Avaya Identity Engines Release Notes
Software Release 9.1.0

NN47280-400
Issue 06.05
October 2015

1. Release Summary

Document Version: 06.05
Document Date: October 2015
Purpose: Identity Engines (IDE) software service pack release to introduce new Features, Enhancements, and to address customer found software issues.

Release Notes Revisions	Description	Comments
06.01	Initial release of Release Notes for IDE 9.1.0	
06.02	Note the incompatibility of CASE Manager 1.0 with Access Portal 9.1	
06.03	• Added Application Note about the incompatibility of CASE Manager 1.0 with Access Portal 9.1. • Added Application Note regarding Aruba and Trapeze device template.	
06.04	• Added Application Notes about Access Portal Admin and OUT interfaces on same VLAN.	
06.05	• Added Application Notes about Access Portal OUT interface configuration for DHCP/Static IP address.	

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

- If you are running release ESXi and 8.0.x then be aware that upgrade from release 8.0.x to 9.x is not available as the hardware system requirements for release 9.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 9.1.0 OVA and then restore the 8.0.x configuration into 9.1.0 instance. Follow the upgrade procedure in "***Chapter 9. Upgrade Procedure"*** of this document.

- If you are running release 9.0.1, 9.0.2 or 9.0.3 and would like to migrate to 9.1.0, you have two options:
  - Take a configuration backup from 9.0.1, 9.0.2 or 9.0.3, deploy a new 9.1.0 VM and perform a configuration restore on the 9.1.0 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, 9.0.2 or 9.0.3 to 9.1.0 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 9.1.0:
VMware ESXi and vSphere version 5.1
VMware ESXi and 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 9.1.0:

File Name	Module or File Type	Comments
AIEIS_RHEL_6_5_LINUX-VM_09_01_00_028005_x86_64.ova	Ignition Server OVA files for vSphere 5.1 and 5.5 environments	Ignition Server release 9.1.0. This file is used if fresh VM install option is desired.
LINUX-VM_09_01_00_028005_server_complete.pkg	Ignition Server upgrade package files for vSphere 5.1 and 5.5 environments	Ignition Server release 9.1.0. These files are used if upgrade option is desired.
DashboardInstaller-9.1.0.28005.exe	Dashboard Installer	Dashboard Installer release 9.1.0 compatible with Ignition Server release 9.1.0
AccessPortal_09_01_00_027925_x86_64.ova	Access Portal OVA files for vSphere 5.1 and 5.5 environments	Access Portal Release 9.1.0 is compatible with Ignition Server release 9.1.0
AIGM_RHEL_6_5_LINUX-VM_09_01_00_027981_x86_64.ova	Guest Manager OVA files for vSphere 5. 1 and 5.5 environments	Guest Manager Release 9.1.0 is compatible with Ignition server release 9.1.0

Identity Engines software file names of Release 8.x and 9.x that are compatible for deployment in conjunction with Identity Engines Release 9.1.0:

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 9.1. • However, CASE Manager 1.0 is not compatible with Access Portal 9.1 with respect to uploading / deploying a CASE Package onto the Access Portal. • Please follow guidelines in Section 8.5 Application Notes
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 9.1.0 software can only be managed with Avaya Ignition Dashboard release 9.1.0.

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

Software	Software Compatibility	Comments
Ignition Server Release 9.1.0	• VMware ESXi versions 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 250 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
Ignition Dashboard Release 9.1.0	• Windows 7 (32 bit or 64 bit) • Windows 8 (32 bit or 64 bit) • Windows 2008 (32 bit or 64 bit) • Windows 2012 (64 bit)	• Minimum 2GB RAM memory • US English Windows
Ignition Access Portal Release 9.1.0	• VMware ESXi versions 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 a x86_64 capable environment • Minimum 2 CPUs • Minimum 4 GB of memory • Minimum 8 GB available disk storage (VMware thin provisioning is allowed) • Preferably 3 physical NIC (minimum 2 NICs) • VMware list of supported hardware platforms for ESXi is available on:

