avaya.com

Avaya Identity Engines Release Notes
Software Release 9.3.3

NN47280-400
Issue 15.02
February 2018

1. Document Summary

Document Version: 15.02
Document Date: February, 2018
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
15.01	First published Release Notes for IDE 9.3.3	
15.02	Revised published Release Notes for IDE 9.3.3 for Network Analytics 9.3.3	

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 9.3.3 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 9.3.3 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 9.3.3 or take a backup and then restore the configuration on a fresh 9.3.3 instance.

- If you are running release 9.1.0, 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1 or 9.3.2 and would like to migrate to 9.3.3, you have two options:
  - Option 1: Take a configuration backup from 9.1.0, 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1 or 9.3.2, deploy a fresh new 9.3.3 VM and perform a configuration restore on the 9.3.3 VM. Updated licenses will be required.
  - Option 2: Perform a Software Package upgrade directly from 9.1.0, 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1 or 9.3.2 to 9.3.3 using the PKG (Package) file. No updated licenses will be required.

- If you are running release 9.2.3 or 9.2.4 and would like to migrate to 9.3.3, you have two options:
  - Option 1: Take a configuration backup from 9.2.3 or 9.2.4, deploy a fresh new 9.3.3 VM and perform a configuration restore on the 9.3.3 VM. Updated 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 9.3.3. No updated licenses will be required. Note that the 9.2.5 intermediate package file is included in the zip file of the 9.3.3 package file.

- Please be reminded that whenever you deploy fresh new OVA, you will have to obtain new licenses.
  - Please contact datalicensing@extremenetworks,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 9.3.3:

VMware ESXi and vSphere version 5.5
VMware ESXi and vSphere version 6.0
VMware ESXi and vSphere version 6.5

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 9.3.3:

File Name	File Type	Comments
AIEIS_RHEL_6_5_LINUX-VM_09_03_03_032442_x86_64.ova	Ignition Server 9.3.3 OVA for VMware ESXi	This file is used for fresh VM install.
LINUX-VM_09_03_03_032442_server_complete.pkg	Ignition Server 9.3.3 Software Package file	This file is used for Software Package upgrade.
DashboardInstaller-9.3.3.32442.exe	Dashboard Installer 9.3.3	Compatible with Ignition Server 9.3.3

5.2. Previous Identity Engines software files compatible with Release 9.3.2:

File Name	File Type	Comments
AIGM_RHEL_6_5_LINUX-VM_09_03_02_032201_x86_64.ova	Guest & IoT Manager 9.3.2 OVA for VMware ESXi	Not compatible with Ignition Server lower releases than 9.3.2
AccessPortal_09_03_02_032201_x86_64.ova	Access Portal 9.3.2 OVA file for VMware ESXi	This file is used for fresh VM install.
AINA_RHEL_6_5_LINUX-VM_09_03_02_032302_x86_64.ova	Ignition Analytics 9.3.2 OVA for VMware ESXi	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 & IoT Manager release 9.3.2 **IMPORTANT**: **IDR 9.2 can communicate with Guest & IoT Manager 9.3.2 release only over HTTPS**
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, 9.3.1, 9.3.2 or 9.3.3**

6. Interoperability and Upgrade Matrix

6.1. Supported Interoperability of Identity Engines Applications:

	Compatible Ignition Server &Dashboard	Compatible Guest & IoT Manager	Compatible Android IDR App	Compatible Access Portal	Compatible Network Analytics
Ignition Server & Dashboard 9.3.3	-	9.3.2	-	9.2.0 9.2.1 9.3.2	9.3.0 9.3.2
Guest & IoT Manager 9.3.2	9.3.2 9.3.3	-	9.2.0	9.2.0 9.2.1 9.3.2	9.3.0 9.3.2
Android IDR App 9.2	-	9.2.3 9.3.0(1) 9.3.2(1)	-	-	-
Access Portal 9.3.2	9.3.2 9.3.3	9.3.0 9.3.2	-	-	9.3.0 9.3.2
Network Analytics 9.3.3	9.3.1 9.3.2 9.3.3 9.4.0	9.3.0 9.3.2 9.4.0	-	9.2.0 9.2.1 9.3.2	-

