avaya.com

Avaya Identity Engines Release Notes
Software Release 9.3.0

NN47280-400
Issue 12.01
September 2016

1. Document Summary

Document Version: 12.01
Document Date: September, 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
12.01	First published Release Notes for IDE 9.3.0	

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 configuration 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.

- As a general best practice guideline, it is highly desired to have a routine configuration backup of each of the Identity Engines applications. Identity Engines have the facility for automated backups. It is recommended to set a schedule for configuration backup in each of the Identity Engines applications.

3. Important Notes about this Release

- If you are running Ignition Server release 9.0.x then please be aware that Software Package upgrade from Ignition Server release 9.0.x to Ignition Server release 9.3.0 is **not** supported.
- If you are running Ignition Server release 9.0.x then please also note that configuration restore of the backup from Ignition Server 9.0.x to 9.3 is **not** supported.
- Should you want to restore your 9.0.x configuration, then first install a fresh 9.1.0 VM using trial licenses and then restore the configuration from 9.0.x into that instance of 9.1.0. Post that you can either upgrade to 9.3.0 or take a backup and then restore the configuration on a fresh 9.3.0 instance.

- If you are running release 9.1.0, 9.2.0, 9.2.1 or 9.2.2 and would like to migrate to 9.3.0, you have two options:
  - Option 1: Take a configuration backup from 9.1.0, 9.2.0, 9.2.1 or 9.2.2, deploy a fresh new 9.3.0 VM and perform a configuration restore on the 9.3.0 VM. New licenses will be required.
  - Option 2: Perform a Software Package upgrade directly from 9.1.0, 9.2.0, 9.2.1 or 9.2.2 to 9.3.0 using the PKG (Package) file.

- If you are running release 9.2.3 or 9.2.4 and would like to migrate to 9.3.0, you have two options:
  - Option 1: Take a configuration backup from 9.2.3 or 9.2.4, deploy a fresh new 9.3.0 VM and perform a configuration restore on the 9.3.0 VM. New licenses will be required.
  - Option 2: Perform a software upgrade from 9.2.3 or 9.2.4 to an intermediate 9.2.5 version using the special purpose PKG (Package) file supplied by Avaya and then upgrade from 9.2.5 to 9.3.0.

- Please be reminded that whenever you deploy fresh new OVA, you will have to obtain new licenses.
  - Please contact datalicensing@avaya,com to request to transfer of your perpetual licenses.
  - You must provide your older Ignition Server Serial Number with your request.
  - Full trial licenses for transitional upgrade process are available on www.avaya.com/identitytrial

- Follow the upgrade procedure in "***Chapter 10. Upgrade Procedure"*** of this document.

4. Hypervisor Platforms Supported

The following VMware ESXi platforms are supported with Identity Engines release 9.3.0:
VMware ESXi and vSphere version 5.1
VMware ESXi and vSphere version 5.5
VMware ESXi and vSphere version 6.0

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 9.3.0:

File Name	File Type	Comments
AIEIS_RHEL_6_5_LINUX-VM_09_03_00_031059_x86_64.ova	Ignition Server 9.3.0 OVA for VMware ESXi	This file is used for fresh VM install.
LINUX-VM_09_03_00_031059_server_complete.pkg	Ignition Server 9.3.0 Software Package file	This file is used for Software Package upgrade.
LINUX-VM_09_02_05_030867_intermediate_server_complete.pkg	Ignition Server 9.2.5 Package file	**IMPORTANT** This file is used for intermediate software upgrade from 9.2.3/9.2.4 only to 9.2.5 as an intermediate step when upgrading to 9.3.0
DashboardInstaller-9.3.0.31059.exe	Dashboard Installer 9.3.0	Compatible with Ignition Server 9.3.0
AIGM_RHEL_6_5_LINUX-VM_09_03_00_031059_x86_64.ova	Guest Manager 9.3.0 OVA for VMware ESXi	Compatible with Ignition Server release 9.3.0 **IMPORTANT**: Guest Manager REST APIs can only be accessed in HTTPS mode from R9.3.0.

