Avaya Identity Engines Release Notes
Software Release 9.2.4

NN47280-400
Issue 11.04
April 2016

1. Document Summary

Document Version: 11.04
Document Date: April, 2016
Purpose: Identity Engines (IDE) software feature pack release to introduce new Features, Enhancements, and to address customer found software issues.

Release Notes Revisions	Description	Comments
11.01	Release Notes for IDE 9.2.4	Ignition Server incorporates an important fix in the log rotate functionality.
11.02	Updates for Access Portal 9.2 release	
11.03	Updated Section 9.2 Issues Resolved in this Release	
11.04	Updates for Access Portal 9.2.1 release	

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).

©2012-2016 Avaya Inc.

- If you are on release 8.0.x then please also note that restore of the backup from 8.0.x to 9.2.4 is not supported. Should you want to restore your 8.0.x config then first upgrade to 9.1.0 and then restore the config from 8.0.x into that instance of 9.1.0. Post that you can either upgrade to 9.2.4 or take a backup and then restore the config on a fresh 9.2.4 instance. Follow the upgrade procedure in "***Chapter 10. Upgrade Procedure"*** of this document.

- If you are running release 9.0.x, 9.1.0, 9.2.0, 9.2.1, 9.2.2 or 9.2.3 and would like to migrate to 9.2.4, you have two options:
    - Take a configuration backup from 9.0.x, 9.1.0, 9.2.0, 9.2.1, 9.2.2 or 9.2.3, deploy a fresh new 9.2.4 VM and perform a configuration restore on the 9.2.4 VM. New licenses will be required. Follow the upgrade procedure in "***Chapter 10. Upgrade Procedure"*** of this document.
    - Perform a software upgrade directly from 9.0.x, 9.1.0, 9.2.0, 9.2.1, 9.2.2 or 9.2.3 to 9.2.4 using the PKG (Package) file. Follow the upgrade procedure in "***Chapter 10. Upgrade Procedure"*** this document.

- Please be reminded that whenever you deploy fresh new OVA, you will have to obtain new licenses.
    - Please contact datalicensing@avaya,com with your request
    - Please provide your older Ignition Server Serial Number

4. Hypervisor Platforms Supported

The following VMware ESXi platforms are supported with Identity Engines release 9.2.4:
VMware ESXi and vSphere version 5.1
VMware ESXi and vSphere version 5.5

IMPORTANT NOTE:
Note that VMware vMotion, VMware Player and VMware Workstation or any other 3rd party migration tools are not supported and cannot be used in conjunction with the Ignition Server.

5. Software Files

5.1. New Identity Engines software files delivered with Release 9.2.4:

File Name	Module or File Type	Comments
AIEIS_RHEL_6_5_LINUX-VM_09_02_04_029832_x86_64.ova	Ignition Server 9.2.4 OVA for VMware ESXi	This file is used for fresh VM install.
LINUX-VM_09_02_04_029832_server_complete.pkg	Ignition Server 9.2.4 Package file	This file is used for software upgrade.
DashboardInstaller-9.2.4.29832.exe	Dashboard Installer 9.2.4	Compatible with Ignition Server 9.2.4.
AccessPortal_09_02_01_030212_x86_64.ova	Access Portal OVA file for vSphere 5.1 and 5.5 environment	This file is used for fresh VM install.

5.2. Previous Identity Engines software files compatible with Release 9.2.4:

File Name	Module or File Type	Comments
AIGM_RHEL_6_5_LINUX-VM_09_02_03_029741_x86_64.ova	Guest Manager 9.2.3 OVA for VMware ESXi	Compatible with Ignition Server release 9.2.4.
Avaya_idEngines_IDR_9.2.apk	Android application package	Ignition Device Registration (IDR) App release 9.2.0 is compatible with Guest Manager release 9.2.3.
AdminConsoleInstaller-1.0.0.22931.exe	CASE Manager Installer 1.0	• Compatible with Ignition Server 9.2.4 • However, CASE Manager 1.0 is not compatible with Access Portal 9.1.0 with respect to uploading / deploying a CASE Package onto the Access Portal. • Please follow guidelines in section "**9.5 Application Notes**" as well as KCS SOLN273086 on Avaya support site.
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

©2012-2016 Avaya Inc.