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 9.3.3	Not Supported	Not Supported

TO	FROM Ignition Server 9.1.0	FROM Ignition Server 9.2.0 / 9.2.1 / 9.2.2	FROM Ignition Server 9.2.3 / 9.2.4	FROM Ignition Server 9.2.5	FROM Ignition Server 9.3.0/9.3.1/9.3.2
Ignition Server 9.3.3	Supported	Supported	Supported MUST use an intermediate step 9.2.5	Supported	Supported

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

	Compatible FROM Ignition Server & Dashboard	Compatible FROM Guest & IoT Manager	Compatible FROM Access Portal	Compatible FROM Network Analytics
Ignition Server & Dashboard 9.3.3	9.1.0 9.2.x 9.3.0 9.3.1 9.3.2	---	---	---
Guest & IoT Manager 9.3.2	---	9.1.0 9.2.x 9.3.0	---	---
Access Portal 9.3.2	---	---	9.2.0 9.2.1	---
Network Analytics 9.3.3	---	---	---	9.3.0 9.3.2

7. System Requirements

Software	Software Compatibility	Comments
Ignition Server Release 9.3.3	• VMware ESXi versions 5.5 or 6.0 or 6.5 • 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 9.3.3 software can only be managed with Avaya Ignition Dashboard release 9.3.3.	• 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 9.3.3	• Windows 7 (64 bit) • Windows 8 (64 bit) • Windows 10 (64 bit) • Windows Server 2008 (64 bit) • Windows Server 2012 (64 bit)	• Minimum 2GB RAM memory • Windows • Desktop/PC or Laptop
Ignition Access Portal Release 9.3.2	• VMware ESXi versions 5.5 or 6.0 or 6.5 • Installation on a VMware ESXi server is done using an OVF file which already incorporates the OS FreeBSD. • Microsoft IE Browser 11 • Firefox Browser 54 - 58 • Chrome Browser 56 –60	• 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 & IoT Manager Release 9.3.2	• VMware ESXi versions 5.5 or 6.0 or 6.5 • 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 • Firefox Browser 54 - 58 • Chrome Browser 56 – 60	• 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 9.3.3	• VMware ESXi versions 5.5 or 6.0 or 6.5 • 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 • Firefox Browser 54 - 58 • Chrome Browser 56 – 60	• The VM requires a x86_64 capable environment • Minimum 2 CPUs (default is 4 CPU) • Minimum 4 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
Avaya Flare	• Identity Engines release 9.3.3 and up does not support Avaya Flare • Identity Engines release 9.3.3 and up does not support Avaya System Manager • Identity Engines release 9.3.3 and up does not support Aura SSO	
Avaya System Manager	• Identity Engines release 9.3.3 and up does not support Avaya System Manager • Identity Engines release 9.3.3 and up does not support Aura SSO	
Citrix XenMobile MDM	Citrix XenMobile MDM 8.7 and 9.0	• Compatible with Ignition Server R9.3.3
AirWatch MDM	Airwatch MDM v8.4.3.0	• Compatible with Ignition Server R9.3.3
Microsoft Active Directory	Windows Server 2008 & 2008 R2 Windows Server 2012 & 2012 R2	• Compatible with Ignition Server R9.3.3

8. Versions of Previous Release Notes

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”

Identity Engines Software release 9.3.0, Release Date – September, 2016
File name “NN47280-400_12_01_IDEngines_9_3_0_Release_Notes.pdf”

Identity Engines Software release 9.3.1, Release Date – September, 2016
File name “NN47280-400_13_01_IDEngines_9_3_1_Release_Notes.pdf”

Identity Engines Software release 9.3.1, Release Date – November, 2016
File name “NN47280-400_13_02_IDEngines_9_3_1_Release_Notes.pdf”

Identity Engines Software release 9.3.1, Release Date – January, 2017
File name “NN47280-400_13_03_IDEngines_9_3_1_Release_Notes.pdf”