5.2. Previous Identity Engines software files compatible with Release 9.3.0:

File Name	File Type	Comments
AccessPortal_09_02_01_030212_x86_64.ova	Access Portal OVA file for VMware ESXi 5.1, 5.5 or 6.0	This file is used for fresh VM install.
Avaya_idEngines_IDR_9.2.apk	Android application package	Ignition Device Registration (IDR) App release 9.2.0 is compatible with Guest

		Manager release 9.3.0 **IMPORTANT**: IDR 9.2 can communicate with Guest Manager 9.3.0 release only over HTTPS

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
Ignition Server & Dashboard 9.3.0	-	9.2.3 9.3.0	-	9.2.0 9.2.1
Guest Manager 9.3.0	9.2.3 9.2.4 9.3.0	-	9.2.0	9.2.0 9.2.1
Android IDR App 9.2	-	9.2.3 9.3.0(1)	-	-
Access Portal 9.2.1	9.2.3 9.2.4 9.3.0	9.2.3 9.3.0	-	-

NOTE (1): Only in HTTPS mode.

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

TO	FROM Ignition Server 8.0.x	FROM Ignition Server 9.0.x
Ignition Server 9.3.0	Not Supported	Not Supported

TO	FROM Ignition Server 9.1.0	FROM Ignition Server 9.2.0	FROM Ignition Server 9.2.1	FROM Ignition Server 9.2.2	FROM Ignition Server 9.2.3	FROM Ignition Server 9.2.4	FROM Ignition Server 9.2.5
Ignition Server 9.3.0	Supported	Supported	Supported	Supported	Supported MUST use an intermediate step 9.2.5	Supported MUST use an intermediate step 9.2.5	Supported

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

	Compatible FROM Ignition Server	Compatible FROM Guest	Compatible FROM Access Portal

	& Dashboard	Manager	
Ignition Server & Dashboard 9.3.0	9.1.0 9.2.x	-	-
Guest Manager 9.3.0	-	9.1.0 9.2.x	-
Access Portal 9.2.1	-	-	9.1.0 9.2.0

7. System Requirements

Software	Software Compatibility	Comments
Ignition Server Release 9.3.0	• VMware ESXi versions 5.1, 5.5 or 6.0 • 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 9.3.0 software can only be managed with Avaya Ignition Dashboard release 9.3.0.	• The VM requires a x86_64 capable environment • 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 9.3.0	• Windows 7 (64 bit) • Windows 8 (64 bit) • Windows 2008 (64 bit) • Windows 2012 (64 bit) • Windows 10 (64 bit)	• Minimum 2GB RAM memory • Windows • Desktop/PC or Laptop
Ignition Access Portal Release 9.2.1	• VMware ESXi versions 5.1, 5.5 or 6.0 • 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 51, 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 9.3.0	• VMware ESXi versions 5.1, 5.5 or 6.0 • 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 • Firefox Browser 45 - 48 • Chrome Browser 48 - 51	• 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”.	• Available for downloaded from Google Play
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 R9.1.0, R9.2.0, R9.2.1, R9.2.2, R9.2.3, R9.2.4 & R9.3.0 SSO
Avaya System Manager	Avaya SMGR release 6.3.17	• Compatible with Identity Engines R9.3.0 SSO
Citrix XenMobile MDM	Citrix XenMobile MDM 8.7 and 9.0	• Compatible with Identity Engines R9.3.0
AirWatch MDM	Airwatch MDM v8.4.3.0	• Compatible with Identity Engines R9.3.0
Microsoft Active Directory	Windows Server 2008 & 2008 R2 Windows Server 2012 & 2012 R2	• Compatible with Identity Engines R9.3.0

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 9.2.0, 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 – April, 2015
File name “NN47280-400_11_04_IDEngines_9_2_4_Release_Notes.pdf”

9. New and Changes in this Release

9.1. Overview of New and Enhanced Features in this Release

- **Password complexity**
  - Following Avaya corporate guidelines, starting from this release, the new password must meet the following complexity checks.
  - Use minimum of eight characters in the password.
  - Password must be a combination of the following character types:
    - Include at least one lowercase letter
    - Include at least one uppercase letter
    - Include at least one number
    - Include at least one special character from !, @, #, $, %, ^, &, *, (,), -, +
    - Note that underscore "-" is not a supported special character
  - New password cannot match the three recently used passwords

