

# Avaya Identity Engines Release Notes

## Software Release 9.0.2

### 1. Release Summary

Document Version: 04.02  
Document Date: October 2014  
Purpose: Identity Engines (IDE) software service pack release to introduce Enhancements, and to address customer found software issues.

### 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

### 3. Important Notes about this Release

- This Identity Engines Service Pack 9.0.2 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).
- If you are running release 8.0.x and would like to migrate to 9.0.2, take a configuration backup from 8.0.x, deploy a new 9.0.2 VM and perform a configuration restore on the 9.0.2 VM.
- If you are running release 9.0.0 or 9.0.1 and would like to migrate to 9.0.2, you have two options:
  - Take a configuration backup from 9.0.0 or 9.0.1, deploy a new 9.0.2 VM and perform a configuration restore on the 9.0.2 VM. New licenses will be required.
  - Perform an upgrade directly from 9.0.0 or 9.0.1 to 9.0.2 using the pkg files.

- 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 9.0.2:

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.

### **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 9.0.2

File Name	Module or File Type	Comments
AIEIS_RHEL_6_3_LINUX-VM_09_00_02_026940_x86_64.ova	Ignition Server OVA files for vSphere 5.x environment	Ignition Server release 9.0.2. This file is used if fresh VM install option is desired.
LINUX-VM_09_00_02_026940_server_complete.pkg	Ignition Server upgrade package files for vSphere 5.x environment	Ignition Server release 9.0.2. These files are used if upgrade option is desired.
DashboardInstaller-9.0.2.26940.exe	Dashboard Installer	Dashboard Installer release 9.0.2 compatible with Ignition Server release 9.0.2

### Identity Engines software file names of Release 8.x and 9.x that are compatible for deployment in conjunction with Identity Engines Release 9.0.2

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 9.0.2
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 9.0.2
GuestManagerInstaller-9.0.0.25816.exe	Guest Manager installer	Bug Fixes and compatibility with Ignition server release 9.0.2

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 9.0.2 software can only be managed with Avaya Ignition Dashboard release 9.0.2.

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

Software	Software Compatibility	Comments
Ignition Server	<ul style="list-style-type: none"> <li>VMware ESXi versions 5.0 or 5.1 or 5.5</li> <li>Installation on a VMware ESXi server is done using an OVA file which already incorporates the OS Red Hat Enterprise Linux.</li> </ul>	<ul style="list-style-type: none"> <li>The VM requires a x86_64 capable environment</li> <li>Minimum 4 CPUs</li> <li>Minimum 4 GB of memory</li> <li>Minimum 260 GB available disk storage (thin provisioning is allowed)</li> <li>Minimum 1 physical NIC (preferably 3 NICs)</li> <li>3 Logical NIC cards</li> <li>VMware lists on its site supported hardware platforms for ESXi: <a href="http://www.vmware.com">http://www.vmware.com</a></li> </ul>
Access Portal	<ul style="list-style-type: none"> <li>VMware ESXi versions 4.0<sup>1</sup> or 4.1<sup>1</sup> or 5.0 or 5.1 or 5.5</li> <li>Installation on a VMware ESXi server is done using an OVF file which already incorporates the OS FreeBSD.</li> </ul>	<ul style="list-style-type: none"> <li>The VM requires 32-bit capable environment</li> <li>Minimum 2 CPUs</li> <li>Minimum 2 GB of memory</li> <li>Minimum 10 GB available disk storage</li> <li>Minimum 2 physical NIC (preferably 3 NICs).</li> <li>VMware lists on its site supported hardware platforms for</li> <li>ESXi: <a href="http://www.vmware.com">http://www.vmware.com</a></li> </ul>
Ignition Dashboard	<ul style="list-style-type: none"> <li>Windows XP sp3 (32 bit)<sup>2</sup></li> <li>Windows 7 (32 bit or 64 bit)</li> <li>Windows 8 (32 bit or 64 bit)</li> <li>Windows Server 2003 (32 bit or 64 bit)<sup>3</sup></li> <li>Windows Server 2008 (32 bit or 64 bit)<sup>4</sup></li> </ul>	<ul style="list-style-type: none"> <li>Minimum 2GB RAM memory</li> <li>US English Windows</li> </ul>
Guest Manager	<ul style="list-style-type: none"> <li>Windows XP sp3 (32 bit)<sup>2</sup></li> <li>Windows 7 (32 bit or 64 bit)</li> <li>Windows 8 (32 bit or 64 bit)</li> <li>Windows Server 2003 (32 bit or 64 bit)<sup>3</sup></li> <li>Windows Server 2008 (32 bit or 64 bit)<sup>4</sup></li> </ul>	<ul style="list-style-type: none"> <li>Minimum 2GB RAM memory</li> <li>US English Windows</li> </ul>
CASE Manager	<ul style="list-style-type: none"> <li>Windows XP sp3 (32 bit)<sup>2</sup></li> <li>Windows Server 2003 (32 bit)<sup>3</sup></li> <li>Windows Server 2008 (32 bit and 64 bit)<sup>4</sup></li> <li>Microsoft IE version 6.0 or later</li> <li>Firefox version 1.5 or later</li> </ul>	<ul style="list-style-type: none"> <li>Minimum 2GB RAM memory</li> <li>US English Windows</li> </ul>
Analytics	<ul style="list-style-type: none"> <li>Windows XP sp3 (32-bit)<sup>5</sup></li> <li>Windows Server 2003 (32-bit)<sup>6</sup></li> <li>Windows Server 2008 (32-bit)<sup>7</sup></li> <li>Windows must have NTFS file system partition</li> </ul>	<ul style="list-style-type: none"> <li>Minimum CPU 2+ GHz processor</li> <li>Minimum 2GB of memory</li> <li>Minimum 3GB available drive storage</li> <li>The hard drive space requirement above is only for the installed application. Be sure to</li> </ul>