6. Interoperability and Upgrade Matrix

6.1. Supported Interoperability of Identity Engines Applications:

	Compatible Ignition Server & Dashboard	Compatible Guest Manager	Compatible Android IDR App	Compatible Access Portal	Compatible CASE Manager
Ignition Server & Dashboard 9.2.4	-	9.2.3	-	9.1.0 9.2.0 9.2.1	-
Guest Manager 9.2.3	9.2.0 9.2.1 9.2.2 9.2.3 9.2.4	-	9.2.x	9.2.0 9.2.1	-
Android IDR App 9.2	-	9.2.3	-	-	-
Access Portal 9.2.1	9.2.3 9.2.4	9.2.3	-	-	8.0(1)
CASE Manager 8.0	-	-	-	9.1.0(1) 9.2.0(1) 9.2.1(1)	-

NOTE (1): Workaround required. Please refer to section "**9.5. Application Notes**".

6.2. Supported Software Upgrade flow using Package (pkg) file:

Compatible From →	Ignition Server 8.0.x	Ignition Server 9.0.x	Ignition Server 9.1.0	Ignition Server 9.2.0	Ignition Server 9.2.1	Ignition Server 9.2.2	Ignition Server 9.2.3
Ignition Server 9.2.4	Not Supported	Supported	Supported	Supported	Supported	Supported	Supported

6.3. Supported Configuration Restore flow using Configuration File Backup & Restore:

	Compatible From Ignition Server & Dashboard	Compatible From Guest Manager	Compatible From Android IDR App	Compatible From Access Portal	Compatible From CASE Manager
Ignition Server & Dashboard 9.2.4	9.0.x 9.1.0 9.2.0 9.2.1, 9.2.2, 9.2.3	-	-	-	-
Guest Manager 9.2.3	-	9.0.x 9.1.0 9.2.0	-	-	-
Android IDR App 9.2	-	-	-	-	-
Access Portal 9.2.1	-	-	-	8.0 9.1.0	-

				9.2.0	

7. System Requirements

Software	Software Compatibility	Comments
Ignition Server Release 9.2.4	• 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. • Identity Engines Ignition Server release 9.2.4 software can only be managed with Avaya Ignition Dashboard release 9.2.4.	• 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 9.2.4	• Windows 7 (64 bit) • Windows 8 (64 bit) • Windows 2008 (64 bit) • Windows 2012 (64 bit)	• Minimum 2GB RAM memory • US English Windows • Desktop/PC or Laptop • NOTE: Dashboard will NOT install on Windows 32-bit
Ignition Access Portal Release 9.2.1	• 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. • Microsoft IE Browser 11, 10 and 9 • Firefox Browser 48, 47 and 46 • Chrome Browser 50, 49 and 48	• 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 9.2.3	• 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 • Microsoft IE Browser 11 and up • Firefox Browser 40 and up • Chrome Browser 47 and up	• 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 • NOTE: Release 9.2.3 is the last release in which HTTP access is supported for Admin/Provisioner. Following releases will ONLY support HTTPS.
Ignition Device Registration (IDR) App Release 9.2.0	• Android Application Package • Android version 4.2.2 or above • Works best with Smartphones of screen sizes 4.7” or 5”.	• Available for downloaded from Google Play
CASE	• Windows Server 2008 (64 bit)	• Minimum 2GB RAM memory

Manager Release 8.0		• 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.x, R9.1.0, R9.2.0, R9.2.1, R9.2.2, R9.2.3 & R9.2.4 SSO
Avaya System Manager	Avaya SMGR release 6.3.10	• Compatible with Identity Engines R9.0.x, R9.1.0, R9.2.0, R9.2.1, R9.2.2, R9.2.3 & R9.2.4 SSO
Service Provider Agent	Apache Tomcat 6.X	• Compatible with Identity Engines R9.0.x, R9.1.0, R9.2.0, R9.2.1, R9.2.2, R9.2.3 & R9.2.4 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 R9.2.4
AirWatch MDM	Airwatch MDM v8.0.5	• Compatible with Identity Engines R9.2.4
Microsoft Active Directory	Windows Server 2003 Windows Server 2008 Windows Server 2012	• Compatible with Identity Engines R9.2.4