- **Guest Manager Enhancements**
  - **Ignition Server Fail-Over for Guest Manager**
    - Starting with this release of Ignition Guest Manager the Guest Manager administrator can configure a Second Appliance IP Address.
    - With this functionality there are two appliances configured on the Guest Manager.
    - The two Ignition Servers must be in HA configuration and not in standalone configuration.
    - Two Ignition Servers in standalone configuration is not supported.
  - **Copy (Cloning) Provisioning Group**
    - Ignition Guest Manager introduces a new enhancement that enables you to create a copy of an existing provisioning group.
    - This feature allows you to clone a Provisioning Group and then make incremental changes for testing the new workflows.
  - **Configuring Logo as a button**
    - Guest Manager administrator can configure a specific URL address to the Logo in User Preferences panel.
  - **Extend expiry of Guest User and Device accounts**
    - This feature enables you to extend the duration of expiry of a guest user or device account(s) at one click.
  - **Customizing End-User Web Portals**
    - This release of Avaya Identity Engines Ignition Guest Manager Configuration allows you to make global customizing that effect the look feel and behavior of the web pages users see in the Guest Manager portals.
  - **HTTPS Redirect**
    - Guest Manager can only be accessed in HTTPS mode from this release.
    - All REST API requests sent over HTTP is redirected to HTTPS.
    - REST client applications sending REST requests over HTTP and expecting HTTP 200 OK response must first handle HTTP Redirect 301 and 302 responses.
  - **Guest Manager Test Mail and SMS configuration**
    - This release of Avaya Identity Engines Ignition Guest Manager Configuration allows you to send a test email or test SMS using the current gateway configuration.
  - **Supporting Language**
    - This release also supports the localization in the Swedish language.
  - **View Guest User and Device details**
    - Starting this release the Guest Manager administrator and provisioner can view the Guest User and Device details using the View button.
  - **Support for Device Sub-Type**
    - Starting this release Device Sub-Type attribute is added for importing and exporting the Device records

- **Change of Authorization (CoA)**
  - This release enhances and adds options to the Identity Engines administrator to control clients access to the network after the clients are already authenticated and authorized to the network.
  - This release adds new CoA commands, enhances the type of clients that CoA commands are applied to and also adds new workflows to re-service the FA Clients.
  - Following is the COA options available:

Identity Engines COA Support			
COA Actions	**Endpoint Client Type**	**WLAN 9100 APs**	**Switches ERS**
COA Disconnect	EAP & non-EAP clients	**Y**	**Y**
COA Re-Authorize	EAP & non-EAP clients	**Y**	**Y**
COA Re-Authenticate	EAP & non-EAP clients	**No**	**Y**
Single & Bulk COA Disconnect	FA Clients	n/a	**Y**
Single & Bulk COA Re-Authorize	FA Clients	n/a	**No**
Single & Bulk COA Re-Authenticat	FA Clients	n/a	**Y**

- **Access Policy with Actions**
  - Starting with this release, a new set of actions Allow With Actions is added under the Access Policy actions.
  - The current Ignition Server Release adds a new and powerful concept in Identity Engines Access Policies.
  - In the previous releases, the key action of a successful authorization policy evaluation was to send Outbound Values. The new Access Policy with Actions allows you to perform additional actions upon successful Authorization Policy. Following are the Actions available in this release:
    - **Provision With** — This Action is the traditional Send Outbound Values action to instruct the Authenticator of what access to be provided using the access-accept or access-reject message.
    - **Register Device** — This Action registers the device in the local store of the Ignition Server. The device MAC address will be registered or updated under the default group if no specific group is set in the Assign Groups action.
    - **Assign Groups** — This Action sets association of the device to a particular group(s) being authorized by this Access Policy.
    - **Trigger COA Disconnect** — This Action triggers a COA-Disconnect command to the Authenticator of the new device being authorized by this Access Policy. Note that, COA is supported only for Avaya ERS switches and WLAN 9100 Access Points.
    - **Email Alert** — This Action sends an Email Alert with the authorization details. The Email is sent to the email address configured in the SMTP configuration.
    - **Expiry Duration** — This Action sets the date and time or duration of expiry for a device, and provides the option to delete the device after expiry.
  - With the current Ignition Server Release the fingerprinting of devices and assigning groups to them setting the date and time or duration of expiry of the devices and selecting to delete a device after it expires can be done through the access policies.
  - Other new enhancements like triggering a COA Disconnect command for onboarded devices and sending an Email alert is added in this release.
  - **Important**: If you are using Access Portal fingerprinting in your current deployment, you will have to make changes in the Access Policy to use Policy Actions. As Ignition Server no longer automatically fingerprints devices from Access Portal. This is a change in behavior. Same note applies if you are using FA Client fingerprinting in your current deployment.

