Avaya Identity Engines Release Notes
Software Release 9.2.2

NN47280-400
Issue 09.02
October 2015

1. Document Summary

Document Version: 09.02
Document Date: October 2015
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
09.01	• Added Application Notes about Access Portal Admin and OUT interfaces on same VLAN. • Added Application Notes about Access Portal OUT interface configuration for DHCP/Static IP address. • Added Application Notes abut CSV Import/Export of Authenticators. • Release Notes for IDE 9.2.2	Ignition Server incorporates an important fix for logging/.Syslog (details below).
09.02	• Fixed typos in Dashboard OS Support section.	

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).
- If you are on release 8.0.x then please also note that restore of the backup from 8.0.x to 9.2.2 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 9.2.2 or take a backup and then restore the config on a fresh 9.2.2 instance. Follow the upgrade procedure in "***Chapter 10. Upgrade Procedure"*** of this document.

- If you are running release 9.0.1, 9.0.2, 9.0.3 or 9.1.0 and would like to migrate to 9.2.2, you have two options:
    - Take a configuration backup from 9.0.1, 9.0.2, 9.0.3 or 9.1.0, deploy a fresh new 9.2.2 VM and perform a configuration restore on the 9.2.2 VM. New licenses will be required. Follow the upgrade procedure in "***Chapter 10. Upgrade Procedure"*** of this document.
    - Perform a software upgrade directly from 9.0.1, 9.0.2, 9.0.3 or 9.1.0 to 9.2.2 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.

4. Hypervisor Platforms Supported

The following VMware ESXi platforms are supported with Identity Engines release 9.2.2:
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 9.2.2:

File Name	Module or File Type	Comments
AIEIS_RHEL_6_5_LINUX-VM_09_02_02_029484_x86_64.ova	Ignition Server OVA files for vSphere 5.1 and 5.5 environments	Ignition Server release 9.2.2. This file is used if fresh VM install option is desired.
LINUX-VM_09_02_02_029484_server_complete.pkg	Ignition Server upgrade package files for vSphere 5.1 and 5.5 environments	Ignition Server release 9.2.2. These files are used if software upgrade option is desired.
DashboardInstaller-9.2.2.29484.exe	Dashboard Installer	Dashboard Installer release 9.2.2 compatible with Ignition Server release 9.2.2.

5.2. Previous Identity Engines software files compatible with Release 9.2.2:

File Name	Module or File Type	Comments
AIGM_RHEL_6_5_LINUX-VM_09_02_00_29095_x86_64.ova	Guest Manager OVA files for vSphere 5. 1 and 5.5 environments	Guest Manager release 9.2.0 is compatible with Ignition Server release 9.2.2.
Avaya_idEngines_IDR_9.2.apk	Android application package	Ignition Device Registration (IDR) App release 9.2.0 is compatible with Guest Manager release 9.2.0.
AccessPortal_09_01_00_027925_x86_64.ova	Access Portal OVA files for vSphere 5.1 and 5.5 environments	
AdminConsoleInstaller-1.0.0.22931.exe	CASE Manager Installer	• CASE Manager Release 1.0 is compatible with Ignition Server release 9.2.2 • 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

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 9.2.2	-	9.2.0	-	9.1.0	-
Guest Manager 9.2	9.2.2	-	9.2.0	-	-
Android IDR App 9.2	-	9.2.0	-	-	-
Access Portal 9.1	9.2.2	-	-	-	8.0(1)
CASE Manager 8.0	-	-	-	9.1.0(1)	-

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

6.2. Supported Software Upgrade flows using Package (pkg) files:

	Compatible from Ignition Server 8.0.x	Compatible from Ignition Server 9.0.x	Compatible from Ignition Server 9.1.0	Compatible from Ignition Server 9.2.0	Compatible from Ignition Server 9.2.1
Ignition Server 9.2.2	Not Supported	Supported	Supported	Supported	Supported

6.3. Supported Configuration Restore flows 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 9.2.2	9.0.x 9.1.0 9.2.0 9.2.1	-	-	-	-
Guest Manager 9.2	-	9.0.x 9.1.0	-	-	-
Android IDR App 9.2	-	-	-	-	-
Access Portal 9.1	-	-	-	8.0	-
CASE Manager 8.0	-	-	-	-	-

7. System Requirements

Software	Software Compatibility	Comments
Ignition Server Release 9.2.2	• 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 9.2.2 software can only be managed with Avaya Ignition Dashboard release 9.2.2.	• 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 9.2.2	• Windows 7 (64 bit) • Windows 8.1 (64 bit) • Windows 2008 (64 bit) • Windows 2012 (64 bit)	• Minimum 2GB RAM memory • US English Windows • Desktop/PC or Laptop •
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 9.2.0	• 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 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
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”.	• Can be downloaded from Google Play
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 & R9.2.2 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 & R9.2.2 SSO
Service Provider Agent	Apache Tomcat 6.X	• Compatible with Identity Engines R9.0.1, R9.0.2, R9.0.3, R9.1.0 & R9.2.2 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 XenMobileMDM	Citrix XenMobile MDM 8.7 and 9.0	• Compatible with Identity Engines R9.2.2
AirWatch MDM	Airwatch MDM v8.0.5	• Compatible with Identity Engines R9.2.2