8. Versions of Previous Release Notes

Identity Engines Software release 9.0.1, Release Date – June, 2014
File name “NN47280-400_03_03_IDEngines_9_0_1_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 9.0.3, Release Date – January, 2015
File name “NN47280-400_05_04_IDEngines_9_0_3_Release_Notes.pdf”

Identity Engines Software release 9.1.0, Release Date – July, 2015
File name “NN47280-400_06_03_IDEngines_9_1_0_Release_Notes.pdf”

Identity Engines Software release 9.2.0, Release Date – August, 2015
File name “NN47280-400_07_01_IDEngines_9_2_0_Release_Notes.pdf”

Identity Engines Software release 9.2.1, Release Date – September, 2015
File name “NN47280-400_08_01_IDEngines_9_2_1_Release_Notes.pdf”

Identity Engines Software release 9.2.2, Release Date – October, 2015
File name “NN47280-400_09_02_IDEngines_9_2_2_Release_Notes.pdf”

Identity Engines Software release 9.2.3, Release Date – December, 2015
File name “NN47280-400_10_01_IDEngines_9_2_3_Release_Notes.pdf”

Identity Engines Software release 9.2.4, Release Date – March, 2015
File name “NN47280-400_11_02_IDEngines_9_2_4_Release_Notes.pdf”

Identity Engines Software release 9.2.4, Release Date – March, 2015
File name “NN47280-400_11_03_IDEngines_9_2_4_Release_Notes.pdf”

9. New and Changes in this Release

9.1. New features in this Release

- **Guest Manager Virtual Appliance**
  A collection of new and enhanced features on the Guest Manager:
  - Updates to the existing REST API framework
    - API to delete (multiple or single) user/device records
    - API to update a single user/device record
    - API to bulk delete users/devices ALL
    - API to retrieve user/device record details with filter
    - API to fetch array of users/devices with filter but without details
    - API to query if a device or list of devices exist
    - API to query if a user or list of users exist
    - Add support for “VLAN Id” and “VLAN Label” attribute in the existing APIs
  - Sponsor enhancement to not send initial email and sponsor response mail to guest
  - Filter to display expired users/devices
  - Filter to display users/devices with First Login not activated and created X date back.
  - CLI command for ping operation

- **Access Policy Templates**
  Rename some of the existing Policy Templates for better readability.

- **General Usability Features**
  - License URL display as Hyperlink in Licensing Tab
  - Dashboard Installer enhancements
    - Remove support for Windows OS 32 bit
    - Do not install any JRE as part of the Dashboard installation
  - Display both Ignition Server and Dashboard version in Status screen for better clarity
  - MAC Auth config enhancement to include “MAC as Password” option
  - Support for Failed MAC Auth Policy

- **Ignition Server Downgrade**
  - Protection against accidental downgrade of the Ignition Server software.
  - VMware snapshots are the recommended method to roll back into an older Ignition Server version

- **Access Portal login via Social Media**
  - Provide support for Social Media login where guest users may use Google/Facebook/LinkedIn credentials to authenticate into a guest network.
  - The landing page with Social Media login buttons will be displayed. On clicking the same, users will be redirected to respective Social Media site for authentication.
  - Users will be requested by the Social Media site to consent before being authenticated.

- **Access Portal Trusted Root CA upload**

- Option to add root CA certificate to the list of trusted certificates from Access Portal.
- Needed in deployments where SSL intercept happens.

- **Access Portal External Login for WLAN 9100**
  - This release of Ignition Access Portal introduces a key new feature of Access Portal as External Captive Portal for WLAN AP 9100. Unlike the traditional operation of the Access Portal, when the External Captive Portal is enabled, following authentication and authorization, the wireless client traffic will flow inline through the AP 9100 as opposed to inline through the Access Portal.