- **OPSWAT Metadefender Endpoint Management (MEM)**
  - Starting with this Ignition Server Release a new directory service, OPSWAT Metadefender Endpoint Management (MEM) is introduced to verify the security and compliance posture of endpoint devices through static analysis. If you are interested in deploying endpoint device posture, you are required to purchase the MEM cloud-based posture service from OPSWAT Inc.

- The endpoint devices must install an MEM client specific to the OPSWAT MEM account. The device attributes along with posture details are stored in the OPSWAT MEM server in the cloud. Ignition Server adds the OPSWAT MEM posture analysis as a Directory Service and fetches devices and stores it's details in the Internal Store.
- To create an OPSWAT MEM server on the Ignition Server Dashboard you must Register IDE application on the OPSWAT Metadefender Endpoint Management Developers Portal (https://gears.opswat.com/developers/app/register).
- A new wizard is added for configuring the OPSWAT MEM server on the Ignition Server Dashboard. To create a new OPSWAT MEM server navigate to Directory Services on the Ignition Server Dashboard.
- The new Identity Engines posture supports Microsoft Windows XP through Windows 10 and above, Apple MAC OSX, and Linux. The posture of mobile devices is not supported. The current Ignition Server Release adds new posture device attributes.

- **Certificate Enhancements**
  - From this release in addition to Certificate Issued to details, the certificate displays now display Issued by, subject alternate name, certificate revocation lists (CRL), validity period, and fingerprint of the certificate.
  - For a RADIUS user authorization policy, the following new Certificates Issuer related authorization constraints are added for the Inbound Attribute Category:
    - Certificate Issuer Common Name
    - Certificate Issuer Country Code
    - Certificate Issuer Email Address
    - Certificate Issuer Locality
    - Certificate Issuer Organization
    - Certificate Issuer Organization Unit
    - Certificate Issuer State/Province

- **Syslog Enhancements**
  - You can select log channels and send channel specific log messages to syslog servers. By default, all the log channels are selected.
  - The log channels are debug, system, access, transaction, security and audit.

- **Extended-HA enhancement**

  The following are enhancements made to the Extended-HA feature:
  - If a user, device, or group detail is deleted from root site that was synced with branch site then it will be deleted on branch site on subsequent import.
  - Improved overall performance of extended HA by exporting only the set (delta) change records to SFTP server. This set (delta) change is determined based on last successful export time.
  - You cannot have more than one export and more than one import schedule on the same
  - Ignition Server. However, if these schedules are restored from backup taken from previous releases you may see multiple schedules being coexisting.
- **Sub-Authenticator enhancement**
  - To use Service Set Identification (SSID) based server certificate, a mapping between an SSID and a server certificate must be established. The sub-authenticator allows you to specify an authenticator value for the authenticator attribute and the value must match exactly for mapping the certificate.
  - The Called-Station-ID attribute format is <macaddress:SSID>. From this release, you can select Contains/Equals/Starts With/Ends With operator from the drop-down list for Called-Station-ID attribute and specify only the SSID as authenticator value to distinguish the sub-authenticator.
  - For all other authenticator attributes, Equals operator is selected by default.

- **Fabric Attach enhancements**

  This release introduces new capabilities for managing access of FA Clients:
  - **FA Clients re-servicing** — An example use case for FA Clients is that after the initial deployment of WLAN 9100 APs, you need to change the VLANs and ISIDs that service a set of 9100 APs. Using this new feature, you simply apply a filter to select the desired set of 9100 APs and then apply a COA bulk re-authenticate, on the FA Clients inventory table. This makes sure the FA

Clients are re-authenticated and go through the updated Access Policy that will apply new VLANs and ISIDs to provide the new service for the FA Clients.

