

Avaya Identity Engines Release Notes

Software Release 8.0

1. Release Summary

Release Date: June 2012

Purpose: Software major release to introduce new feature enhancements and to address customer found software issues.

2. Important Notes before Upgrading to This Release

Avaya provides the Identity Engines Ignition Server and Ignition Access Portal as Virtual Appliances. Do not install or uninstall any software components on these Virtual Appliances unless Avaya specifically provides the software and/or instructs you to do so. Also, do not modify the configuration or the properties of any software components of the VMs (including VMware Tools) unless Avaya documentation and/or personnel specifically instruct you to do so. Avaya does not support any deviation from these guidelines.

Identity Engines Software Upgrade Requirements:

In order to maximize configuration compatibility during upgrade, Avaya does not recommend upgrading directly from release prior to 7.0.0. If you are using the software prior to 7.0.0, you must upgrade to release 7.0.0 first and then proceed with upgrade to 8.0. It is not required to upgrade from 7.0.0 to 7.0.1 or 7.0.2 before upgrading to 8.0.

As a good practice, Avaya recommends that you perform a backup of your configuration as well as an export of your licenses before you begin any software upgrades. Also, write down the Serial Numbers of your Ignition Servers.

Please refer to 7.0.x Release Notes to upgrade the system from 6.0.1 to 7.0.x.

Saved Configuration File Compatibility

In order to maximize configuration compatibility during upgrade, Avaya does not recommend performing configuration backup/restore from release prior to 7.0.x.

3. Platforms Supported

VMware vSphere version 4.0

VMware vSphere version 4.1

VMware vSphere version 5.0

Note that vMotion, VMware Player and VMware Workstation are not supported and cannot be used in conjunction with neither the Ignition Server nor the Ignition Access Portal.

4. Notes for Upgrade

File Names for This Release

File Name	Module or File Type	File Size (bytes)
AIEIS_RHEL_5_5_LINUX-VM_08_00_00_022931_x86_64	OVF files for vSphere 4.x/5.0 environment	991136515
LINUX-VM_08_00_00_022931_server_complete.pkg	Upgrade Package	150119136
DashboardInstaller-8.0.0.22931.exe	Dashboard Installer	88169015
GuestManagerInstaller-8.0.0.22931.exe	Guest Manager Installer	88878805
AdminConsoleInstaller-1.0.0.22931.exe	Admin console Installer	87219260
AccessPortal_01.00.00_022931_x86_32	OVF files for Access Portal	79801978

System Requirements

Software	System Requirements	Comments
Ignition Server	<ul style="list-style-type: none"> VMware ESXi versions 4.0 or 4.1 or 5.0 Installation on a VMware ESXi server is done using an OVF file which already incorporates the OS Red Hat Enterprise Linux. 	<ul style="list-style-type: none"> The VM requires a x86_64 capable environment Minimum 2 CPUs Minimum 2 GB of memory Minimum 30 GB available disk storage 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	<ul style="list-style-type: none"> VMware ESXi versions 4.0 or 4.1 or 5.0 Installation on a VMware ESXi server is done using an OVF file which already incorporates the OS FreeBSD. 	<ul style="list-style-type: none"> The VM requires a x86_64 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
Dashboard	<ul style="list-style-type: none"> Windows XP sp3 (32 bit) Windows 7 (32 bit or 64 bit) Windows Server 2003 (32 bit or 64 bit) Windows Server 2008 (32 bit and 64 bit) 	<ul style="list-style-type: none"> Minimum 2GB RAM memory
Guest Manager	<ul style="list-style-type: none"> Windows XP sp3 (32 bit) Windows Server 2003 (32 bit and 64 bit) Windows Server 2008 (32 bit and 64 bit) Microsoft IE version 6.0 or later Firefox version 1.5 or later 	<ul style="list-style-type: none"> Minimum 2GB RAM memory
CASE Administration	<ul style="list-style-type: none"> Windows XP sp3 (32 bit) Windows Server 2003 (32 bit) Windows Server 2008 (32 bit) Microsoft IE version 6.0 or later Firefox version 1.5 or later 	<ul style="list-style-type: none"> Minimum 2GB RAM memory
Analytics	<ul style="list-style-type: none"> Windows XP sp3 32-bit Windows Server 2003 32-bit Windows Server 2008 32-bit 	<ul style="list-style-type: none"> Minimum CPU 2+ GHz processor Minimum 2GB of memory Minimum 3GB available drive storage

	<ul style="list-style-type: none"> • Windows must have NTFS file system partition • Microsoft IE version 6.0 or later, running on Windows • Firefox 1.5 or later, running on Windows 	<ul style="list-style-type: none"> • 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.
--	---	--

5. Version of Previous Releases

Software Version 7.0.0, Release Date – Dec 13th 2010

Software Version 7.0.1, Release Date – Mar 31st 2011

Software Version 7.0.2, Release Date – Sep 30th 2011

6. Compatibility

This software release can only be managed with Avaya Ignition Dashboard release 8.0.