  - With Access Portal feature of External Captive Portal to WLAN 9100, there are numerous advantages as follows:
    - Highly customizable login page
    - Highly customizable success page
    - Fingerprinting of wireless client including the following attributes:
      - Device MAC address
      - Device Operating System (e.g. MAC OSX)
      - Device Operating System Version (e.g. 10.6.8)
      - Device Type (e.g. Mobile)
      - Device Sub-Type (e.g. iPad)
    - Fingerprinting over L2 or L3 network
    - Once Ignition Access Portal can serve multiple WLAN 9100 APs
    - Multiple different External Captive Portals zones may be configured on the Access Portal
  - This new feature provides new BYOD onboarding capabilities to accommodate customer deployment, IT experience and user experience needs.

- **Access Portal Support for Lightspeed Integration**
  - Many organizations, in particular education institutions, deploy security gateways for web filtering in order to protect their students and users. This release of Ignition Access Portal supports integration of Web Filter by Lightspeed Systems.
  - You now have the option to configure and send RADIUS accounting records to a server other than the Ignition Server used for authentication and authorization.
  - This feature allows enabling RADIUS accounting and configuring a primary and a secondary RADIUS accounting server, so that you can receive these accounting packets. For more information, see Configuring the Appliance Access Portal Settings on page 43.
  - In addition, by default, the traffic going through OUT interface of the Access Portal is NATed and any system will see the OUT interface IP and not the client IP. You can change the configuration by disabling NAT rule in Access portal. This feature allows Lightspeed security gateway to see the individual IP addresses of the network (client), by changing the configuration in Firewall > NAT > Outbound tab.

- **Access Portal Support User-Defined VSA**
  - Some deployment scenarios require the user to provide input at the time of access so that the input will be taken into consideration during the Ignition Server Access Policy decision. For example, a contractor arrives to customer site needing access to the network. However, in certain days of the week the contractor works on one portion of the network and in certain other days of the week, the contractor works on another portion of the network. With the User-defined VSAs, the Access Portal login page may be configured in such a fashion that the contractor will be able to enter text, or possibly select a radio button or any other means that the Identity Engines customer desires, to pass information to the Ignition Server Access Policy for evaluation.

  - The current release introduces two new users defined VSAs:
    - Avaya-Access-Portal-Custom-VSA1 of type String.
    - Avaya-Access-Portal-Custom-VSA2 of type String
  - Use a text editor or HTML editor to create customized user-visible input fields to capture the user input and populate one or the two VSAs and then pass the value(s) to the Ignition Server Access Policy for evaluation.

- **Access Portal Support for Scheduled Backups**
  - Enterprise customers require methodic backup of their IT infrastructure for business continuity reasons driven by regulatory compliance or internal corporate governance.
  - Access Portal already provided the ability to You can save the your Access Portal configuration to a backup file and later restore the configuration by loading the saved file.
  - This release of Ignition Access Portal introduces the ability to configure and You can schedule backups to run once, daily, weekly, or monthly using Scheduled Export tab. You can also perform Backup on-demand basis.

- **Access Portal Support DHCP on OUT Interface (Demo Mode Only)**
  - Ignition Access Portal supports multi-IN and multi-OUT interfaces. This requires that static IPs to be configured on the IN and OUT interfaces. However at times for testing and demo, there may be a need to have DHCP on the OUT interface. This release of the Access Portal provides to ability to enable DHCP on the OUT interface for demo or lab deployment only.
  - This feature is **NOT** supported in production live deployments.
  - See Access Portal manual for details.

- **Access Portal Additional Updates**
  - Fixed RADIUS attribute Called-Station-Id = MAC of IN interface that the client came through
  - Updated Fingerprint for Chromebooks and support for IE11.

©2012-2016 Avaya Inc.