- **FA Clients Dual Keys** — This feature requires an appropriate FA Switch software code level. New FA VSAs facilitates this feature where the FA Switch may be configured not to decline FA Client access due to mismatch of FA Security Key. But rather attempt to authenticate the FA Client against the FA Policy Server (Identity Engines) and provide the FA Security Key status to Ignition Server.
- **Trusted FA Client** — This feature requires an appropriate FA Switch software code level. New FA VSAs facilitates this feature where FA Policy Server (Ignition Server) controls the trust of the FA Client on which VLAN: ISID binding the FA Client is trusted. Trusted FA Client is useful in a multi-tenant environment to make sure that FA Clients from different tenants do not overlap with service requests resulting in a security breach.

- **Additional Enhancements**
  - **Kerberos Support in MS-CHAPv2 flow** - Default authentication protocol used in SMB messages is changed from NTLM to Kerberos. You have the choice to either use this default option (Kerberos) or use NTLMv1 or anonymous login option while connecting to AD.
  - **RFC 4675** - Starting this release four new attributes are added in RADIUS Dictionary from RFC 4675. Following is the newly added attributes list:
    - Egress-VLANID
    - Ingress-Filters
    - Egress-VLAN-Name
    - User-Priority-Table
  - **VMware ESXi 6.0 Support** - Starting this release, Ignition Server and Guest Manager can be deployed on VMware's ESXi server version 6.0.
  - **Max Devices per User** - For a RADIUS user authorization policy, you can restrict the maximum number of devices per user, using the newly added max-devices-per-user authorization constraints for a Device Attribute Category. To use this feature, registering a device is mandatory for this rule, without which the functionality of this attribute doesn't work.
  - Dashboard Internationalization - Starting this release, Ignition Dashboard can now be installed on non-English Windows machines as well. Menus and presentations are displayed in English however installation of the Dashboard does not require US-English PCs.

9.2. Issues Resolved in this Release

Item Number	Description
JUPITER-1189	Ignition Server: Running Packet Capture Orphaned if Dashboard Crashes or Client PC Shutdown
JUPITER-1225	RHSA-2014:1365-01] Important: kernel security and bug fix update
JUPITER-1262	CVE-2015-0235 GHOST: glibc gethostbyname & CVE-2015-7547 glibc buffer overflows
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.
JUPITER-1859	Ignition Server: Policies using Device Types and Device sub-types stop working after upgrading to 9.3
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).
JUPITER-1982	Syslog observation during beta trials
JUPITER-2074	[Guest Manager] SSLHandshakeException Error shown while navigating to Provisioning Groups, Self-Service, Guest Users and Devices
JUPITER-2321	Identity Engines: Failover functionality of proxy radius server doesn't work
JUPITER-2323	IDE 9.2.3 Duplicate machine accounts causing unique constraint error still occurring

JUPITER-2324	IDE 9.2.3 EAP-TLS is shown as MAC-AUTH in the IDE failed authentication logs when the CN is a number
JUPITER-2388	Security Vulnerabilities (OpenSSL + Apache)
JUPITER-2399	AD Anonymous Service account not enabled
JUPITER-2498	Ignition Scheduled Backup Failure Due To Use Of Insecure Ciphers
JUPITER-2540	Password changes when created user account is viewed
JUPITER-2821	CRL time stamp sync issue between CRL publish time and IDE dashboard under certificate revocation list last update.
JUPITER-2872	user principal name fix for light speed
JUPITER-2889	Adding Base and Delta CRL URLs to Certificate Revocation List Breaks EAP-TLS Revocation Checking
JUPITER-3042	Problem in authorization policy rule execution when posture is enabled
JUPITER-3106	Device record import via dashboard CSV file template fails

9.3. Outstanding Issues

Item Number	Description
JUPITER-1210	RSA Ready Partner Program Certification Test Failures
JUPITER-3220	Notify_Logging_ Service Repeatedly Restarted Note that authentication and authorization services are not affected.
JUPITER-3259	Disable insecure ciphers in the SFTP/SCP protocol exchange for scheduled backup Ignition Server now supports highly secure aes-ctr type ciphers in the SFTP/SCP protocol exchange. However, the support for less secure CBC type ciphers still remains in the system for support with legacy remote file servers. These ciphers will be disabled in a future release.

