minimum 260 GB available disk storage (thin provisioning is allowed) • Minimum 1 physical NIC (preferably 3 NICs) • 3 Logical NIC cards • VMware lists on its site supported hardware platforms for ESXi: http://www.vmware.com
Access Portal Release 8.0	• VMware ESXi versions 4.0(1) or 4.1(1) or 5.0 or 5.1 or 5.5 • Installation on a VMware ESXi server is done using an OVF file which already incorporates the OS FreeBSD.	• The VM requires 32-bit capable environment • Minimum 2 CPUs • Minimum 2 GB of memory • Minimum 10 GB available disk storage • Minimum 2 physical NIC (preferably 3 NICs). • VMware lists on its site supported hardware platforms for • ESXi: http://www.vmware.com
Ignition	• Windows 7 (32 bit or 64 bit)	• Minimum 2GB RAM memory

Dashboard Release 9.0.3	• Windows 8 (32 bit or 64 bit) • Windows 2008 (32 bit or 64 bit) (2)	• US English Windows
Guest Manager Release 9.0.0	• Windows 7 (32 bit or 64 bit) • Windows 8 (32 bit or 64 bit) • Windows Server 2008 (32 bit or 64 bit) (2)	• Minimum 2GB RAM memory • US English Windows
CASE Manager Release 8.0	• Windows Server 2008 (32 bit and 64 bit) (2) • Microsoft IE Browser • Firefox Browser	• Minimum 2GB RAM memory • US English Windows
Analytics Release 9.0	• Windows 7 (64 bit) • Windows Server 2008 (64 bit) • Microsoft IE Browser • Firefox Browser	• Minimum CPU 2+ GHz processor • Minimum 2GB of memory • Minimum 3GB available drive storage • The hard drive space requirement above is only for the installed application. Be sure to increase the hard drive space based on storage requirements for data logs and level of application usage. • US English Windows
Avaya Flare	Avaya Flare release 1.2 for iPad Avaya Communicator release 2.0 for iPad	• Compatible with Identity Engines R9.0.1, R9.0.2, R9.0.3 SSO
Avaya System Manager	Avaya SMGR release 6.2 FP3	• Compatible with Identity Engines R9.0.1, R9.0.2, R9.0.3 SSO
Service Provider Agent	Apache Tomcat 6.X	• Compatible with Identity Engines R9.0.1, R9.0.2, R9.0.3 SSO • Any servlet container compliant with the Servlet API specifications version 2.4 or higher will work, like Tomcat 6.x, JBoss or Websphere

Notes for Identity Engines OVA/OVF VMware ESXi versions

(1) Release 9.0.2 was the last release to support Access Portal on ESX 4.x versions

Notes for Dashboard/CASE Manager/Guest Manager Windows versions

(2) Release 9.0.2 was the last release to support Dashboard/CASE Manager/Guest Manager on Windows 2008 32-bit

7. Version of Previous Releases

Identity Engines Software release 9.0.2, Release Date – October, 2014
File name “NN47280-400_04_02_IDEngines_9_0_2_Release_Notes.pdf”

Identity Engines Software release 9.0.1, Release Date – June, 2014
File name “NN47280-400_03_03_IDEngines_9_0_1_Release_Notes.pdf”

8. Changes in this Release

8.1. New features in this Release

- Intelligent RADIUS Proxy
  - Ignition Server 9.0.3 introduces Intelligent RADIUS Proxy. Intelligent RADIUS Proxy enhances the Identity Engines RADIUS Proxy feature to allow forwarding RADIUS authentication requests to a remote RADIUS server and manipulate the response by adding, deleting, or modifying the RADIUS attributes returned by the Remote RADIUS server before delivering them to the Authenticator that originated the RADIUS authentication request.
  - A key use case of the Identity Engines Intelligent RADIUS Proxy is EDUROAM (Education Roaming). The EDUROAM is a secure, world-wide roaming access service which allows students and staffs from participating institutions to obtain network access in the campus when they visit other participating institutions. The core idea is that the authentication server at the new campus would simply proxy the authentication requests to the other authentication server where user account is originally provisioned. Identity Engines Ignition Server Intelligent RADIUS Proxy feature is enhanced to act as a RADIUS proxy server and forwards the authentication requests to remote RADIUS server to support EDUROAM while providing the administrator full control of network access.
  - Another key use case of the Identity Engines Intelligent RADIUS Proxy is to allow overlaying the Ignition Server over any network infrastructure and allow forwarding authentication requests to NAC system that may already exist and customer may choose not to replace it or may choose to gradually over time migrate from their existing NAC to Identity Engines.