9.2. Issues Resolved in this Release

Item Number	Description
JUPITER-513	[RHSA-2014:1552-02] Moderate: openssh security, bug fix, and enhancement update
JUPITER-704	[RHSA-2014:2024-1] Important: ntp security update
JUPITER-1086	Should throw proper error message when user tries to downgrading the system from higher version to lower version.
JUPITER-1205	Dashboard Stuck In "Upgrade In Progress" Loop Ignition Server Radius "Initializing"
JUPITER-1416	Identity Engines 9.02 If a client cert is a number IDE will perform Mac auth
JUPITER-1420	[GM-IDE Server] "SOAP Service might be disabled" error seen in Guest Manager GUI when IDE server was rebooted
JUPITER-1722	The import of a “backup data” does not restore the VLAN Method “Label or ID” for built in VSA’s
JUPITER-1795	Multiple RADIUS Restarts & Queue Full Outage
JUPITER-1984	[Guest Manager] Anonymous login fails with exchange SMTP server
JUPITER-1913	Guest Manager User Export and Device Export - Consistency in content and from where User and Device Exports are performed. Customer are advised to pay special care to changes in the export file content,
JUPITER-1983	While importing authenticators using csv file from 9.2 to any 9.2+ releases the COA configuration will not be imported.
JUPITER-2001	Ignition Server Did Not Automatically Switch to Secondary AD Server With Primary Instability
JUPITER-2007	Dashboard Import/Export missing items. Some user and device attributes were missing from the export files. Customers are advised to pay special care to the changes in the export file content.
JUPITER-2060	User should not allow downgrading the image when he activated the package after upgrade.
JUPITER-2099	Authentication fails for users other domain in the same forest when Ignition server is configured to use Global Catalog Active Directory
JUPITER-2117	[GM - provisioner] - Wrong error message, 'Error: null' while Loading 'Guest Users' and 'Device' in one scenario when no selection made.
JUPITER-2139	Identity Engines 9.2.2 cannot authenticate both an email and Sam account to Active directory if the email name is not the same as the Sam account.
JUPITER-2024	Appropriate log rotate mechanism added for the /var/log/messages to prevent the partition from getting filled.
JUPITER-1331	Access Portal 9.1 User Manager Admin Password Change Breaks GUI Access
JUPITER-1328	Identity Engines: Vulnerability Assessment for CVE-2014-3566 POODLE Padding Oracle On Downgraded Legacy SSLv3, SSL 3.0
JUPITER-2418	When using Access Portal as External Login for WLAN 9100 AP, Device Fingerprint is not working when client is more than one hop away from IAP.
JUPITER-2042	External Captive Portal fails after enabling Mac Authentication.

9.3. Outstanding Issues

Item Number	Description
JUPITER-1189	**Ignition Server: Running Packet Capture Orphaned if Dashboard Crashes or Client PC Shutdown**
JUPITER-1251	**Dashboard: Dashboard does not show “version mismatch” alert message while reconnecting to Dashboard when user upgraded IDE from 9.0 to 9.0.3** NOTE 1: Dashboard 9.0.x cannot be used to connect to 9.2.3 Ignition Server. As part of

	upgrading 9.0.x to 9.2.3, the connection from Dashboard to Ignition Server could terminated abnormally as the Ignition Server reboots. The admin needs to reconnect to the 9.2.3 Ignition Server using 9.2.3 Ignition Dashboard. NOTE 2: There are no plans to fix this issue. Customers are advised to follow above workflow recommendation in NOTE 1. This item will be removed next update to the Release Notes.
JUPITER-1225	**RHSA-2014:1365-01] Important: kernel security and bug fix update**
JUPITER-1262	**CVE-2015-0235 GHOST: glibc gethostbyname buffer overflow**
JUPITER-1320	**Identity Engines 9.02 not logging** NOTE: There are no plans to fix this issue. Customers are advised to upgrade to a current release of Identity Engines. This item will be removed next update to the Release Notes.
JUPITER-1210	**RSA Ready Partner Program Certification Test Failures**