9.4. Known Limitations

Item Number	Description
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 Site-group 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-2773	Ignition Dashboard – [IGD] Devices-“Bulk delete” fails If the bulk delete operations results in deleting large number of devices (greater than 10K devices), sometimes an error window appears with a message “Could not delete devices in

	the table" The operation has actually completed and sometimes this message appears incorrectly. *As a workaround*, just click "Ok" and refresh the screen to see the changes take effect.
JUPITER-3124	[IGD]Dashboard is not logging out automatically to take affect with new password after changing the password from CLI Sometimes after changing the password from CLI, the Dashboard doesn't disconnect automatically and force user to connect with the new password. *As a workaround*, always close any active Dashboard session before initiating password change from CLI or perform the password change operation from Dashboard
JUPITER-3252	The RADIUS attribute Egress-VLANID for RFC 4675 support was made as Unsigned 32 instead of Octet As workaround until this issue is fixed, please use a scientific calculator to convert the desired value for the attribute so that you can enter it as integer in the Dashboard. The attribute should be sent properly to the Authenticator though.

9.5. Important Application Notes

It is strongly recommended to thoroughly read the following Application Notes before upgrading your system in order to ensure a smooth transition:

- **Password Related Updates**
  - This release implements Avaya corporate guidelines for enhanced password complexity for increased security protection:
  - A password complexity check is now enforced for any new password configured in the Ignition Server or Ignition Guest Manager
  - A password history is now maintained on Ignition Server and Ignition Guest Manager that prevents the admin from specifying or repeating any older password. For this release, the number is set to 3 (meaning admin cannot repeat any of the 3 earlier provided passwords)

- **Guest Manager HTTPS**
  - All REST API requests sent over HTTP will be redirected to HTTPS.
  - REST client applications sending REST requests over HTTP and expecting HTTP 200 OK response must first handle HTTP Redirect 301 and 302 responses."

- **Policy with Actions**
  - A new and powerful "Allow with Actions" option is provided in RADIUS/MAC Access Policies that allow the admin to perform the fingerprinting related operations.
  - Access Portal Fingerprinting
    - Ignition Server release 9.3 no longer automatically fingerprints devices from Access Portal
    - All fingerprint configurations for Access Portal devices is now configured and controlled using the Allow with Actions feature
    - This was done in order to streamline all fingerprinting options through same consistent method
  - FA Client Fingerprinting
    - Ignition Server release 9.3 no longer automatically fingerprints FA Client devices
    - The Access Portal and FA Client fingerprint is now controlled through this "Policy with Actions" flow
    - Use the inbound FA-Client-Type attribute coming from the FA Switch to identify and FA Client device
    - This was done in order to streamline all fingerprinting options through same consistent method
  - The actions that can be performed as part of this flow includes

        - Register Device
        - Assign Groups
        - Set Expiry date/duration
        - Trigger COA disconnect
        - Send Email Alert
    - Read through the Ignition Server Administration guide to understand the logic of Policy with Actions

- **Change of Authorization (CoA)**
    - Please be aware that 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.
    - In order to make use of the "Replay Protection" security feature, you must have the switch be configured to use NTP. Kindly sync up the time on the Ignition Server and ERS/WLAN 9100 with a NTP Server. In the absence of this sync, disable the "Replay Protection" setting to get the CoA functionality working.
- **Ignition Device Registration (IDR) Smartphone App**
    - IDR 9.2 APP can only communicate via HTTPS with Guest Manager 9.3 release. Support for HTTP is no longer available in IDR APP if it wishes to communicate with Guest Manager 9.3 release.

- **Syslog Configuration**
    - Any Syslog related settings on the Ignition Server are not restored as part of the configuration backup/restore unless the "Primary node network configuration" checkbox is enabled as part of the restore workflow from Ignition Dashboard.
    - Be aware that by checking the checkbox "Primary node network configuration" the IP addresses from the backup configuration file will replace the IP addresses currently configured on the Ignition Server.
    - This is an existing behavior and not something newly introduced and mentioned here so that customers take a note.

