

Avaya Identity Engines Release Notes

Software Release 8.0.2

NN47280-400

1. Release Summary

Release Date: June 2013

Purpose: Software minor release 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 complete 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.
 - 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.
- 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. You may need to obtain new licenses in case you have created a new instance of the Ignition Server(s).
 - Restore the configuration
- Ignition Server is partitioned to store **no more than 3 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 8.0.2 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.

Identity Engines Software Upgrade Requirements:

In order to maximize configuration compatibility during upgrade, Avaya does not support upgrading directly from release prior to 8.0.0. If you are using the software prior to 8.0.0, you must upgrade to release 8.0.0 first and then proceed with upgrade to 8.0.2.

As a good practice, Avaya recommends that you take a VMware snapshot of your VM, 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 8.0.0 Release Notes to upgrade the system from 7.0.x to 8.0.0.

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_02_024535_x86_64.mf	OVF files for vSphere 4.x/5.0 environment	199
AIEIS_RHEL_5_5_LINUX-VM_08_00_02_024535_x86_64.ovf		35900
AIEIS_RHEL_5_5_LINUX-VM_08_00_02_024535_x86_64.vmdk		990038016
LINUX-VM_08_00_02_024535_server_complete.pkg	Upgrade Package	150269778
DashboardInstaller-8.0.2.24535.exe	Dashboard Installer	88184004

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
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

5. Version of Previous Releases

Software Version 8.0.1, Release Date – October, 2012

6. Compatibility

This software release can only be managed with Avaya Ignition Dashboard release 8.0.2.

7. Changes in This Release

7.1. Problems Resolved in This Release

Work item Number	Description
wi01079258	<p>WPA keys not forwarded to the client authenticator when Ignition Server used as Proxy Radius Server</p> <p>In a wireless environment with Ignition Server acting as Radius Proxy Server, VSA's like MS_MPPE_RECVKEY_ATTR and MS_MPPE_SENDKEY_ATTR sent by the end Radius Server are not forwarded back to the WLAN Controller.</p> <p>Fixed this issue in release 8.0.2 so that VSA's are forwarded correctly by the Proxy Server</p>
wi01092894	<p>Outbound attribute based on device VLAN information is not sent in the Radius response when performing MAC authentication</p> <p>Device VLAN information includes VLAN-ID and VLAN label. When the user configures an outbound attribute based on the device VLAN information, the data is not formatted which causes the attribute not being sent in the response.</p> <p>Corrected the formatting of device VLAN information and the data is now sent correctly in the response</p>
wi01051129	<p>With user authentication disabled and only MAC authentication enabled on the Ignition Server, Radius process restarts intermittently when Ignition Server receives Radius user authentication requests.</p> <p>Some authenticators like ERS support checking Radius server reachability using Radius requests. When Ignition Server receives these requests, it tries to process the requests even though user authentication is disabled and it causes intermittent radius process crashes.</p> <p>Fixed this issue in release 8.0.2 by ignoring radius requests when user authentication is disabled.</p>
wi01064919	<p>When doing device lookup through troubleshooting from Dashboard, the lookup operation throws an error even though the Device exists in the Ignition Server's internal store.</p> <p>Corrected the lookup process in release 8.0.2.</p>
wi01095891	<p>After installing 8.0.1 Ignition Server VM using OVF, users not able to upgrade to 8.0.2 release using 8.0.1 Dashboard</p> <p>To upgrade from 8.0.1 OVF to 8.0.2 release, first install the 8.0.2 Dashboard and then use the 8.0.2 Dashboard to upgrade the Ignition Server from 8.0.1 to 8.0.2.</p>
wi01053087	<p>Ignition Server sometimes takes longer time to power down when shutdown is initiated from Dashboard</p> <p>When shutdown process is initiated from Dashboard, the watchdog process on the Ignition Server waits up to 5 minutes until all Ignition Server processes are shutdown gracefully before actually shutting down the entire system. Watchdog sometimes gets invalid process count status even though all the processes are shutdown.</p> <p>Fixed the process count logic so that watchdog gets the right status when all the processes are shut down and the system shutdown is initiated immediately.</p>
wi01096786	<p>When downloading CRL information from a Web server using a virtual Web Server instance, Ignition Server doesn't include 'HOST:' field(FQDN) in the HTML request which causes the Web server to respond with '404: Host not found' and the download fails.</p> <p>Updated the HTTP library used for CRL retrieval functionality which sends the correct header format while sending HTTP requests.</p>

wi01102375	<p>Ignition Server not able to learn and register unknown device information as sent by Access Portal</p> <p>With device finger printing enabled, when a user tries to login to the Access Portal using an unknown device, Access Portal sends only partial data to the Ignition Server. Ignition Server treats this partial data as invalid and the device is not registered in its internal datastore.</p> <p>This issue is fixed this issue in 8.0.2 by registering the device successfully but skips the unknown device attributes.</p>
wi01048433	<p>Manual Refresh of CRL list throws an error message on the Dashboard even though the operation succeeds</p> <p>When trying to update the CRL list using 'Refresh' option from the Dashboard, the operation throws an error message 'Failed to refresh the CRL URLs'. The refresh operation doesn't set the status correctly even though it actually succeeded and the CRL list is updated.</p> <p>Fixed this issue in release 8.0.2.</p>
wi01048920	<p>MAC & EAP authentication not processed in right order while using wild card mac entries</p> <p>In some scenarios where the client machines does MAC authentication first and then do EAP-TLS, Ignition Server sometimes doesn't complete the MAC authentication and responds to EAP-TLS authentication which could put the hosts in incorrect VLAN's.</p> <p>This issue is seen when MAC authentication is performed against a wild card mac entry on the Ignition Server internal data store.</p> <p>Fixed this issue in release 8.0.2 by handling the MAC authentication properly.</p>

7.2. New Outstanding Issues

Work item Number	Description
wi01097935	<p>Ignition Dashboard has its own internal Daylight Savings library which doesn't reflect some of the recent DST changes in some countries</p> <p>Ignition Dashboard includes Java 2 Standard Edition Runtime Environment (JRE) 6 update 27 which has its own library for managing various time zones. Some countries have changed the way DST is implemented in their countries but the Java time zone library is not up-to-date with these changes.</p> <p>A workaround has been provided on how to update the java library. Please refer to the section "Time Zone update for Dashboard Java installation" in this document for more information about the time zone changes and the workaround to update the Java library.</p>

7.3. New Known Limitations

- None.