9.4. Known Limitations

Item Number	Description
JUPITER-1830	**Access Portal: Mismatch in registered device details before & after mac-auth through portal** If any device is created with sub type “android-phone” or “android-tablet” and this device then gets fingerprinted (during MAC-AUTH) as well from Access Portal then the sub type gets changed to “generic-android”. Any policy defined to use sub type of “android-phone” or “android-tablet” for this particular device will therefore fail. *As a workaround,* any policy that uses the sub type “android-phone” or “android-tablet” need to change to “generic-android” to take care of this potential mismatch. **NOTE: “android-phone” and “android-tablet” will be removed as sub-types from the next release so customers are advised to move away any internal device or access policies which use these two sub-types.**
JUPITER-1836	**Ignition Dashboard: CoA messages are not send when initiated from AAA summary in an HA scenario when Dashboard is connected to the Database secondary node** In case of non-VIP active-active HA setup, if we log into the secondary node and try to trigger CoA from any request in the RADIUS AAA Summary then it fails. *As a workaround,* when you login to the secondary node, trigger the CoA from the Access Logs section of the respective node
JUPITER-1799	**Ignition Dashboard: Inbound Attributes not displayed for Policies in Sitegroup scenario** In case of a Site Group scenario, the configured Inbound attributes are listed in the Access Policy section only for the first node in the site group and when you navigate to the other nodes, this information is missing. *As a workaround,* if you want to use these inbound attributes in the Access Policy then login to the specific node using a different instance of Dashboard and the all the configured inbound attributes are listed and can be used in the policy.
JUPITER-1794	**Guest Manager: Canada SMS gateways are removed and Nextel SMS gateway is added after restoring 9.0.1 GM configuration on 9.2/9.2.3 GM** NOTE 1: As part of importing 9.0/9.1 configuration in Guest Manager, newly added Canada SMS gateways will be removed.

	As a workaround, use the following procedure to add the Canada SMS gateways back in 9.2/9.2.3 Guest Manager-> Administrator-> SMS Gateways, Add following gateway manually. 1. Carrier Name: Cingular, Carrier Gateway: mycingular.net 2. Carrier Name: Bell, Carrier Gateway: “txt.bell.ca 3. Carrier Name: Rogers, Carrier Gateway: pcs.rogers.com 4. Carrier Name: Telus, Carrier Gateway: msg.telus.com NOTE 2: There are no plans to fix this issue. Customers are advised to follow above workflow recommendation in NOTE 1. This item will be removed next update to the Release Notes.
JUPITER-1681	**Ignition Server: Not able to view the dashboard after re-log in to IDE by using re-authorize option. Got "session already exist" after log in the system again.** Sometimes due to some transient communication issue between Ignition Dashboard and Ignition Server, the session established between them is broken. Since this connection is abruptly terminated, the session created on the Ignition Server is not closed gracefully due to which subsequent Dashboard admin login is not possible. *As a workaround,* if you see a session already existing on the Ignition Server then delete that session from the Ignition Server CLI.
JUPITER-1508	**Guest Manager: Able to connect the older GM version (9.1) to the latest 9.2/9.2.3 ignition server.** NOTE 1: Ignition Guest Manager 9.2/9.2.3 is only compatible with Ignition Server 9.2/9.2.3. If you had a Guest Manager 9.1 connected to Ignition Server 9.1 and you then upgraded to Ignition Server 9.2/9.2.3 then the Ignition Guest Manager 9.1 connected to this system doesn’t flag an incompatibility message. However, proper functioning will be impacted as Guest Manager 9.1 is not compatible with Ignition Server 9.2/9.2.3 Customers are advised to upgrade the Guest Manager to 9.2/9.2.3 for proper compatibility with Ignition Server 9.2/9.2.3 NOTE 2: There are no plans to fix this issue. Customers are advised to follow above workflow recommendation in NOTE 1. This item will be removed next update to the Release Notes.
JUPITER-1879	**Ignition Server: Policies using Device Types and Device sub-types stop working after upgrading to 9.2** If any custom device types/sub types (user created) were associated with Internal Device in 9.0.x/9.1 or earlier then they are no longer associated with Internal Device when the data is migrated or Ignition Server is upgraded to 9.2. In addition, any policy using these custom device types/sub types may not work *As a workaround*, recreate the custom device type/sub type and then either associate it with the Internal device or use in the Access Policy.
JUPITER-1922	**Radius request rejected when user trying to authenticate with user name as email address (test@blr.in) when there is another user account present with same name in internal database without any realm(test)** If email based usernames e.g. ‘test@avaya.com’ created via dashboard or guest manager and already there is a user called ‘test’ present in the internal store, then the user test@avaya.com never gets authenticated. If an account with realm (test@avaya.com) exists, do not have an account with the same name but without realm (test) in the internal store.