Identity Engines Software release 9.3.2, Release Date – May, 2017
File name “NN47280-400_14_01_IDEngines_9_3_2_Release_Notes.pdf”

Identity Engines Software release 9.3.2, Release Date – June, 2017
File name “NN47280-400_14_02_IDEngines_9_3_2_Release_Notes.pdf”

9. New and Changes in this Release

9.1. Overview of New and Enhanced Features in Recent 9.3.x Releases

9.1.1 New and Enhanced Features in Releases 9.3.0

- **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 & IoT Manager Enhancements**
  - **Ignition Server Fail-Over for Guest & IoT Manager**
    - Starting with this release of Ignition Guest **& IoT** Manager the Guest **& IoT** Manager administrator can configure a Second Appliance IP Address.
    - With this functionality there are two appliances configured on the Guest **& IoT** 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 **& IoT** 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 **& IoT** 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 **& IoT** Manager Configuration allows you to make global customizing that effect the look feel and behavior of the web pages users see in the Guest **& IoT** Manager portals.
  - **HTTPS Redirect**
    - Guest **& IoT** 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 & IoT Manager Test Mail and SMS configuration**
    - This release of Avaya Identity Engines Ignition Guest **& IoT** 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 **& IoT** 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 **& IoT** 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.

9.1.2 New and Enhanced Features in Releases 9.3.1

- **Network Analytics**
  - **Analytics Dashboard and Reports**
    - Network Analytics Dashboard provides overview of network access summary of last 7 days.
    - Graphs on Network Analytics Dashboard displays authentication trends based on Access Requests, Ignition Servers and Users/Devices.
    - Network Analytics reports are of four categories, Authentication, Usage, Guest Access and FA Clients.
    - Graph on Network Analytics reports displays the top 10 results and table displays top 100 results.
    - Authentication Reports provides statistics and trends based on user access authentications.
    - Usage Reports provides statistics and trends based on the network usage by Users and Devices.
    - Guest Access Reports provides statistics and trends for Guest User authentications and Guest sessions.
    - FA Client Reports provides statistics and trends based on the authentication of Fabric Attach Clients.
    - Reports can be exported in PDF, HTML and CSV formats.
    - Administrator can search through the table for any text in the table.
  - **Administration**

- User can configure Company Settings, including Company Name and Logo; also there is a provision to restore the settings using Restore Defaults option.
- User can configure Email Settings, which will be used by scheduler for sending reports, as well user can test the Email configuration once configured using Test Configuration option.
- User can Export/Import configuration which contains Company Settings, Email (SMTP) settings and License.
- User can take DB Backup which includes Report data, Scheduler jobs metadata, and it uses SFTP, on the backup page user can view Backup Status and Last Backup details.
- User can Restore previously backed up DB from SFTP server, on the Restore page user can view Restore Status and Last Restore details.

o **Scheduler**
- Automatic generation of various reports at specified recurring intervals.
- Schedule one time or Recurrence job, as well as immediate run or on a particular date run.
- Schedule Daily, Weekly OR Monthly multiple occurrences job.
- Can download or email scheduled reports, in PDF, HTML or CSV format.

o **Monitor Logs and Trouble Ticketing**
- User can view Application and Scheduler logs.
- User can create Trouble Ticket at any point of time using Trouble Ticket option, which will collect all required logs along with configuration in zip format and download automatically at default download location of the machine.

o **System**
- Avaya Ignition Network Analytics supports KRS licensing and to apply license internet access is not required.
- User can install license using Choose a File or Copy Paste option.
- License details can be viewed under License details section on same page.
- Network Analytics is provided as a Virtual Appliance application for VMware ESXi

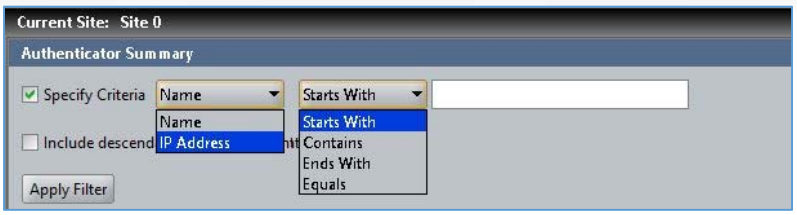
9.1.3 New and Enhanced Features in Releases 9.3.2