- Avaya WLAN 9100 Licensing Support
  Ignition Server release 9.0.3 introduces and updated licensing logic:
  - Ignition Server Base LITE - 5 Standard Authenticators + 75 x AP 9100
  - Ignition Server Base SMALL - 20 Standard Authenticators + 300 x AP 9100
  - Ignition Server Base LARGE - Unrestricted Authenticators

  To make use of the enhanced licensing support for WLAN9 100, release 9.0.3 introduces a new Vendor called ‘Avaya-WLAN’ with Vendor Id 45. While configuring a WLAN 9100 AP as an authenticator on the Ignition Server, you must choose the following configuration settings:

Authenticator Type:	Wireless
Vendor:	Avaya-WLAN
Device Template:	generic-avaya-wlan

- Note: If you’ve previously added WLAN 9100 APs as authenticators on the Ignition Server, after upgrading to release 9.0.3 make sure to update the authenticator settings to use the above settings so that the WLAN 9100 authenticators can be counted against the enhanced WLAN 9100 licensing model. Please see “***Chapter 9. Upgrade Procedure”*** for more detail.

- Minimum software release for the WLAN 9100 AOS is 7.2.5

8.2. Problems Resolved in this Release

Work item Number	Description
wi01196879	IDE cannot cache both OU and CN groups with a “Custom Start DN”
wi01185322	Unexpected "Radius Request Timed out" message in Security log when using IDE as a RADIUS proxy server
wi01151857	Not able to associate internal users with internal devices

8.3. Outstanding Issues

Work item Number	Description
wi01211922	SAML authentication failure when SAML Access Policy uses Inbound attributes
wi01208520	CVE-2015-0235: GHOST glibc gethostbyname buffer overflow A new security vulnerability nicknamed "GHOST" was announced by the Common Vulnerabilities and Exposures organization of the US Department of Homeland Security. Its base risk score CVSS=6.8 by the time of risk assessment and Avaya security council also rated as “Medium” risk. To exploit on Ignition server, malicious user must understand internals of software to overflow the gethostbyname call • Access Portal/Guest Manager/Admin Console are NOT vulnerable Please, see Avaya Support knowledge base for more detail: https://support.avaya.com/kb/ext/SOLN262985
wi01208757	CVE-2014-3566: POODLE SSLv3 vulnerability A new security vulnerability was announced by the Common Vulnerabilities and Exposures organization of the US Department of Homeland Security Its base risk score CVSS=4.3 and Avaya security council rated as “Low-middle” risk. Enterprise customers are advised not to use browser or web clients using SSLv3. Identity Engines Portfolio server-side remediation plan is under investigation.
wi01132335	Identity Engines Access Portal requires a reboot after deleting a firewall rule
wi01038838	Guest Manager email notification notes are not sent when users are first created. They will show up if you resend the notification
wi01153249	Access Portal Syslog Stops Functioning if State Table Is Full
wi01170515	Access Portal disabling "HTTPS Login" ineffective until reboot
wi01170525	Access Portal - Captive Portal returns HTTP 500 Response for various reasons
wi01179781	MAC Authentication fails when "Trapeze" vendor is being used Please, see Avaya Support knowledge base for more detail and work-around: https://support.avaya.com/kb/ext/SOLN255242
wi01180963	Dashboard stuck in "Upgrade In Progress" loop during Ignition Server RADIUS "Initializing"
wi01185244	Identity Engines MAC authentication does not work when using Calling Station ID by default for Aruba WLAN controller Please, see Avaya Support knowledge base for more detail and work-around: https://support.avaya.com/kb/ext/SOLN255242
wi01189183	Identity Engines Access Portal 8.0 locks up during high volume of traffic
wi01190693	Identity Engines cannot import two certificates with the same CN
wi01183916	IDE failed to failover to RSA replication server when primary server is offline
wi01155908	When the connection between Dashboard sys-admin session and Ignition Server **is lost, sys-admin cannot login to dashboard again** With multi-administrators support in R9.0, only one sys-admin session is allowed at any time. If the sys-admin has not gracefully closed the Dashboard session and the connection between the Ignition Server and the Dashboard sys-admin session is lost for any reason (like network failure or the machine from the Dashboard is running is shut down), sys-admin cannot login to the system. As a work around, • login to console or open a SSH connection (must have previously enabled SSH on the Dashboard) to Ignition Server and run ‘show sessions’ command • Note down the ‘Id’ of the session entry for sys-admin Run ‘session delete id <id>’ to clear the stale session and the sys-admin can now login to the Dashboard
wi01126383	**In a deployment where Guest Manager and an Enterprise Web Server application using the Identity Engines Service Provider package for SSO are installed on the same server, user not able to add Guest Manager server configuration on the IDE** Typically, Guest Manager application which ships with its own Tomcat Web Server will be deployed on separate machines from the Enterprise web application servers. But if the user wants these two applications to co-exist on the same Tomcat server, first deploy the Guest Manager application on the server and then deploy your Enterprise