JUPITER-2156	**[GM]Not able to provide special character _ in the password field for Guest User** Password field for guest user can be configured to accept special characters. However, when the Provisioner is trying to configure a guest user password, the "_" character is not getting considered as a special character *As a workaround*, please provide any other special character apart from "_" while configuring password from the Provisioner flow (if Password field is configured mandatorily to take a special character).
JUPITER-2074	**[Guest Manager] SSLHandshakeException Error shown while navigating to Provisioning Groups,Self-Service, Guest Users and Devices.** While logged in as an Admin, sometimes the following error "*Error:java.net.ssl.SSLHandshakeException: server certificate change is restricted during renegotiation*"" is seen while navigating to any of the screen mentioned above. As a workaround, please re-launch GM and re-login as Admin. If the problem persists, please restart the tomcat service from CLI.
JUPITER-2192	**[Guest Manager]Default route got deleted after reboot on a fresh Guest manager vm** After a fresh GM OVA deployment (after configuring interface IP and Default route), sometimes the default route added gets removed after a VM reboot. NOTE 1: As a workaround, please repeat the Interface and Default route changes (i.e. configure the interface IP again and add back the default route) and trigger a reboot again. This issue is caused by having more than one instance of Guest Manager with same IP address. Customers are advised to ensure there are no duplicated IP addresses configured. NOTE 2: There are no plans to fix this issue. Customers are advised to follow above workflow recommendation in NOTE 1. This item will be removed next update to the Release Notes.
JUPITER-2187	**Not able to delete manually created VSA's after upgrading Ignition server.** As part of upgrading IDE from 9.0.x/9.1.0 to 9.2.3 if the following intermediate upgrade path was followed (i.e. 9.0.x to 9.1 and/or 9.2.2 and finally to 9.2.3) then admin will not be able to delete the custom VSAs created. This issue will not be seen if IDE was directly upgraded from 9.0.x/9.1.0 to 9.2.3 If the admin's intention in deleting the VSA was to create a new one with the same ID then, as a workaround, the admin can create another VSA with the same ID but with a different name
JUPITER-2215	**After Mac Authentication click logout button on success page shows error message.** Post successful user authentication using External Captive Portal, no user session is maintained in Ignition Access Portal and control goes from Ignition Access Portal to WLAN9100. Therefore upon clicking the Logout button on success page user the gets error message. To prevent this, please ensure that the custom Success Page chosen does not have a Logout button in it.

9.5. Application Notes

- **CASE Manager**

- CASE Manager Release 1.0 is compatible with Ignition Server release 9.2.4
- However, CASE Manager 1.0 is not compatible with Access Portal 9.2.1 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 9.2.1
- However the automated process of uploading CASE Wizard Packages is not compatible with Access Portal release 9.2.1. 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 9.2.1
- 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 9.2.1 using the File Manager.
- Additional details in See KCS SOLN273086 @ https://support.avaya.com/kb/ext/SOLN273086

- **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 9.2.1
  - 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.

- **Change of Authorization (CoA)**
  - CoA Reauthorize facilitates changing the VLAN service authorization, but the client may not request a new IP because the client may not have recognized the change. As result client may be disconnected until a new DHCP request is triggered.
  - CoA is not supported for NEAP on all of Avaya ERS switches. Future releases of Avaya ERS switches are planned to support CoA for NEAP.

- **Authenticator Updates**
  - When administrator creates maximum number of authenticators per license limit and tries to modify both authenticator name and IP address fields in single action, then that authenticator will be disabled
  - As work around, admin can perform this edit as two separate actions
    1. Modify Authenticator name in the first attempt
    2. Modify IP address in the second attempt

- **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 9.2.1 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 9.2.1, 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 9.2.1 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”.

10. Upgrade Procedure

10.1. Pre-upgrade Checklist

Ignition Server Checklist

- By design, neither Software Upgrade flow nor Configuration Restore flow form 8.0.x to 9.2.4 is supported.
  - See section “**6. Interoperability and Upgrade Matrix”** for details
- If you are running 8.0.x perform a Software Upgrade or Configuration Restore to release 9.1.0 and then use either Software Upgrade or Configuration Restore to 9.2.3 release.
  - Temporary licenses for R9.x for this process are available on www.avaya.com/identitytrial
- If you are running 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.1.0, 9.2.0, 9.2.1, 9.2.2 or 9.2.3 you may perform Software Upgrade or Configuration Restore to 9.2.4 release.
- As best practice, always perform the following before any upgrade or restore
  - Take a backup of your Ignition Server configuration
  - Take a VMware snapshot of the Ignition Server Virtual Machine while the VM is in shutdown state.