- **Ignition Server & Dashboard**

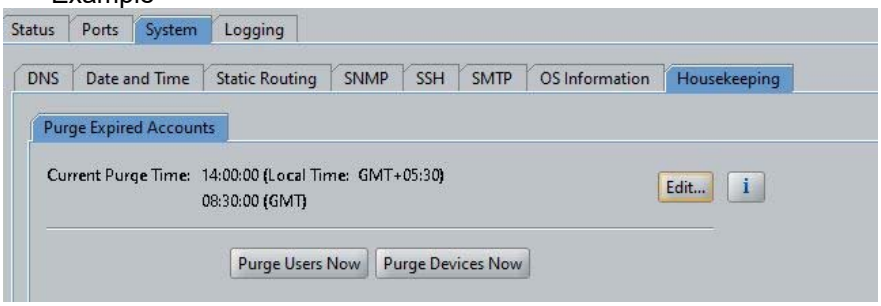
o **Alignment and Consistency of Filenames**
- Alignment of Identity Engines export filenames
- All filenames include: abbreviation of the application, release number, short content description, IP address of the application, date, and time.
- Example: “IGS_9.3.2_users_10.133.140.25_20170201_153942.csv”
- Abbreviation of Identity Engines applications:
  - IGS = Ignition Server
  - IGM = Ignition Guest & IoT Manager
  - IAP = Ignition Access Portal
  - INA = Ignition Network Analytics
  - IGT = Ignition Guest Tunneling

o **Authenticator Export and Import from Root Container**
- Authenticators Import and Export are now only allowed from Root container. Child containers do not have the option to export or import Authenticators.
- If any issue is encountered with a single record, only that specific Authenticator will not be imported and will not have impact on other Authenticator entries.

o **Display Filters for Authenticators**
- Customers with large number of Authenticators can now filter the display out on:
  - Authenticator Name
  - Authenticator IP Address
- Example filter



- o **CSV Import of Users and Devices**
  - Import of Users and Devices enhanced to allow import of at least the key fields:
    - Username for import of Users
    - MAC Address for import of Devices
  - In addition, extra columns beyond the required format are ignored
- o **Extended-HA**
  - Preventing admin error of configuring both recurring export and recurring import for Extended-HA
- o **Clone Outbound Value**
  - Allow admin to clone an Outbound Value eliminates user errors
  - An Outbound may be configured to be comprised of a number of Outbound Attributes that admin may want to modify only a subset for different network services (e.g. VLAN:ISID) while maintaining other Outbound Attributes the same.
  - This feature allows to modify only a subset of Outbound Attributes.
- o **Ignition Server Housekeeping Task of Purge Time for Expired Records**
  - Admin can now set the specific time of day that purging of Expired Users and Expired Devices occur.
  - This feature enables to avoid conflicts with records with short term expiration time
  - This feature also allows for better timing control of database housekeeping operations
  - Example



- o **Ignition Server Security Enhancement - Login History Display**
  - Display of last successful login
  - Display of the number of failed login attempted since last successful login
- o **Ignition Server RFC 4675**
  - Enhanced Ignition Dashboard configuration of RFC 4675 Outbound attribute
- o **Ignition Server COA Replay Change of Default Setting**
  - COA Replay default setting for an Authenticator is now aligned with the default setting on the ERS switched.
- o **Ignition Server Quick Add MAC Address**
  - Added ability to add MAC address of user device from the Actions of user authentication logs

- **Access Portal**
  - o Access Portal can now collect Social Media data for users who consent to login using Social Media:
    - Facebook
    - LinkedIn
    - Google+
  - o Access Portal may be configured to send Social Media data up to two syslog servers
  - o Example of Social Media data for LinkedIn:
    - email
    - company name