- **Posture Service**
    - Microsoft has taken a business decision not to support Posture MS-NAP as of Windows 10 and up.
    - With Identity Engines release 9.3, Avaya offers a new posture feature that is part of the Ignition Server Base license and is based on interworking with a 3rd party cloud-based posture service from OPSWAT Inc.
    - Avaya recommends customers to purchase the OPSWAT Metadefender Endpoint Management (MEM) Cloud Service that helps in Posture assessment. Ignition Server can sync up with OPSWAT MEM and take Authorization decisions based on the Posture related attributes obtained from this cloud service.
    - No new IDE license is needed to integrate with OPSWAT MEM.
    - Please note that having devices with both MDM and OPSWAT Posture agents installed on them is not a supported configuration on the Ignition Server.
    - Please note that OPSWAT Posture for mobile devices is not supported on the Ignition Server.

- **Kerberos Support in MS-CHAPv2 flow**
    - Default authentication protocol used in SMB messages is changed from NTLM to Kerberos
    - Customers have the choice to either use this default option (Kerberos) or use NTLMv1 or Anonymous login option while connecting to AD. This setting can be specified via a CLI
    - *Usage:*

      "directory-service protocol <protocol>" where protocol can be
      anonymous
      serviceaccount //used for NTLMv1
      kerberos

- **Fabric Attach**
    - CoA Reauthorize is not yet supported in ERS with FA Clients.
    - FA Client devices were automatically fingerprinted till release 9.2.3. From the 9.3 release, fingerprinting will only happen if configured through the "Policy with Actions" workflow.
    - A sample "Policy with Actions" rule for this workflow could look like below for AP 9100:

IF Inbound.Inbound-Fabric-Attach-Client-Type = 6 THEN Allow with Actions
Register Device
Assign Groups: MAC
Expiry Duration: 2016-08-23 14:36:05

NOTE: The AP 9100 identifies itself as Fabric-Attach-Client-Type = 6

- **Active Directory**
  - Ignition Server needs SMB v1 to be enabled on Windows Server to establish the initial connection with the Active Directory. If SMB version1 is disabled on Windows Server 2012, then please refer to the below mentioned article which provides a workaround to enable it.
    https://support.microsoft.com/en-us/kb/2976994

- **Max-Devices**
  - Starting Ignition Server 9.3 release, admin can take certain authorization decisions based on number of devices registered to a user. This feature can enable the admin to restrict the number of devices using which the network could be accessed. This is achieved using a device based attribute constraint in the access policy and a sample rule could look like below:

    IF Device.max-devices-per-user < 3 THEN Allow
    Send Outbound Values: Session-Timeout

  - **NOTE:** For this functionality to work, the admin needs to ensure that the device is registered using the new "Policy with Actions" workflow introduced in this release or ensuring that the username attribute is populated correctly for all the devices corresponding to a user.

- **Access Portal**
  - The configuration related to fingerprinting devices and associated actions like associating groups, specifying expiry duration etc. is no longer supported from the Access Portal Server screen. The same settings have moved to the "Policy with Actions" workflow.
  - If you are currently using the Device Fingerprinting from the Access Portal, then you MUST make changes to the Access Policy to explicitly fingerprint the devices coming from the Access Portal. If these changes are not done, then devices will NOT get fingerprinted and your workflow may break.
  - A sample "Policy with Actions" rule for fingerprinting a device from Access Portal could look like below:

    IF User.group-member contains [IgnitionTemplate-Guests-Grp] THEN Allow with Actions
    Register Device
    Assign Groups: GUEST
    Expiry Duration: 0 day(s) 8 hours
    Delete on Expiry

  - 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”.

- Please note that when using the Access Portal as external Captive Portal for the WLAN 9100, then user accounts with passwords containing certain special characters($, #, &) may fail to get authenticated. The second authentication (triggered by AP 9100) fails in case the password contains certain special characters. As a workaround until this is fixed, chose the "External Splash" option on the AP 9100.
- Please note that when using the Access Portal as external Captive Portal for the WLAN 9100, then if the "Redirect Secret" (shared key between Access Portal and AP 9100) contains certain special characters ($, #, &) the second authentication (triggered by AP 9100) fails for all user accounts. No workaround exist. Avoid using these special characters in the “Redirect Secret”.