	web application and the Identity Engines Service Provider package for SSO next. After installing these applications, first configure the Guest Manager server details first on the IDE and then add the Service Provider details for SSO.

8.4. Known Limitations

Work item Number	Description
wi01121113	**In Form-based SSO authentication where a client trying to access a protected resource is redirected to the Ignition Server IdP, If IdP hostname contains special character like underscore, IdP login page shows unspecified service provider** Underscore is not considered a valid character for DNS hostname. Only following characters are allowed for DNS hostnames: • Alphabets, Numeric, Hyphens
wi01119478	**IdP summary shows two entries in HA even though SAML service is bound to VIP** In HA, if DNS configuration is not valid or not reachable on either of the HA nodes, then SSO configuration will not be valid. **Note: SSO feature requires a valid DNS configuration to be added to each IDE in HA which can then use it to resolve hostname to the interface IP address (or VIP) to which the SAML service is bound to.**
wi01127410	**While restoring large configuration, system takes additional 4-5 minutes for all the SSO services to come up** While restoring large config which contains many Directory services and large group cache information, Ignition Server will try to establish connectivity with the Directory services for group cache and service account creation. If any of these Directory services are unreachable, Ignition Server will keep trying to connect to them until time out. Eventually, the entire configuration will be loaded and the applications will come online. Users can make use of 'System Health' and 'Directory Service Status' tabs until 'monitor' to make sure all the services are up and running
wi01155806	**After session timeout triggers from Dashboard, session is not cleared from Ignition Server side immediately. It will take 30sec to 1 minute to clear** Each Dashboard connection will have a session time out after which the session is automatically disconnected. Though the session is closed from the Dashboard, it'll take 30-60 seconds for the session to be cleared from the Ignition Server side. If any user tries to login within this short interval (30-60 seconds), the login will not be allowed with an error saying 'session already exists'. Ignition Server session cleanup process runs every 60 seconds to clear any timed out sessions.
wi00852520	**One node IP address was truncated after breaking and creating HA multiple times from Dashboard** This issue is seen occasionally after breaking and creating HA multiple times. This issue does not affect any functionality. As a work around, users can logout and re-login to the Dashboard to fix the issue
wi01199049	**Not able to take IDE configuration backup if user gives back up file name as date format (example: Backup_11/19/2014).** Manual backup may fail if backup filename consists of special characters like "\", "/" or space. Only following characters are allowed for file names: • Alphabets (A-Z a-z), Numeric (0-9), Hyphens (-), Underscore (_) and Dot (.) **NOTE:** Spaces " " are not allowed in the filename with manual backup. Automated backups are not affected.

9. Upgrade Procedure

9.1. Pre-upgrade Checklist

Ignition Server Checklist

- Note that by design, users cannot upgrade an existing 8.0.x or earlier VM to 9.0.3 VM using software upgrade procedure.