	<ul style="list-style-type: none"> <li>• Microsoft IE Browser</li> <li>• Firefox Browser</li> </ul>	<p>increase the hard drive space based on storage requirements for data logs and level of application usage.</p> <ul style="list-style-type: none"> <li>• US English Windows</li> </ul>
Avaya Flare	Avaya Flare release 1.2 for iPad Avaya Communicator release 2.0 for iPad	<ul style="list-style-type: none"> <li>• Compatible with Identity Engines R9.0.1 SSO</li> </ul>
Avaya System Manager	Avaya SMGR release 6.2 FP3	<ul style="list-style-type: none"> <li>• Compatible with Identity Engines R9.0.1 SSO</li> </ul>
Service Provider Agent	Apache Tomcat 6.X	<ul style="list-style-type: none"> <li>• Compatible with Identity Engines R9.0.1 SSO</li> <li>• Any servlet container compliant with the Servlet API specifications version 2.4 or higher will work, like Tomcat 6.x, JBoss or Websphere</li> </ul>

**Notes for Identity Engines OVA/OVF VMware ESXi versions**

<sup>1</sup> Release 9.0.2 is last release to support Access Portal on ESX 4.x versions

**Notes for Dashboard/CASE Manager/Guest Manager Windows versions**

<sup>2</sup> Release 9.0.2 is last release to support Dashboard/CASE Manager/Guest Manager on Windows XP versions

<sup>3</sup> Release 9.0.2 is last release to support Dashboard/CASE Manager/Guest Manager on Windows 2003 versions

<sup>4</sup> Release 9.0.2 is last release to support Dashboard/CASE Manager/Guest Manager on Windows 2008 32-bit

**Notes for Analytics Windows versions**

<sup>5</sup> Release 9.0.2 is last release to support Analytics on Windows XP versions

<sup>6</sup> Release 9.0.2 is last release to support Analytics release 8.0.0/8.0.1 on Windows 2003 (32-bit)

<sup>7</sup> Release 9.0.2 is last release to support Analytics release 8.0.0/8.0.1 on Windows 2008 (32-bit)

Please note that Analytics with support for Windows 7 (64-bit) and 2008 (64-bit) versions is planned

## **7. Version of Previous Releases**

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**

### **New features in This Release**

#### **UserNameAttribute Enhancement for Active Directory**

##### *Synopsis*

UserNameAttribute enhancement is an Active Directory Service enhancement to provide flexibility to choose different User Object attribute as User Naming attribute for non-NTLM and NTLM authentications in Active Directory. It is useful when a customer would like to use attribute other than sAMAccountName for authentication such as User Principal Name (UPN). It is particularly useful for IDE SSO support with SMGR (System Manager) where customer can use attribute other than sAMAccountName for authentication such as User Principal Name (UPN).