- WLAN 9100 REMINDER
  - Please be reminded, that release 9.0.3 introduces a new Vendor and device-template that must be used to for interoperability with 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 you are migrating from 9.0.0, 9.0.1, 9.0.2 into 9.2.4, the source configuration **must not** have the same Vendor and Device Template names as stated above. You **must** rename existing Vendor Name and Device Template to some arbitrary names **prior** to performing the configuration backup or software upgrade into 9.2.4. This is a **mandatory** procedure otherwise new licensing model for WLAN 9100 will not function properly after Configuration Restore or Software Upgrade.

- If you are migrating from 9.0.3 or 9.1.0 into 9.2.4, then Avaya had already provided the above said Vendor and Device Template built in into the Ignition Server.
- Release 9.2.4 cannot be downgraded to a previous version. If the Ignition server is accidentally upgraded to 9.2.4 without renaming procedure as stated above, please use VM backup snapshot to restore back to original state.

- FABRIC ATTACH REMINDER
  - If your configuration includes manually configured Fabric Attach VSAs, it is **required** to delete any such previously manually configured Fabric Attach VSAs **prior** to performing the configuration backup or software upgrade into 9.2.4. This is a **mandatory** procedure otherwise the Fabric Attach feature will not function properly after Configuration Restore or Software Upgrade.

Dashboard Checklist

- Identity Engines 9.2.4 includes a new Dashboard installer that must be installed. Ignition Server release 9.2.4 cannot be managed from any previous versions of Dashboard.
- Due to updated certificates for the Dashboard as of Release 9.0, it is necessary to delete the following keystore of the certificates. Dashboard keeps the cached keystore of these certificates at following locations:
  - **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**

10.2. Software Upgrade Procedure

- If you are running Ignition Server 8.0.x and would like to migrate to release 9.2.4:
  - Migrate to 9.1.0
    - Take a configuration backup from 8.0.x
    - Deploy a fresh new VM 9.1.0
    - Temp licenses are required (use temp licenses from www.avaya.com/identitytrial)
    - Perform a configuration restore from 8.0.x into 9.1.0
    - Perform a new backup of the 9.1.0 configuration
  - Migrate to 9.2.4
    - Deploy a fresh new VM 9.2.4
    - Temp licenses are required (use temp licenses from www.avaya.com/identitytrial)
    - Perform a configuration restore from 9.1.0 into 9.2.4
    - Perform a new backup of the 9.2.4 configuration
    - New permanent licenses will be required
      - Send email request to datalicensing@avaya.com
    - Perform a new backup of the 9.2.4 configuration with the perm licenses

- If you are running Ignition Server 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.1.0, 9.2.0, 9.2.1, 9.2.2 or 9.2.3 and would like to migrate to release 9.2.4 using a new VM:
  - Take a configuration backup from 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.1.0, 9.2.0, 9.2.1, 9.2.2 or 9.2.3
  - Deploy a fresh new VM 9.2.4
  - Perform a configuration restore from 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.1.0, 9.2.0, 9.2.1, 9.2.2 or 9.2.3 into 9.2.4
  - Perform a new backup of the 9.2.4 configuration
  - New permanent licenses will be required
    - Send email request to datalicensing@avaya.com
  - Perform a new backup of the 9.2.4 configuration with the perm licenses

- If you are running Ignition Server 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.1.0, 9.2.0, 9.2.1, 9.2.2 or 9.2.3 and would like to migrate to release 9.2.4 using Software Upgrade flow:
  - Take a configuration backup from 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.1.0, 9.2.0, 9.2.1, 9.2.2 or 9.2.3

- 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 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.1.0, 9.2.0, 9.2.1, 9.2.2 or 9.2.3 to 9.2.4 using the Package (pkg) file.
- Perform a new backup of the 9.2.4 configuration
- No new licenses are required.

11. 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.

© 2016 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

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/