8. Versions of Previous Release Notes

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 9.0.3, 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"

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"

9. New and Changes in this Release

9.1. New features in this Release

- **AirWatch Mobile Device Management (MDM) Support**
  Identity Engines Release 9.2.x extends the current support for Mobile Device Management (MDM) by integrating third-party AirWatch MDM. In addition, there are enhancements to the display of MDM devices and a new device attribute "Device,device-enrolled" that may be used in an Access Policy.

- **Guest Manager Virtual Appliance**

A collection of new and enhanced features on the Guest Manager:

- Localization – support for non-English languages for Self-Service and Sponsor pages
  - Dutch
  - English (US)
  - French

    - German
    - Italian
    - Portuguese
    - Russian
    - Spanish
  - REST APIs for programmatic provisioning of Users and Devices for network access for use by 3rd party applications
  - Android App for onboarding network attached devices
  - Improved Sponsor workflow - allowing using a group of users on AD as sponsors
  - Schedule facility for Guest Manager configuration backup
  - Added new SMS gateways for Canada

- **Fabric Attach**
  New and enhanced feature support for Avaya Fabric Attach:
  - A new FA client inventory table capturing all the details of the learnt FA Client devices
  - Access Policy Template for access of FA Clients

- **Change of Authorization (CoA)**
  Support for Avaya ERS and WLAN 9100 Change of Authorization of already connected clients:
  - Disconnect
  - Service Re-authorization

- **Access Policy Templates**
  Set of Access Policy Templates that admin can do Copy & Paste & Edit to for quick start with IDE:
  - Template Policy for Domain PCs
  - Template Policy for ERS Switch Administration policy
  - Template Policy for Users accessing a Fabric Connect network
  - Template Policy for MDM policy
  - Template Policy for FA Clients attaching to a Fabric Attach switch.

- **General Usability Features**
  - User defined Device Type and Sub-Type
  - Copy Button for Serial Number
  - IDE CNF account in AD updated every 30days instead of 24hrs
  - Access to AD using Service Account
  - Dashboard windows re-sizing for better clarity
  - Dashboard unified folder for browsing
  - Dashboard version number display on Dashboard
  - Syslog compliance with RFC
  - Right-click to view RADIUS Vendor ID

9.2. Issues Resolved in this Release

Item Number	Description
JUPITER-1593	Guest Manager Guest Users "Error Fetching Records, Please see log for details"
JUPITER-1488	Identity Engines 9.1 CRL automatic update does not work
JUPITER-1332	Ignition Console - DNS Invalid dotted notation: 10.0.10.1 (syntax is N[NN].N[NN].N[NN].N[NN])
JUPITER-1324	IDE 9.02 cannot add a CRL URL with blank spaces.
JUPITER-1283	Guest manager login username case-sensitive.
JUPITER-1198	Ignition Server Syslog Not RFC 3164 Compliant
JUPITER-1474	Dashboard Policies Do Not Accept Spaces, Equal or Pound Signs
JUPITER-1468	Guest Manager - Unable to Disable E-mail User Authentication
JUPITER-1326	Duplicate CNF Issue in Windows Active Directory

JUPITER-1311	Dashboard Scheduled Task Does Not Maintain Root Path Value
JUPITER-1310	Scheduled Backup Status Automatic Refresh & Manual Refresh Issues
JUPITER-839	9.1 Dashboard Login Dialog does not save the IP address
JUPITER-1773	RADIUS protocol engine service restart due to unhandled Active Directory Out of Memory Response Code.
JUPITER-1327	Identity Engines: Vulnerability Assessment for CVE-2014-3566 POODLE Padding Oracle On Downgraded Legacy SSLv3, SSL 3.0
JUPITER-1300	If AD is configured with OU = sales, marketing then IDE will not see it as it is. It would see it as "sales\, marketing.
JUPITER-1921	Possible authentication issue when using MSCHAPv2 workflow with large AD groups as AD response may be fragmented and Ignition Server 9.2 is mishandling this specific fragmentation.
JUPITER-1948	Resolve possible error when launching Dashboard
JUPITER-1970	Resolve possible race condition affecting logging process while Syslog is enabled.