## Constraints

NTLM authentication will have the restriction of followings:

- MSCHAP and MSCHAPv2 authentications can use only following User Object Attributes as User Naming Attribute:
  1. UserPrincipalName
  2. sAMAccountName
  3. ObjectGUID
  4. ObjectSid
  5. sIDHistory

Typically, only UPN and sAMAccountName are used for authentication.

## 8.1. Problems Resolved in This Release

Work item Number	Description
<b>wi01179620</b> <b>wi01190221</b>	Importing of 8.0.x backup configuration to 9.0.0 or 9.0.1 failed with "Access Not Allowed" in Dashboard due to custom VSA conflicting with new default 9.0 attributes.
<b>wi01182928</b>	ECP client is not working with short FQDN
<b>wi01172381</b>	SOAP server debug log enabled by default which could results in disk space exhaustion
<b>wi01180020</b>	OpenSSL Security Advisory [05 Jun 2014] CVE-2014-0224 and other
<b>wi01178645</b>	"Device VLAN" is not returned to authenticator despite successful authentication
<b>wi01178675</b>	Unable to restore configuration file that contains duplicate directory server entries with different directory service type
<b>wi01184074</b>	Flood of "Device attribute VLAN unexpected" warning message in syslog
<b>wi01185242</b>	OpenSSL Security Advisory [6 Aug 2014] CVE-2014-3511 and others
<b>wi01185699</b>	Identity Engines 9.0.0 and 9.0.1 database corruption causing newly added outbound attributes cannot be used
<b>wi01190688</b>	CVE-2014-7169 bash environment variable code injection; aka ShellShock
<b>wi01179781</b>	MAC authentication fails when "Trapeze" vendor is being used

## 8.2. Outstanding Issues

Work item Number	Description
<b>wi01038838</b>	Guest Manager email notification notes are not sent when users are first created. They will show up if you resend the notification
<b>wi01132335</b>	Identity Engines Access Portal requires a reboot after deleting a firewall rule
<b>wi01170515</b>	Access Portal disabling "HTTPS Login" ineffective until reboot
<b>wi01170525</b>	Access Portal - Captive Portal returns HTTP 500 Response for various reasons
<b>wi01174482</b>	Ignition Server syslog message is not RFC 3164 compliant
<b>wi01180963</b>	Dashboard stuck in "Upgrade In Progress" loop during Ignition Server RADIUS "Initializing"
<b>wi01185244</b>	Identity Engines MAC authentication does not work when using Calling Station ID by default for Aruba WLAN controller
<b>wi01189183</b>	Identity Engines Access Portal 8.0 locks up during high volume of traffic

wi01190614	New VLAN attribute is not sent back to the authenticator while MAC authentication
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	<p><b>When the connection between Dashboard sys-admin session and Ignition Server is lost, sys-admin cannot login to dashboard again</b></p> <p>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.</p> <p>As a work around,</p> <ul style="list-style-type: none"> <li>login to console or open a SSH connection (must have previously enabled SSH on the Dashboard) to Ignition Server and run 'show sessions' command</li> <li>Note down the 'Id' of the session entry for sys-admin</li> </ul> <p>Run 'session delete id &lt;id&gt;' to clear the stale session and the sys-admin can now login to the Dashboard</p>
wi01151857	<p><b>Not able to associate internal users with internal devices</b></p> <p>While adding internal users to the Ignition Server, internal devices could also be mapped to each user which can then be used in the authorization policies. However, this operation although shows successful, the mapping is lost when we try to view the user details.</p> <p>As a work around, the same association can be mapped by associating the internal device with the internal user (instead of internal user with internal device).</p>
wi01126383	<p><b>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</b></p> <p>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.</p>
wi00852520	<p><b>One node IP address was truncated after breaking and creating HA multiple times from Dashboard</b></p> <p>This issue is seen occasionally after breaking and creating HA multiple times. This issue does not affect any functionality.</p> <p>As a work around, users can logout and re-login to the Dashboard to fix the issue</p>