		http://www.vmware.com
Ignition Guest Manager Release 9.1.0	• VMware ESXi versions 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 (5)	• The VM requires a x86_64 capable environment • Minimum 2 CPUs (default is 4 CPU) • Minimum 2 GB of memory (default is 4 GB) • Minimum 80 GB available disk storage (VMware thin provisioning is allowed) • Minimum 1 physical NIC (preferably 3 NICs). • VMware list of supported hardware platforms for ESXi is available on: http://www.vmware.com
CASE Manager Release 8.0	• Windows Server 2008 (64 bit)	• 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 & R9.1.0 SSO
Avaya System Manager	Avaya SMGR release 6.3.10	• Compatible with Identity Engines R9.0.1, R9.0.2, R9.0.3 & R9.1.0 SSO
Service Provider Agent	Apache Tomcat 6.X	• Compatible with Identity Engines R9.0.1, R9.0.2, R9.0.3 & R9.1.0 SSO • Any servlet container compliant with the Servlet API specifications version 2.4 or higher will work, like Tomcat 6.x, JBoss or Websphere
Citrix XenMobile MDM	Citrix XenMobile MDM 8.7 and 9.0	• Compatible with Identity Engines R9.1.0

7. Version of Previous Releases

Identity Engines Software release 9.0.3, Release Date – January, 2015
File name “NN47280-400_05_04_IDEngines_9_0_3_Release_Notes.pdf”

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

- **Mobile Device Management (MDM) Support**
  Identity Engines Release 9.1 adds support for Mobile Device Management (MDM) by integrating third-party MDM services. Identity Engines Release 9.1 supports Citrix XenMobile MDM.

  The MDM feature provides more control and secure access to Bring Your Own Device (BYOD) deployments in the corporate network. With the new MDM feature in 9.1 release, Ignition Server interfaces with the MDM server to collect the mobile device attributes and save them in the Internal Store. During the user authentication, the device attributes are evaluated and fed to the policy engine for the final authorization process.

- **Access Portal Platform Upgrade & Enhancements**
  Access Portal Release 9.1 provides new and enhanced capabilities for management and access control of Bring Your Own Device (BYOD) technology.

  Release 9.1 includes the following enhancements:
  - Platform upgrade from pfSense 1.2.3 to pfSense 2.1.x with code from pfSense® software revised on Feb 9th 2015
  - Multiple IN interfaces, Multiple OUT interfaces and Multiple Success Pages along with the concept of Captive Portal Zones and Access Groups allow customized access that provide flexibility to control and present what different users or a group of users experience through Access Portal
  - VMware Tools support to allow Access Portal be VMware vMotion and HA friendly
  - Updated device fingerprinting support for Windows 8, Windows Server 2012, Windows Surface RT, MAC OS Maverick (10.9), IOS 7.x, Android 4.4, Blackberry 7 OS, Kindle Fire and Blackberry 10 OS
  - Limit for concurrent logins
  - Support for RADIUS session time-out
  - Login and Logout support for CLI
  - Inbound and Outbound RADIUS VSA attributes for granular access policy control

- **Guest Manager Virtual Appliance**
  From Release 9.1, Guest Manager is shipped as a Virtual Appliance. The Guest Manager Virtual Appliance uses RHEL as base OS. It also incorporates VMware Tools to allow Guest Manager be VMware vMotion and HA friendly.

  As of Release 9.1, Guest Manager is no longer available as a Windows application.

  Release 9.1 Guest Manager also includes the following enhancements:
  - New sponsor approval workflow
    - Visitor registers using self-service guest template and employee received and email with links to approve or deny guest.
    - Sponsor expiration time for response can be set.
    - Default action (approve or deny) upon expiration can be set
  - Simplified Self-Service workflow
    - Visitor registers using self-service guest template and employee received and email with links to approve or deny guest.
    - Sponsor expiration time for response can be set.
    - Default action (approve or deny) upon expiration can be set
  - Admin can limit to number of devices with self-registration.
  - Admin can limit number of guest accounts that can be created for a given email/cellphone within a certain time window.
  - Email service configuration may also be web based service (e.g. gmail.com).
  - Usability enhancements to the GM Monitoring screens.

- Hide SMS Gateway if external SMS service is used.
- Enhanced SMTP configuration support
- Address known security vulnerabilities

- **Extended-HA**
  Release 9.1 introduces the first phase of an Extended High Availability (HA) configuration for geographically redundant Avaya Identity Engines (IDE) Ignition servers.