7. Changes in This Release

7.1. New Features in This Release

Avaya Identity Engines Ignition Access Portal with Device Profiling

Ignition Access Portal is a virtual machine based captive portal and firewall distribution that controls the access of client devices to the network. The Access Portal blocks all traffic from client devices and allow network access only after successful authentication. Access Portal allows guests with non-802.1X compatible devices to authenticate and connect to the network in your organization.

Device Profiling works on a Device Fingerprint which is a compact summary of software and hardware settings collected from a client device. In the Identity Engines environment, Device Profiling is used as an automated way to register the devices with the Identity Engines Internal Store. The Access Portal contains the intelligence to discover the device attributes.

Avaya Identity Engines CASE Client & Administrative Console

The Avaya Identity Engines Ignition Client for Accessing Secure Enterprise (CASE) feature grants network access to devices and users. CASE automatically verifies and corrects wired and wireless configuration on Windows endpoint machines, automating the client configuration required to enable 802.1x and Microsoft Network Access Protection (NAP).

CASE includes:

- CASE Administrative Console (for the network administrator)
- CASE Client (for the end-user)

CASE Administrative Console

The Ignition CASE Administrative Console is a web-based application. The network administrator uses the CASE Administrative Console to build a configuration that specifies the end user settings for specific network access. This configuration is called a network profile. Network administrators can define multiple network profiles, each with its own configuration and behavior settings. The network administrator then builds CASE deployment packages that contain one or more network profiles and deploys these packages directly to Access Portal.

CASE Application

The CASE Application is an application that guides a user while it applies the settings the network administrator configured for the network access. The first time the end user connects to the network, they are presented with a link to the CASE Client (or the CASE Client automatically launches). If the end user agrees to the terms and conditions presented by the Enterprise, the CASE Client runs and automatically sets up the end user's network configuration.

RADIUS Proxy

In release 8.0, Avaya Identity Ignition Server introduces an enhancement called Radius Proxy.

With Radius proxy, the Avaya Ignition Server can be made to act as a Radius Client and forward (or proxy) certain requests to another designated Radius Server. The choice of which requests to be forwarded is based on the authentication "realm".

Avaya Ignition Server can function both as a forwarding server and a remote Radius server, serving as a forwarding server for some 'realms' and a remote server for other realms.

Guest Manager Enhancement

Release 8.0 introduces a new Guest Manager enhancement for import/export of Guest Manager Configuration. This feature enables the user to port Guest Manager Configurations between multiple Guest Manager deployments.

The import/export of configuration includes:

- Appliance Configurations.
- Radius configurations.
- User Certificates.
- Tomcat Configurations (HTTP, SSL etc).
- User Preferences

Bulk Load of Authenticators

Release 8.0 introduces the facility to bulk load Authenticators data from a CSV file.

7.2. Old Features Removed From This Release

Avaya Identity Engines Ignition Server Release 8.0 no longer supports ESX 3.5 environment. The Ignition Server can now only be deployed on VMWare vSphere 4.0, 4.1 and 5.0 versions.

If you're currently running Ignition Server 7.0.x release in ESX 3.5 environment, the following must be followed:

- Upgrade the Ignition Server software from 7.0.x to 8.0 release using the [upgrade procedure](#) mentioned below.
- Then upgrade your VMware environment from ESX 3.5 to the vSphere 4.0 or above environment using the VMware migration tools
- Alternatively, take a backup of configuration from the 7.0.x setup. Deploy a new Ignition Server VM on ESX 4.x/5.0 server and perform restore of 7.0.x configuration on the 8.0 Server. Note that you will need to obtain a trial license in order to be able to be back in services in a short time as the process for receiving a new permanent license may take a few days.