### 8.3. Known Limitations

Work item Number	Description
wi01121113	<p><b>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</b></p> <p>Underscore is not considered a valid character for DNS hostname. Only following characters are allowed for DNS hostnames:</p> <ul style="list-style-type: none"> <li>Alphabets, Numeric, Hyphens</li> </ul>
wi01119478	<p><b>IdP summary shows two entries in HA even though SAML service is bound to VIP</b></p> <p>In HA, if DNS configuration is not valid or not reachable on either of the HA nodes, then SSO configuration will not be valid.</p>

	<b>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.</b>
wi01127410	<p><b>While restoring large configuration, system takes additional 4-5 minutes for all the SSO services to come up</b></p> <p>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.</p> <p>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</p>
wi01155806	<p><b>After session timeout triggers from Dashboard, session is not cleared from Ignition Server side immediately. It will take 30sec to 1 minute to clear</b></p> <p>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.</p>

## 9. Upgrade procedure

### Pre-upgrade Checklist from Ignition Server

#### *Ignition Server*

- Note that by design, users cannot upgrade an existing 8.0.x or earlier VM to 9.0.2 VM using software upgrade procedure
- Existing 8.0.x, 9.0.0 and 9.0.1 configurations can be migrated to 9.0.2 using the backup & restore functionality. Restore of configuration data on 9.0.2 release can only be performed from the following versions:
  - Backup of 8.0.x (or 9.0.1) configuration data
  - If you're running version older than 8.0.x and would like to upgrade to release R9.0.1, first perform an incremental upgrade to 8.0.x release and then use backup & restore functionality to migrate your existing configuration to 9.0.2 VM
  - Please contact Avaya support if you will need temporary licenses for IDE R8.0 for this process of incremental migration of your configuration to IDE release 9.0.2.
- Existing 9.0.1 can be migrated to 9.0.2 using one of the following two options:
  - Take a configuration backup from 9.0.1, deploy a new 9.0.2 VM and perform a configuration restore on the 9.0.2 VM. New licenses will be required.
  - Perform an upgrade directly from 9.0.1 to 9.0.2 using the "pkg" files.

#### *Dashboard*

- Identity Engines 9.0.2 also includes a new Dashboard installer that must be installed. Ignition Server release 9.0.2 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\\Application Data\Avayalsecurity**

Win 7

**C:\Users\\AppData\Roaming\Avaya\security**

Win 8

C:\Users\\AppData\Roaming\Avaya\security

**Delete these directories from your system before launching the new Dashboard**

**Note that these folders may be hidden folders.**

- 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 9.0.2 release for these applications.

## Software Upgrade Procedure

The following upgrade procedure is only applicable for customers who are upgrading from 9.0.1 to 9.0.2 release.

- There's no change in the license model and customers with 9.0.1 licenses can continue to use them on 9.0.2 software
- Take a backup of entire VM using the VMware Backup or snapshot utility prior to the upgrade.
- Take a backup of the policy configuration data from the Dashboard
- Export and save your licenses
- Release 9.0.2 includes a new Dashboard installer. Close any running Dashboard instances and install new 9.0.2 Dashboard
  - You must have Administrator Rights in order to install the Dashboard
- From the 9.0.2 Dashboard, upgrade the Ignition Server to release 9.0.2 as mentioned in the 'Ignition Server – Administration Guide section 'Activating a firmware Image or Package'
- Release 9.0.2 Ignition Software will continue to work with 8.0.0 versions of Access Portal, CASE Administration, and Guest Manager and Analytics software.
- The installed 9.0 licenses will be retained after the upgrade to 9.0.2.

## 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>.



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/](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/>