8. Upgrade procedure

Pre-upgrade Checklist for Ignition Server

- Note that by design, upgrades to minor or update releases can only be performed from the earlier releases of the same major version. For example, upgrade to 8.0.2 can only be performed from 8.0.x and not 7.0.x.

- Note that upgrade to 8.0.2 release can only be performed in the following scenarios:
 - Upgrade from 8.0.0 -> 8.0.2
 - Upgrade from 8.0.0 -> 8.0.1 -> 8.0.2
 - Upgrade from 8.0.1 -> 8.0.2
- Alternatively, users can deploy a new 8.0.2 Virtual Machine using the OVF and perform restore of older configuration data. Restore of configuration data on 8.0.2 release can only be performed in the following scenarios:
 - Backup of 7.0.x configuration data
 - Backup of 8.0.x configuration data
 - Note that you may be required to reapply licenses or obtain new licenses
- To recover from any issues during the upgrade process, It is highly recommended to:
 - Take a backup of the configuration
 - Take a backup/snapshot of the entire VM so that user can revert back to the original 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 3 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 8.0.2 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.
- 8.0.2 Release also includes a new Dashboard installer and must be installed.
- 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/snapshot 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 customers who are upgrading from 8.0.x to 8.0.2 release. If you're running any older version (e.g. 7.0.x) and would like to upgrade to 8.0.2, you must first upgrade to 8.0.0 release. Refer to the Release Notes of the Identity Engines 8.0.0 release for more information on licensing requirements & upgrade procedure.

Follow the instructions given below before proceeding with the upgrade.

- There's no change in the license model and customers with 8.0 licenses can continue to use them on 8.0.2 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 8.0.2 includes a new Dashboard installer. Close any running Dashboard instances and install the new 8.0.2 Dashboard.
 - *You must have Administrator Rights in order to install the Dashboard*
 - *Ignition Server 8.0.2 cannot be managed from an 8.0.x or earlier Dashboard versions*
 - *Note that 8.0.2 Dashboard upgrades the Java platform to JRE release 6 update 27*
- From the 8.0.2 Dashboard, upgrade the Ignition Server to release 8.0.2 as mentioned in the '*Ignition Server – Administration Guide section Activating a firmware Image or Package*'
- Release 8.0.2 Ignition Software will continue to work with 8.0.0 versions of Access Portal, CASE Administration, and Guest Manager and Analytics software.
- The installed 8.0.0 licenses will be retained after the upgrade to 8.0.2.

Time Zone update for Dashboard Java installation

Ignition Server always runs in UTC time-zone whereas the Ignition Dashboard runs in the local time-zone of the PC on which the Dashboard is installed.

Ignition Dashboard includes Java 2 Standard Edition Runtime Environment (JRE) 6 update 27 which has its own library for managing various time zones. To accommodate some of the recent time zone changes with respect to Daylight Savings Time (DST) in various countries, users are highly advised to install Java SE Time Zone updater patch by following these instructions.

1. Close all the applications that use JRE 1.6_27 in C:\Program Files\Java\jre1.6.0_27. This will include Ignition Dashboard and if users have configured any other applications that use this JRE instance
2. Get the tzupdater zip file from <http://www.oracle.com/technetwork/java/javase/downloads/tzupdater-1-3-39-download-402444.html>
3. Extract the zip contents to C:\Program Files\Java
4. This should create a folder C:\Program Files\Java\tzupdater-1.3.40-2011h
5. From the command prompt, navigate to C:\Program Files\Java\tzupdater-1.3.40-2011h
6. Type the command: C:\PROGRA~1\Java\jre1.6.0_27\bin\java -jar tzupdater.jar -u -v

Output:

java.home: C:\PROGRA~1\Java\jre1.6.0_27

java.vendor: Sun Microsystems Inc.

```
java.version: 1.6.0_27
JRE time zone data version: tzdata2011g
Embedded time zone data version: tzdata2011h
Extracting files... done.
Renaming directories... done.
Validating the new time zone data... done.
Time zone data update is complete.
```

7. Confirm whether the patch was installed:

Output:

```
C:\PROGRA~1\Java\jre1.6.0_27\bin\java -jar tzupdater.jar -t -v
```

```
java.home: C:\PROGRA~1\Java\jre1.6.0_27
```

```
java.vendor: Sun Microsystems Inc.
```

```
java.version: 1.6.0_27
```

```
JRE time zone data version: tzdata2011h
```

```
Embedded time zone data version: tzdata2011h
```

```
Validating the time zone data
```

```
Validation complete
```

It is important to ensure that the time zone data confirms to tzdata2011h

9. 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>.

© 2013 Avaya Inc. All Rights Reserved.

Notice

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

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya 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](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, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "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.

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.

Virtualization

Each vAppliance will have its own ordering code. Note that each instance of a vAppliance must be separately ordered. If the end user customer or Avaya channel partner would like to install two of the same type of vAppliances, then two vAppliances of that type must be ordered.

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.