7.3. Problems Resolved in This Release

Work item Number	Description
wi00852604	Issue with clock sync between Active Directory Server with Ignition Server

	<p>When Ignition Server connects to an Active Directory Server, the Ignition Server must be in sync with the clock on the Active Directory Server. The periodic NTP sync operation on the Ignition Server was not being called due to which the Ignition Server could not sync with the NTP Server.</p> <p>This issue is fixed in 8.0 so that the Ignition Server will now try to sync with the NTP server every 60 minutes</p>
wi00861651	<p>After upgrade to 7.0.1 release with 'halt' operation, if the user manually tries to 'reboot', the system still goes to 'halt'</p> <p>The 'halt' status which is initially set after the upgrade is not getting cleared after the upgrade. This issue has been corrected in release 8.0</p>
wi00852597	<p>Failed to restore blank password data with ***** HA SETUP ERROR (Configuration Restore) ***** Secondary node does not have HA-role as Secondary</p> <p>In HA setup, when both nodes are not in fully synchronized state, certain operations like restore cannot be performed until both nodes are fully synchronized</p>
wi00852608	<p>Radius service is restarted due to load testing</p> <p>Exception handling for the incoming radius requests has been corrected in release 8.0 so that the Radius service doesn't crash under heavy load</p>
wi00852602	<p>RSA Agent library uses system calls to ps and netstat which can cause defunct process</p> <p>Changes to RSA Agent library to provide thread safe calling of sub-process is now included in release 8.0.</p>
wi00941231	<p>One of the node loses the license after breaking the HA</p> <p>In release 8.0, data synchronization between the nodes in HA has been improved so that the node doesn't lose any license info once the HA is broken</p>
wi00572310	<p>Default gateway not always restored after upgrade in a HA scenario</p> <p>Modified the routing module to correctly handle the route change events from the kernel. Also modified the logging mechanism so that the Ignition Server will now correctly report whether a route has been added/deleted in the kernel routing table and reason code in case the route updation fails</p>
wi00999491	<p>On 64-bit systems, while installing Guest Manager 8.0, installer doesn't force the user to Uninstall older GM installation.</p> <p>Corrected the install procedure to detect the previous installations of Guest Manager and let the user uninstall the previous version before installing the new GM installation on 64-bit systems</p>
wi00983264	<p>Add support to pass outbound_framed_ip_address in string format</p> <p>Currently the LDAP IP address attribute is in int format. It's been modified to support string format as well. while mapping the value of a virtual user attribute of type IPv4 address.</p>
wi00982777	<p>Populate NapSohAVProdInfo and NapSohASProdInfo to the transaction log export</p> <p>Currently, Transaction log file does not write Anti-virus and anti-spyware info received through NAP posture information. It only writes FW info the transaction log.</p> <p>The transaction logs have been updated in release 8.0 to include Anti-Virus and Anti-Spyware information</p>
wi00981017	<p>Log Export function crashes when enabling Access Details export logs under Site>logging</p> <p>While exporting access details logs that include NAP posture information, log export fails. This is happening due to accessing of null data while writing access details log. This is fixed in release 8.0 by using the right parameters for writing access details log.</p>
wi00980632	<p>Ignition Server froze and needed rebooting Two issues have been noticed at the site 1) SLogExport process crashing continuously 2) High number of defunct process not cleaned up</p> <p>The issue is addressed in release 8.0 by fixing the Log Export function crash (wi00981017) and by adding a timer task to clean up defunct processes periodically.</p>
wi00974950	<p>password-expiration = 13405530045032358810 in the access log under device details.</p> <p>Display log of Password-expiration value in the access log is corrected in release 8.0</p>