10. Upgrade Procedure

10.1. Pre-upgrade Checklist

Ignition Server Checklist

- By design, neither Software Upgrade flow nor Configuration Restore flow form 9.0.x to 9.3.0 is supported.
- If you are running 9.1.0, 9.2.x you may perform Configuration Restore to 9.3.0 release.
- If you are running 9.1.0, 9.2.x you may perform Software Package upgrade as follows:
  - If you are running 9.1.0, 9.2.0, 9.2.1, 9.2.2 you may perform Software Upgrade directly to 9.3.0 release.
  - If you are running 9.2.3 or 9.2.4, you may perform Software Upgrade to 9.3.0 release via an intermediate 9.2.5 path (i.e. 9.2.3/9.2.4 to 9.2.5 then to 9.3.0)
- 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**.

Dashboard Checklist

- Identity Engines 9.3.0 includes a new Dashboard installer that must be installed. Ignition Server release 9.3.0 cannot be managed from any previous versions of Dashboard.
- Due to updated certificates for the Dashboard as of Release 9.0.0, 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**
  - **Win 10 > 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

- **Migrating from IDE 9.0.x**
  If you are running Ignition Server release 9.0.x and would like to migrate to Ignition Server release 9.3.0:
  - First step migrate to 9.1.0
    - Take a configuration backup from 9.0.x

        - Deploy a fresh new VM 9.1.0
        - Perform a configuration restore from 9.0.x into 9.1.0
        - Perform a new backup of the 9.1.0 configuration as a safety precaution step
        - **NOTE:** No temporary licenses are needed for this intermediate step. You will be able to restore the configuration file and re-take a backup of the configuration without licenses applied.
        - **NOTE:** If your 9.0.x configuration includes manual configuration of WLAN 9100, make sure to follow the Release Notes instructions of 9.1 on how to migrate to native IDE support for WLAN 9100.
    - Second step migrate 9.1.0 to 9.3.0
        - Deploy a fresh new VM 9.3.0
        - Perform a configuration restore from 9.1.0 into 9.3.0
        - Perform a new backup of the 9.3.0 configuration as a safety precaution step
        - New perpetual licenses will be required. Send email request to datalicensing@avaya.com
        - Perform a new backup of the 9.3.0 configuration once the perpetual licenses are installed
        - **NOTE:** Until you receive your new perpetual licenses from Avaya, you may use temp licenses www.avaya.com/identitytrial

- **Migrating from IDE 9.1.0 or 9.2.x using fresh OVA install**
  If you are running Ignition Server 9.1.0 or 9.2.x and would like to migrate to release 9.3.0 using a new VM:
    - Take a configuration backup from your 9.1.0 or 9.2.x
    - Deploy a fresh new VM 9.3.0
    - Perform a configuration restore from 9.1.0 or 9.2.x
    - Perform a new backup of the 9.3.0 configuration
    - New perpetual licenses will be required. Send email request to datalicensing@avaya.com
    - Perform a new backup of the 9.3.0 configuration once the perpetual licenses are installed
    - **NOTE:** Until you receive your new perpetual licenses from Avaya, you may use temp licenses www.avaya.com/identitytrial

- **Migrating from IDE 9.1.0, 9.2.0, 9.2.1 or 9.2.2 using Software Package File Upgrade process:**
  If you are running Ignition Server 9.1.0, 9.2.0, 9.2.1 or 9.2.2 and would like to migrate to release 9.3.0 using Software Package upgrade flow:
    - Take a configuration backup from 9.1.0, 9.2.0, 9.2.1 or 9.2.2
    - 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 Software Package upgrade directly from 9.1.0, 9.2.0, 9.2.1 or 9.2.2 to 9.3.0 using the Package (pkg) file
    - Perform a new backup of the 9.3.0 configuration
    - No new licenses are required

- **Migrating from IDE 9.2.3 or 9.2.4 using Software Package File Upgrade process:**
  If you are running Ignition Server 9.2.3 or 9.2.4 and would like to migrate to release 9.3.0 using Software Package upgrade flow:
    - 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 intermediate Software Package upgrade from 9.2.3 or 9.2.4 to 9.2.5 using the intermediate Package (pkg) file.
    - Take a configuration backup from 9.2.5
    - 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 Software Package upgrade directly from 9.2.5 to 9.3.0 using the Package (pkg) file.
    - Perform a new backup of the 9.3.0 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.

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

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/