  One site is designated as a root site, which contains the primary, active Ignition Server (pair). One or more sites are designated as branch sites, which contain secondary, inactive Ignition Server (pairs). Configuration of guest device and guest user accounts occurs on the root site, and periodic synchronization of the information to the branch sites. In the event of site failure, a branch site can take over access requests.

  On the Ignition Server (pair) which is designated as a root site, you configure a scheduled export that'll export all the guest accounts to a remote SFTP Server. On one or more branch sites, you configure scheduled import that fetches the guest account records from the remote SFTP server and store in its local store.

- **Two-Click Onboarding of Unknown Devices in the Network**
  Administrator can register device MAC address from RADIUS Access Log that is failed on MAC authentication.

  Administrator can go to Monitor tab, select the log record and use right click and select 'Add MAC to Internal Devices' option. This will launch a New Device Record with the pre-populated MAC addresses. Once the MAC addresses are added to the internal store, MAC Authentication would now succeed.

- **Avaya Fabric Attach Support**
  Avaya Fabric Attach extends Fabric Connect to deliver Edge Automation capability that reduces the complexity of adding or modifying services. Any FA-capable device (such as a switch or AP) can now be securely connected to the network, be authorized for a network service, and attach to the appropriate network service instance – all automated and based on IT policy

  The Fabric Attach elements consist of the following:
  - FA Server - Avaya Ethernet switch that supports FA Signaling and is Fabric Connect capable
  - FA Proxy - Avaya Ethernet switch that supports FA Signaling and is not Fabric Connect capable
  - FA Client: Ethernet device that supports FA Signaling, and may or may not be an Avaya device
  - FA Policy Server: Avaya network access policy server

  Fabric Attach uses FA Signaling. FA Signaling is an application-level protocol that leverages standard network protocols to exchange messages and data between Fabric Attach elements to orchestrate network edge automation.

  Identity Engines Ignition Server R9.1 takes the role of the FA Policy Server. The Identity Engines components required for FA Policy are the following:
  - Ignition Server
  - Ignition Dashboard

  Other Identity Engines components such as the Ignition Guest Manager and Ignition Access Portal are optional and not required for Fabric Attach. These components may be required for other workflows depending on customer requirements.

  Identity Engines Fabric Attach automates service provisioning of the access edge for standard clients and FA Clients such as the WLAN 9100 AP connecting to a FA Proxy Standalone switch, FA Proxy switch, or FA Server switch.

8.2. Customer Found Issues Resolved in this Release

Work item Number	Description
wi01132335	Identity Engines Access Portal requires reboot after deleting firewall rule.
wi01153249	Access Portal Syslog stops functioning if State Table is full
wi01170515	Access Portal disabling "HTTPS Login" is ineffective until next system reboot
wi01170525	Access Portal returns HTTP 500 - Various Reasons
wi01038838	IDE 8.0 Guest Manager EMAIL notification notes are not sent when users are first created. The notification will show up if it is resent.
wi01179781	IDE 9.0.1 - MAC Authentication fails when "Trapeze" vendor is being used
wi01185244	Identity engines 9.0.1 MAC authentication does not work when the RADIUS policy is enabled
wi01026384	Guest Manager is not using the correct Notification Email template

8.3. Outstanding Issues

Work item Number	Description
wi01211342	**If AD is configured with OU = sales, marketing then IDE will not see it as it is. It would see it as "sales\, marketing.**
wi01212920	**IDE 9.1 BETA - Dashboard Scheduled Task Does Not Maintain Root Path Value** If the scheduled backup path is simply “/”, user will be able to save the config. However, if the user opens the task to edit some settings, as a workaround, users have to re-enter the root path
wi01212915	**IDE 9.1 BETA - Scheduled Backup Status Automatic Refresh & Manual Refresh Issues** Once a backup scheduled task is executed, the refresh button does not refresh the status on the Dashboard. As work around, users have to select respective schedule task and then click refresh, it updates the task status correctly
wi01160583	**Running Packet Capture Orphaned if Dashboard Crashes or Client PC Shutdown**
wi01204910	**Dashboard does not show “version mismatch” alert message while reconnecting to Dashboard when user upgraded IDE from 9.0 to 9.0.3** 9.0/9.0.x Dashboard cannot be used to connect to 9.1 Ignition Server. As part of upgrading 9.0/9.0.x to 9.1, the connection from Dashboard to Ignition Server could terminated abnormally as the Ignition Server reboots. The admin needs to reconnect to the 9.1 Ignition Server using 9.1 Ignition Dashboard.
wi01204903	When administrator creates maximum number of authenticators per license limit and if administrator tries to modify any of the authenticators with both authenticator name and IP address fields in single action, that authenticator is going into disable state. As work around, user can edit operation in multiple actions like 1. Modify Authenticator name in the first attempt 2. Modify IP address in the second attempt
wi01208841	**Ignition Access Portal 9.1 cannot upload file which is bigger than 130MB through Captive Portal File Manager**
wi01208839	**“show httpd” command does not reflect the httpd listen and allow configurations correctly**
wi01111636	**Dashboard intermittently displays “server-side Exception: null and Session already exists” error messages during login** Observed while login to dashboard server-side Exception: null and Session already exists error messages As workaround, close the existing Dashboard session and re-launch the Dashboard