wi00964751	<p>NAP is not working with EAP-PEAP/TLS when crypto-binding is enabled</p> <p>The problem was happening as the Ignition Server was assuming that the inner method is always PeapMschapV2. Modified to use the appropriate session for generating InnerSession Key.</p>
wi00952904	<p>After restoring the configuration, HA lost the license</p> <p>The issue is addressed in 2 ways. One, as explained below, the 2nd node which cleans up its database and waits to sync with the 1st master, will be in client status until sync is complete. That'll avoid the scenario when it becomes the master and it doesn't have any config data. Other behavior is, once the restore is complete and both nodes come up after a reboot, each node reads the database and updates its radius run time cache. If the config database is large, the updation might take some time. During this time, if Dashboard is connected and asks for Radius data, it can get exception. This issue is also handled by adding dependency in the process init functionality so that users will not be able to connect to the dashboard unless all the services are up.</p>
wi00898683	<p>NAP posture checking don't work with non Windows systems even though non-NAP allow rule is in place</p> <p>Non-Windows client like Ubuntu or MAC OS running in to a NAP enabled rule fail with "No valid posture license" even though a non-NAP-allow definition is in place. This issue is happening as the non-windows clients use PEAPv1 for authentication and Ignition Server treats this as a TNC posture check and looks for a TNC license. The issue is addressed in 8.0 by correctly treating the requests as NAP posture check and validating against NAP posture license</p>
wi00573426	<p>Get error message in Dashboard logs saying OPSWAT download of files failed</p> <p>In release 8.0, we no longer support TNC posture check. Hence the periodic check of downloading OPSWAT files is disabled and the logs are no longer displayed</p>

8. Upgrade procedure

Pre-upgrade Checklist for Ignition Server

- Upgrades can only be performed from the last major version or maintenance releases of the same major version. For example, upgrade to 8.0 can only be performed from 7.0.x and not 6.0.x.
- Once the Ignition Server is upgraded to a major version, it cannot be downgraded. It is highly recommended to:
 - Take a backup of the configuration
 - Take a back of the entire VM so that user can revert to the backed up VM if needed.
 - Export and save your licenses
 - Record in a safe place the Serial Number of your existing Ignition Servers.
- Ignition Server is partitioned to store **no more than 2 versions** in the boot partition. If your Ignition server has been upgraded multiple times, it's mandatory that you **delete the oldest software versions** prior to upgrading to 8.0 so that no more than 2 images are displayed under the Images tab before package activation is initiated.
 - To delete previous versions, login to **Dashboard → Configuration → Site → Actions → Upgrade Systems → Image**. Select the oldest software first and 'Delete'. Repeat the same to delete additional versions.
- When upgrading the Ignition Server to a major version (for example, 7.0 to 8.0), all the Ignition components like Ignition Dashboard, Ignition Guest Manager, Ignition Analytics must also be upgraded.
- Users should never update VMware Tools or modify the configuration or the properties of Avaya provided Virtual Appliances which include Ignition Server and Access Portal. Avaya does not support upgrading of VMware tools or any other software components unless the upgrade package is provided by Avaya.

- If you have already updated VMware tools or unsure, stop the upgrade and follow the procedure given below.
 - Take a backup of configuration from your existing VM's
 - Deploy a new Ignition Server & Access Portal using the OVF
 - Install the necessary licenses
 - Restore the configuration

Upgrade Procedure

This upgrade procedure is only applicable for those who're upgrading from 7.0.x to 8.0 release or between 8.0 loads. If you're running any older version and would like to upgrade to 8.0, you must first upgrade to 7.0.x release. Refer to the Release Notes of the Identity Engines 7.0.x release for more information on licensing requirements & upgrade procedure.

Follow the instructions given below before proceeding with the upgrade.

- Customers with appropriate support contract which entitles them to receive the software upgrade, contact Avaya and make a request for an upgrade of your license from 7.0 to 8.0 license:
 - Send an email request to idengines@avaya.com
 - Include the Serial Numbers of your existing Ignition Servers
 - Make sure you provide details as to which servers are in HA configuration
 - Make sure you provide information as to which other licenses you have installed (e.g. Guest Manager, MS-NAP etc).
- Take a backup of entire VM using the VMware Backup utility prior to the upgrade.
- Take a backup of the policy configuration data from the Dashboard
- Export and save your licenses.
- From the Dashboard, upgrade the Ignition Server to release 8.0 as mentioned in the '*Ignition Server – Administration Guide section Activating a firmware Image or Package*'
- Once the Server is upgraded, close the Dashboard and install 8.0 Dashboard
 - *You must have Administrator Rights in order to install the Dashboard*
 - *Ignition Server 8.0 cannot be managed from a 7.0.x Dashboard.*
 - *Note that 8.0 Dashboard upgrades the Java platform to JRE release 6 update 27*
- Release 8.0 Ignition Software will not work with any previous versions of Guest Manager and Analytics software. All the associated components must be upgraded as well.
- Upgrade Guest Manager & Analytics to release 8.0
 - *Note that Guest Manager 8.0 will also install/upgrade the Apache Tomcat Web server 6.0.29 as well as the JRE release 6 update 27*
- If installing the 8.0 Guest Manager over an existing Guest Manager version or installing on a system where another instance of Tomcat web server is running, note that the GM 8.0 would install a new instance of Tomcat web server 6.0.29