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** Dashboard 9.0.x cannot be used to connect to 9.2.0 Ignition Server. As part of upgrading 9.0.x to 9.2, the connection from Dashboard to Ignition Server could terminated abnormally as the Ignition Server reboots. The admin needs to reconnect to the 9.2.0 Ignition Server using 9.2.0 Ignition Dashboard.
JUPITER-1250	**Dashboard: 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
JUPITER-1268	**Access Portal: While uploading more than 130 MB file under File manager shows blank page**
JUPITER-1266	**Guest Manager: "show httpd" command does not reflect the httpd listen and allow configurations correctly**

9.4. Known Limitations

Item Number	Description
JUPITER-1722	**Ignition Server: The import of a "backup data" does not restore the VLAN Method "Label or ID" for built in VSA's** Identity Engines is shipped to use 'VLAN Label' for 'generic-aruba' and 'generic-trapeze' device templates. Customers could change the template definition instead to use 'VLAN ID" to suit their specific environment. If the customer has changed the default configuration to use "VLAN ID" in the pre-9.1 release and upgrades to 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.

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 GM** 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 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
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 ignition server.** Ignition Guest Manager 9.2 is only compatible with Ignition Server 9.2. If you had a Guest Manager 9.1 connected to Ignition Server 9.1 and you then upgraded to Ignition Server 9.2 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 You need to upgrade the Guest Manager to 9.2 for proper compatibility with Ignition Server 9.2
JUPITER-1420	**Guest Manager: "SOAP Service might be disabled" error seen in Guest Manager GUI when IDE server was rebooted** After performing a reboot/restore/upgrade on Ignition Sever, the above mentioned error is sometimes observed on the Guest Manager. *As a workaround,* do the following: 1) Wait for at least 5 mins after any of the above operation was carried out on the Ignition Server and try again **2)** If the error still persists then from Ignition Dashboard disable/enable the SOAP service.
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-1884	**Not able to create new provisioning group when user selects "sponsor approval" option first and then selects "guest user and device provisioning" option while creating** As a workaround, if admin wants to change group type from "Guest Self Service with Sponsor Approval" to "Guest User and Device Provisioning" then perform the following: 1. Change group type to "Guest Self Service with Sponsor Approval" 2. Unchecked "Sponsor approval required" in Sponsor tab 3. Change group type to "Guest User and Device Provisioning"
JUPITER-1983	**CSV Import/Export of Authenticators** • Change of authorization (CoA) support for Avaya ERS switches and WLAN 9100 was first introduced in IDE Release 9.2. • CoA configuration (such as Shared Secret, Port etc.) of Authenticators is not yet included in CSV Import/Export flow from the Dashboard. • Hence when the same config is imported, the CoA settings will be missing if they were configured for any Authenticator. • As a workaround, manually configure CoA settings for Authenticators post the import operation.

9.5. 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.
- 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 9.1
  - 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.
- **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”.
- **CSV Import/Export of Authenticators**
    - Change of authorization (CoA) support for Avaya ERS switches and WLAN 9100 was first introduced in IDE Release 9.2.
    - Note that CoA configuration of Authenticators is not yet included in CSV Import/Export from the Dashboard.
    - Hence when the same config is imported, the CoA settings will be missing if they were configured for any Authenticator.
    - As a workaround, manually configure CoA settings for Authenticators post the import operation.

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 9.2.2 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 9.2.2 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 or 9.1.0 you may perform Software Upgrade or Configuration Restore to 9.2.2 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 9.2.2, 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 9.2.2. 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 9.2.2, then Avaya had already provided the above said Vendor and Device Template built in into the Ignition Server.
  - Release 9.2.2 cannot be downgraded to a previous version. If the Ignition server is accidentally upgraded to 9.2.2 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 9.2.2. This is a **mandatory** procedure otherwise the Fabric Attach feature will not function properly after Configuration Restore or Software Upgrade.

Dashboard Checklist

- Identity Engines 9.2.2 includes a new Dashboard installer that must be installed. Ignition Server release 9.2.2 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 9.2.2:
  - 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 9.2.2
    - Deploy a fresh new VM 9.2.2
    - Temp licenses are required (use temp licenses from www.avaya.com/identitytrial)
    - Perform a configuration restore from 9.1.0 into 9.2.2
    - Perform a new backup of the 9.2.2 configuration
    - New permanent licenses will be required
      - Send email request to datalicensing@avaya.com
    - Perform a new backup of the 9.2.2 configuration with the perm licenses

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

- If you are running Ignition Server 9.0.1, 9.0.2, 9.0.3 or 9.1.0 and would like to migrate to release 9.2.2 using Software Upgrade flow:
  - Take a configuration backup from 9.0.1, 9.0.2, 9.0.3 or 9.1.0
  - 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, 9.0.3 or 9.1.0 to 9.2.2 using the Package (pkg) file.
  - Perform a new backup of the 9.2.2 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.

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.

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/