8.4. Known Limitations

Work Item Number	Description
wi01196915	**VMWare tool on Access Portal is not functioning correctly on some hardware** See following URL for more detail on this limitation: http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2011350
wi01197770	**In the following scenario unable to re-authenticate the clients if the policy is defined with inbound attributes (with Avaya inbound attributes)** Inbound attributes sent by Access Portal are obtained during fingerprinting which happens only when the user logs in. As work around, if inbound attributes need to be used in the policy then use hard session timeout OR use soft session timeout with the device attributes in the policy instead of inbound attributes. Use of the soft session timeout implies that it is the same user session and within the same session the device fingerprinting attributes do not change, so the use of device attributes instead of inbound attributes is offering the exact functionality.
wi01187244	**On 9.0.2 SP build no Inbound attributes listed under created policy after restoring VSA vendor backup configuration.**
wi01199284	**User not able to stop tcpdump (Filter Log) through SSH session**
wi01210516	**When using the new Two-Click to Add MAC feature when high rate or bursts of access logs are received, it is recommended do disable Auto Refresh as the display refresh may cause the access log records to move fast during the Two-Click to Add MAC operation.**

8.5. Application Notes

- **CASE Manager**
  - CASE Manager Release 1.0 is compatible with Ignition Server release 9.1
  - However, CASE Manager 1.0 is not compatible with Access Portal 9.1 with respect to uploading / deploying a CASE Package onto the Access Portal.
  - CASE Wizard Packages created by CASE Manager 1.0 (aka CASE Console) are compatible with Access Portal release 9.1.
  - However the automated process of uploading CASE Wizard Packages is not compatible with Access Portal release 9.1. A manual process, as per the following guidelines, is required in order to upload the CASE Wizard Package onto a Zone on Access Portal release 9.1
  - Obtain the CASE Package files from the following CASE Manager folder
    "C:\Program Files\Apache Software Foundation\Tomcat6.0\conf \AdminConsole\admin\TBD\" where TBD is the CASE Wizard Package name.
  - Upload the files onto the desired Captive Portal Zone on the Access Portal 9.1 using the File Manager
- **CASE Manager Example**
  - CASE Wizard Package was created with the name EAP
  - The CASE Wizard Package files will be found in the following folder
    "C:\Program Files\Apache Software Foundation\Tomcat6.0\conf \AdminConsole\admin\EAP"
  - There will be 7 files in this folder:
    - CASE.zip
    - CASEActiveX.cab
    - SEApplet.jar
    - CASEJavaLauncher.zip
    - CASESuccess.html
    - EAP_CASE.xml
    - EAP_CASEProfile.zip
  - Upload these 7 files to the desired Zone on Access Portal release 9.1
  - Once this is complete change the Portal Page Contents to "CASESuccess.html" so that the Access Portal Success Page that has the link to the CASE Wizard will be displayed after successful authentication.
- **Device Templates for Aruba WLAN and Trapeze WLAN**
  - Identity Engines is shipped to use 'VLAN Label' for 'generic-aruba' and 'generic-trapeze' device templates. As part of Identity Engines configuration, customers may choose to change the template definition instead to use 'VLAN ID" to suit their specific environment.
  - If you have changed the default configuration to use "VLAN ID" in an IDE pre-9.1 release and you have upgraded to IDE 9.1 release either through software upgrade or backup/restore, the settings will be reset to use 'VLAN Label".
  - As a work around, users are advised to edit the above two templates and set it to use 'VLAN ID" after the upgrade to 9.1.
- **Access Portal**
  - Avaya does not recommend configuring Access Portal ADMIN interface and OUT interface to be on same VLAN. Such configuration may result in intermittent communication issues.
  - Avaya recommends configuring the ADMIN interface and OUT interface to be on different VLANs.
  - Access Portal 9.1 only supports Static IP configuration on the OUT interface(s). Access Portal 8.0 supported both Static IP as well DHCP configuration on the OUT interface, Hence take one of the following actions:
    - It is recommended that prior to exporting the Access Portal 8.0 configuration with the intention to restore it into Access Portal 9.1, change the OUT interface configuration on Access Portal 8.0 to Static IP and only then export the configuration.
    - If you have already restored into Access Portal 9.1 a configuration from Access Portal 8.0 that has OUT interface configured as DHCP, then perform the following:
      - Navigate to System > Routing > Gateways
        - Identify the Gateway associated with OUT interface.
        - Click on the Edit Gateway button.