        - 'id'
        - 'email-address'
        - 'first-name'
        - 'last-name'
        - 'location'
        - 'industry'
        - 'num-connections'
        - 'positions'
    - Example of Social Media data for Facebook:
        - email
        - name
        - id
        - about
        - birthday
        - education
        - location
        - hometown
        - likes
        - work
        - tagged_places
    - Example of Social Media data for Google+:
        - family_name
        - name
        - email
        - given_name
        - id
        - picture
        - locale
        - verified_email
        - age_range
        - language

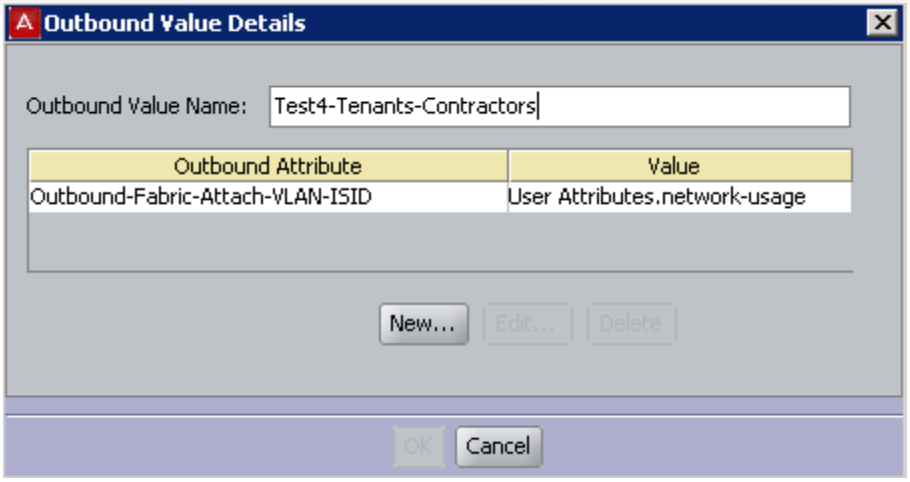
    - **Login History Display**
        - Display of last successful login
        - Display of the number of failed login attempted since last successful login

- **Guest & IoT Manager**
    - **Sponsor Response Text**
        - In Sponsor approval flow for guest access, Sponsor can now add a text to be sent to the guest requesting sponsor approval.
        - Example use case is Sponsor telling the guest to meet in the lobby at time zyx.
    - **Single Sponsor**
        - Customers can now set a single Sponsor that all guess access approvals flow through without requiring the guest to select a sponsor
        - Example is case is in small remote offices where there is smaller number of employees where there is no need to display a long sponsor list to choose from.
    - **Sponsor Node on Navigation Tree**
        - Fetches all guests for which the Provisioner is a Sponsor
        - Bulk Approve: Allow selection of multiple guest users and approve their requests.
        - Bulk Deny: Allow selection of multiple guest users and deny their requests.
        - Bulk Extend Expiration: Allow extend expiration of multiple guest user accounts.
        - Send message: Allow to send email with text to Guest Users.
    - **Random Guest Username Generation**
        - Admin can now configure random username generation with or without static password.
    - **Security Enhancement – Manage Certificates from GUI**
        - “Certificate” is added in the admin navigation tree,
        - Admin can now add/bind/bind chain/delete Httpd chain certificate, certificate and key.
    - **Self Service Guest Account Recreation**

- Admin while creating or editing a provisioning group can specify the limit of creating number of guest accounts for the duration in the “Guest User” tab by checking the checkbox.
- This feature allows admin to control the duration within which the guest can recreate an account and the second text field is for the number of accounts that can be created.
- This feature prevents abusing guest access by unwanted recurring visitors