- Existing 8.0.x, 9.0.0, 9.0.1 and 9.0.2 configurations can be migrated to 9.0.3 using the backup & restore functionality. Restore of configuration data on 9.0.3 release can only be performed from the following versions:
    - Backup of 8.0.x or 9.0.x configuration data
    - If you're running version older than 8.0.x and would like to upgrade to release 9.0.3, first perform an incremental upgrade to 8.0.x release and then use backup & restore functionality to migrate your existing configuration to 9.0.3 VM
    - Temporary licenses for IDE R8.0 and IDE R9.0 for this process of incremental migration of your configuration to IDE release 9.0.3 are available on www.avaya.com/identitytrial
- Release 9.0.3 introduces a new Vendor and device-template that must be used to configure the WLAN 9100 APs as authenticators on the Ignition Server. The new entries are created with the following names:
    - Vendor Name: Avaya-WLAN
        - Vendor Id: 45
        - Device Templates: generic-avaya-wlan
- Always take a backup of your Ignition Server configuration.
- Always take a snapshot of the Virtual Machine on the ESXi Server as a backup in case of upgrade failure.
- If the new Vendor and Device Template with the exact same names as above were already previously manually added on your current running Ignition Server, it is **required** to rename the existing entries to a different name prior to upgrade. This is a **mandatory** procedure otherwise new licensing model for WLAN 9100 will not function properly after upgrade.
- Release 9.0.3 cannot downgraded to a previous version. If the Ignition server is accidentally upgraded to 9.0.3 without renaming procedure as stated above, please use VM backup snapshot to restore back to original state.
- If it is migration procedure from existing 8.0.x/9.0.x configuration into a 9.0.3, the backup configuration **shall not** have the same Vendor and Device Template names as stated above. You **must** rename existing Vendor Name and Device Template prior to configuration backup and then restore on the 9.0.3.

Dashboard Checklist

- Identity Engines 9.0.3 also includes a new Dashboard installer that must be installed. Ignition Server release 9.0.3 cannot be managed from any previous versions of Dashboard

  Dashboard keeps the cached keystore of these certificates at following locations:

  Win XP
  C:\Documents and Settings\<user id>\Application Data\Avaya\security

  Win 7
  C:\Users\<user id>\AppData\Roaming\Avaya\security

  Win 8
  C:\Users\<user id>\AppData\Roaming\Avaya\security

  Delete these directories from your system before launching the new Dashboard

  Note that the above keystore folders may be hidden folders

- With Identity Engines release 9.0.3, no new update/upgrade software packages available for Guest Manager, Access Portal, CASE Manager and Analytics applications. Existing 8.x release software continues to be compatible with 9.0.3 release for these applications. See section ***6. Compatibility*** for details

9.2. Software Upgrade Procedure

- If you have Ignition Server 8.0.x then you must install 9.0.3 as a new VM:
  - Take a configuration backup from 8.0.x
  - Deploy a new 9.0.3 VM
  - Perform a configuration restore on the 9.0.3 VM
  - New licenses will be required
  - Perform a new backup of the 9.0.3 configuration

- If you have Ignition Server 9.0.1 or 9.0.2 and would like to install 9.0.3 as a new VM:
  - Take a configuration backup from 9.0.1 or 9.0.2
  - Deploy a new 9.0.3 VM
  - Perform a configuration restore on the 9.0.3 VM
  - New permanent licenses will be required.
    - You may use temporary licenses from www.avaya.com/identitytrial
  - Perform a new backup of the 9.0.3 configuration

- If you have Ignition Server 9.0.1 or 9.0.2 and would like to perform a 9.0.3 using software upgrade process:
  - Take a configuration backup from 9.0.1 or 9.0.2
  - In case of Ignition Server Standalone
    - Power down Ignition Server
    - Take a VMware Snapshot of the VM
    - Power up Ignition Server
  - In case of Ignition Server HA
    - Power down Ignition Server #1
    - Take a VMware Snapshot of VM #1
    - Power up Ignition Server #1
    - Power down Ignition Server #2
    - Take a VMware Snapshot of VM #2
    - Power up Ignition Server #2
  - Perform an upgrade directly from 9.0.1 or 9.0.2 to 9.0.3 using the pkg (Package) file.
  - Perform a new backup of the 9.0.3 configuration

10. Documentation

For latest documentation and for details on other known issues, please download the product documentation available from the Avaya Technical Support web site at: https://support.avaya.com/css/Products/P0622.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support

Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

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

Copyright

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

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding

distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(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 is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

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