- To avoid any conflicts while running multiple instances of web server on the same system, select a different port number while installing the Tomcat web server
- Once all the components are upgraded, connect to the Dashboard and install a new 8.0 license. If the new license is not installed, the Ignition Server continues to run for a grace period of 30 days after which the Ignition Server would stop running
 - Grace period is only applicable if you're upgrading from a previous major release (7.0.x) to a new major release (8.0)
- To use the newly introduced Avaya Identity Engines Ignition Access Portal and Ignition CASE Client, order a SMALL or LARGE FEATURE_PORTAL license.

9. New Outstanding Issues

Work item Number	Description
wi00977909	<p>While restoring large database in a HA setup, restore status on the 2nd node may be stuck at 'syncing config...'</p> <p>While performing restore of a large configuration (more than 100,000 records), the 2nd node may sometimes gets stuck at 'syncing config'. The primary node continues to work and handle any configuration changes.</p>
wi00978646	<p>Client certificate was not installed when deploying no-admin network profiles on all Window OS</p> <p>The generic user certificate will not be installed in the right key-store if the user trying to execute CASE does not have administrative rights. The privilege level for CASE needs to be raised by providing the administrator credentials if the user does not have admin rights. In this condition, the CASE will install the user certificate in the personal key store of administrator.</p>
wi00978524	<p>After Uninstalling GM on 64 bit windows XP machine registry entries are not get removed from x86 Microsoft –windows-current version-Uninstall</p> <p>When the user tries to uninstall Guest Manager installation from a 64-bit Windows XP machine, some of the registry entries are not cleaned up. However, this will not have any impact on the system</p>
wi00977445	<p>Should display a warning message if not able to install client certificate after installing CASE on clients</p> <p>While deploying CASE on the client PC that includes client certificates, currently there's no alert message displayed if the installation of client certificate fails. Users have to look at the logs to check the result</p>
wi00977199	<p>Able to add duplicate radius proxy services with same IP address under Directory services</p> <p>In release 8.0, while adding radius proxy service, currently there's no validation of multiple proxy services of same IP addresses are added. However, the validation will work if the user tries to use the same proxy service name.</p>
wi00965938	<p>It takes quite a long time around 40s to Install Active X on Windows</p> <p>While installing Active-X version of CASE client on windows clients, it takes about 40 seconds for the installation to complete</p>
wi00953222	<p>Directory Root DN is not discovered automatically when adding Novell and Oracle internet directory service</p> <p>If Novell or Oracle Internet Directory services are configured, the directory Root DN is not discovered automatically like that of Active Directory. Users have to manually add the Root DN information</p>
wi00978520	<p>After Uninstalling Dashboard on 64 bit windows XP machine, certain registry entries are not get removed from Microsoft –windows-current version-Uninstall & Local machine-Software-Avaya-Dashboard</p>

	When the user tries to uninstall Dashboard installation from a 64-bit Windows XP machine, some of the registry entries are not cleaned up. However, this will not have any impact on the system
--	---

10. New Known Limitations

Work item Number	Description
wi00989301	<p>The clients are not redirect to the login page if there are some issues with the connectivity between Access Portal and Radius Server.</p> <p>This issue can happen when connectivity between Access Portal and Ignition Server is lost for some time due to network congestion / RADIUS server not responding. Workaround for the client is to retry the HTTP request after 10-15 seconds again.</p>
wi00958605	<p>Proxy forwarded requests information are not showing under Access/Debug logs.</p> <p>Release 8.0 supports Radius Proxy support wherein Ignition Server can forward/proxy incoming authentication/accounting requests to a remote Radius Server. Since the remote server handles all the authentication/authorization, no logs about the proxy are shown on the forwarding server. Alternatively, use the Monitor → Node → Protocols → RADIUS statistics to check how many packets have been forwarded to/received from proxy.</p>
	<p>Cannot add default route from Access Portal console</p> <p>Access Portal console does not have any configuration option to add default route. User can only configure ADMIN IP address from the console and then access the Portal's WebUI to configure default route or any other static routes. The same has been clarified in the Access Portal administration guide.</p>

1. 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/>