- **Adaptation for Wide Screen Displays**
  - Tables display adapted to wide screen displays
- **Option to exclude Network Config during Import**
  - Admin can now exclude network configuration when restoring configuration file
  - Similar and consistent behavior as with Dashboard
- **Custom Device Types and Sub Types**
  - Admin can now limit the Device Types and Sub-Types that are available for Provisioners to use in a specific Provisioning Group.
  - This applies to Provisioner Device Registration, Self-Service Device Registration and REST APIs Device Registration flows.
- **Export Comments for Devices**
  - Export of Devices now also include Provisioner comments
- **Security Enhancement – Encrypt Export of Configuration File**
  - Admin can now add password to protect exported configuration file
- **Resend Password**
  - Both admin and Provisioners have new button to “Resend Password” to guests.
  - This feature allows guests to receive again their password in case was forgotten
  - The workflow is also available to Self-Service guest and may be enabled or disabled by admin to be available to the self-service guest
- **Localized Characters in Provisioner Username**
  - Allow AD authentication of Provisioners whose username/Password contains Localized characters.
- **Network Usage Field for Simplified Access Policies**
  - New field in the Guest User Tab for admin use: “Network Usage” where the admin can enter a Static String value.
  - Example for VLAN:ISID would be static value 100:10000
  - The value entered will be stored in the Guest Users “Network-Usage” attribute in the local store.
  - Example One usage of this value could be to provide access based on which Network Usage group they belong to.
  - With this feature, an Access Policy can now be generic and send network service Outbound Value that is pre-defines for the users based on the Provisioning Group template (good for example in multi-tenant situations).
  - Example of Access Policy:
    - Single Access Policy rule that will provision different network services to be based on “Network-Usage” value (e.g. VLAN:ISID = 100:100000) as configured on the Provisioning Group:

    - Outbound Values that will be sent out for users based on the “Network-Usage” attribute value (e.g. VLAN:ISID = 100:100000) as configured on the Provisioning Group:



- **Increase allowed max duration value to 9999**
  - Provisioning Group – Max Duration field now accommodates the maximum value of 9999.
- **Security Enhancement - TLSv1.2 for SOAP**
  - Guest & IoT Manager and Ignition Server now support SOAP communication over TLSv1.2
  - STARTTLS is also supported
  - This feature imposes limitation of compatibility between Ignition Server and Guest & IoT Manager versions. See table above in this Release Notes showing version compatibility.
- **Login History Display**
  - Display of last successful login
  - Display of the number of failed login attempted since last successful login
- **REST APIs Enhancements**
  - Provisioning Group option to manage all users and devices regardless if they were originally created by the Guest & IoT Manager GUI and/or REST APIs.
    - The new option shows as "Provisioners in this group can view all records"
  - Modified Device API to retrieve all attributes for a given device
  - Modified User API to retrieve all attributes for a given user
  - Modified Device API to retrieve all attributes for a devices accessed by a given username
  - Modified Device API for updating additional device attributes for a given device
  - Modified User API for updating additional user attributes for a given user
  - Modified Device API for specifying specific expiration date and time for a given device
  - Modified User API for specifying specific expiration date and time for a given user

- **Network Analytics**
  - **Ignition Server Data Source settings from GUI**
    - Admin is allowed to configure up to 4 Ignition Servers as data sources
    - Data Source settings get exported as part of the configuration export
  - **Exclude admin defined username from all Reports**
    - Admin can exclude username from reports
    - Used in order to eliminate biased reports because of high usage users (e.g. switch RADIUS reachability user)
    -
  - **Default filename changes**
    - Change default filenames for Export configuration, Backup configuration, Trouble Ticket, Export Reports and Scheduler files to include version no.
    - New filename examples are
      - INA_9.3.2_Configuration_135.123.151.48_20170516_111622.zip
      - INA_9.3.2_Backup_135.123.151.48_20170516_160947.zip
      - INA_9.3.2_Trouble_Ticket_135.123.151.48_20170516_142944.zip
  - **Option to Exclude Network config during Import**
    - Admin can choose to Exclude/Include Network config during Import.

- Network config includes IP's, Gateways, Routes, DNS and certificates.
- Default is Exclude Network config during import.