- Under “Gateway” field the word “dynamic” will be seen as value populated.
- Delete the word “dynamic” and configure the IP address of the gateway. This will be the gateway for OUT interface which will be configured next.
- “Save” configuration and click on “Apply Changes”.

- Navigate to Interfaces > OUT.
  - Under “Static IPv4 configuration” configure OUT interface static IP address.
  - Choose the gateway from the drop-down (you should be able to see the gateway you configured above).
  - Save configuration and click on “Apply Changes”.

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 9.1.0 VM using software upgrade procedure.

- Existing 8.0.x, 9.0.0, 9.0.1, 9.0.2 and 9.0.3 configurations can be migrated to 9.1.0 using the backup & restore functionality. Restore of configuration data on 9.1.0 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 9.1.0, first perform an incremental upgrade to 8.0.x release and then use backup & restore functionality to migrate your existing configuration to 9.1.0 VM
    - Temporary licenses for IDE R8.0 and IDE R9.0 for this process of incremental migration of your configuration to IDE release 9.1.0 are available on www.avaya.com/identitytrial
- Always take a backup of your Ignition Server configuration.
- Always take a VMware snapshot of the Virtual Machine on the ESXi Server as a backup in case of upgrade failure.
- 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
- If the new Vendor and Device Template with the exact same names as above were already previously added manually 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 9.1.0 cannot be downgraded to a previous version. If the Ignition server is accidentally upgraded to 9.1.0 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 9.1.0, 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 9.1.0.
- Release 9.1.0 introduces a set of RADIUS VSA extensions for Avaya Fabric Attach support. It is **required** to delete any Fabric Attach VSAs previously manually configured prior to upgrade or prior to restoring a configuration from a previous release. This is a **mandatory** procedure otherwise the migration process might fail.

Dashboard Checklist

- Identity Engines 9.1.0 also includes a new Dashboard installer that must be installed. Ignition Server release 9.1.0 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 9.1.0 as a new VM:
  - Take a configuration backup from 8.0.x
  - Deploy a new 9.1.0 VM
  - Perform a configuration restore on the 9.1.0 VM
  - New licenses will be required
    - You may use temporary licenses from www.avaya.com/identitytrial
  - Perform a new backup of the 9.1.0 configuration

- If you have Ignition Server 9.0.1, 9.0.2 or 9.0.3 and would like to install 9.1.0 as a new VM:
  - Take a configuration backup from 9.0.1, 9.0.2 or 9.0.3
  - Deploy a new 9.1.0 VM
  - Perform a configuration restore on the 9.1.0 VM
  - New permanent licenses will be required.
    - You may use temporary licenses from www.avaya.com/identitytrial
  - Perform a new backup of the 9.1.0 configuration

- If you have Ignition Server 9.0.1, 9.0.2 or 9.0.3 and would like to perform a 9.1.0 using software upgrade process:
  - Take a configuration backup from 9.0.1, 9.0.2 or 9.0.3
  - 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, 9.0.2 or 9.0.3 to 9.1.0 using the pkg (Package) file.
  - Perform a new backup of the 9.1.0 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/