- **Option to Exclude License during Import**
  - Admin can choose to Exclude/Include License during config Import.
  - Default is Exclude License during import.
- **Facility to Ping**
  - This allows Admin to ping any host and check its reachability.
- **Security Warning banner display**
  - This allows Admin to configure 'Terms of Use' text; which will be displayed to user on login page.
- **Social Media Reports**
  - Reports based on Social Media login is added, and is made available below FA client reports.
  - Reports shows data as per 'Session by Social Media', 'Unique Social Media Users', 'Session Duration by Social Media Users' and 'Top 5 Social Media Users'.
- **Custom Start Date on all screens**
  - This option is available on all Report screens.
  - Admin is allowed to select any from (Start) date and then end date will be 7 days from Start (from) date.
  - Admin cans set this option as default option for all reports.
- **Allow admin to configure Housekeeping Tasks**
  - This option allows admin to set Database purge time in HH:MM format (24 hr), default purge time is set to 1.00 AM (GMT).
  - When user tries to save Scheduler job which is supposed to run during Housekeeping time, they will receive error and operation will not be allowed.
- **Install Certs from GUI**
  - Allows Admin to Add/Delete there Certificate/Key and Chains to system.
  - Allows Admin to bind Certificate/Chain to Analytics server.
  - Admin can see Active certificate details.
  - Certificate/Chain and Keys will get exported/imported as part of Config Export/Import operation.
  - Admin can any point of time reset certificate from Console, which will bind Default Avaya chain/certificate.
  - During config Export Keys will be in encrypted form.
- **Password change from GUI**
  - Allows Admin to change password as per enforced complexity, which says password must have at least one small case, one upper case, one number and one special characters among '!, @, #, $, %, ^, &, *, (,), -, +'.
  - Admin is not allowed to change password with password value which were used for most recent 3 passwords.
  - Username is not allowed to change, and change password capability is now removed from CLI.
  - Maximum length for password is 16 characters.
- **Install License using System Serial Number**
  - Allows Admin to install license which is based on System Serial Number of Analytics system using 'Choose a File' or 'Copy & Paste' option.
  - System Serial Number can be obtained / generated from console using command, show systemserialno / show systemserialno <IP-Address>.
  - Now admin should be able to install Analytics license from a file which contains multiple licenses along with valid Analytics license.
- **Login History details and display**
  - When admin logs in to Analytics system, we are displaying **Last successful login** time (before this login), and **Failed login attempts** count (before this successful login).
  - When admin logs in to Analytics system for first time, that time for **Last successful login** we are displaying **'FIRST LOGIN'**
  - **Sync Time format in GUI**Time which gets displayed to user on all pages (wherever applicable) will be in local time zone by default.

- For Backup and Restore pages time gets displayed in GMT, so we are displaying GMT after timestamp.

- **Optional Password during config Export**
  - Allows Admin to set optional password during config export operation.
  - When Admin tries to Import such config (which has password protection), that password needs to be specified correctly, otherwise Import will fail.
  - When any user tries to open Exported configuration zip file with password protection, it should be asked to enter the password, file will open only after providing correct password.

9.1.4 New and Enhanced Features in Releases 9.3.3

- **Ignition Server & Dashboard**
  - **Microsoft Netlogon Remote Protocol changes**
    - Remote Procedure Call (RPC) used for user and machine authentication on domain based networks changed from RPC over SMB using NETLOGON to RPC over TCP/IP. *With this change, interaction between Ignition Server and Active Directory (AD) no longer uses SMB (currently used v1) protocol*.
  - **Enhanced debug logging**

- **Network Analytics**
  - **Increase Disk space partition size for database**

9.2. Issues Resolved in this Release

Item Number	Description
JUPITER-3875	Ignition CLI Backup Not Functional. 'backup' command from CLI can perform backup of the Ignition Server configuration and upload to a remote file server. This command requires DNS to be properly configured which is now displayed to the administrator when they try to run the CLI command.
JUPITER-4013	Random ConfigServer Core; General System Instability In certain race conditions, ConfigServer process was running out of memory and that was causing the process to be unstable. The process limit of ConfigServer was tweaked and additional memory was allotted.
JUPITER-4239	Radius CORE Analysis In a heavy load scenario where multiple DB operations like MDM sync, statistics collection and device fetch happen in parallel, it was observed in in some race condition DB exception would occur and was not handled gracefully. Exception handling is now added to prevent such crashes in future. Also additional logging has been added to capture the conditions when this conflicts trigger..
JUPITER-4314	Radius CORE 9.3.2_32201 Mixing Non-Proxy and Proxy Directory Service in Directory Set. Dashboard now prevents this configuration which is not a supported combination.
JUPITER-4544	Network Analytics: 9.x Analytics Out of Disk Space /var PostgreSQL Database
JUPITER-4334	Network Analytics: Unable to get systemserialno while configuring admin interface IP other then /24 subnet

9.3. Outstanding Issues

Item Number	Description
JUPITER-3597	NTP Skew May Cause Bootup Delay.
JUPITER-3878	Ignition STATUS_PIPE_EMPTY During Authentications Unknows Win32 Status Error.

JUPITER-4231	Provisioner E-mail Validation Fails for New gTLDs (generic top level domains).
JUPITER-4236	Access Portal 9.3.2 – Issue with social media redirect using external captive portal + social media
JUPITER-4302	Network Analytics: Email validation on scheduler page is not complete.
JUPITER-4310	Cannot Create MDM w/ Different Server URL yet with same Group ID
JUPITER-4313	ZdbServer Core "Queue is Full" 9.3.1_31472

9.4. Known Limitations

Item Number	Description
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-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-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-3418	Network Analytics: Device type appears as unknown during first authentication of FA client. Device type appears as FA client for subsequent successful authentication, this creates two entries for same FA client in Authentication and Usage reports.
JUPITER-3228	Network Analytics: When DNS server is configured after configuring Email settings, Email settings will not take effect. As workaround Restart nodejs service from console. NOTE: to restart nodejs, login to Analytics server console and run command nodejs restart
JUPITER-3229	Network Analytics: Device type and subtype is not appearing for dot1x, MAC authenticated and wireless clients in Authentication reports.
JUPITER-3347	Network Analytics: User may lose data during DB restore, if restore is attempted on Analytics server which already has some data in it. It is recommended that user should do DB restore on a freshly deployed server.
JUPITER-3348	Network Analytics: When user creates FA outbound values with the default templates present on the dashboard, Analytics server is not showing any outbound values under the FA client details report.

JUPITER-3359	Network Analytics: If Username is starting with % character, it is appearing altered in UI.
JUPITER-4053	Ignition Server: [IGS]Ext-HA Export/Import is allowing both to co-exist in case of upgrade and restore scenarios. 9.3.2 release supports only one Ext-HA Import or Export schedule. However, if config from 9.1.0, 9.2.x, 9.3.x is restore (or the system upgraded to 9.3.2 from these releases) then multiple Ext-HA export/import schedules can be present on the system. During Dashboard launch, an appropriate warning is issued to the End user to keep only one Ext-HA Import or Export schedule.
JUPITER-4063	Guest & IoT Manager: [IGM] - While adding key option should be there to enter passphrase While importing private keys in Guest & IoT Manager application, keys with passphrase is not supported. As a workaround, please import only those keys which are not passphrase protected.
JUPITER-4126	Ignition server: During the head traffic or load if Ext-HA export is triggered. Some time it shows the status as failed in spite of in-progress. Once export activity is completed the status will update to success.
JUPITER-4203	Ignition server: If the user is being authenticated by remote proxy server then Analytics accounting log type shows empty.
JUPITER-4232	Ignition Server: SMTP Client Does Not Support TLS, STARTTLS or Other Dialects
JUPITER-4242	Ignition server: Authenticator import fails if the “Enable Radius Access” field is missing in the CSV file. While importing Authenticator from CSV file, if the “Enable Radius Access” field value is left blank then internally the code assumes that RADIUS is enabled and validates corresponding mandatory fields like RADIUS Access Policy, RADIUS Secret. If these fields are not specified in the CSV file, then Authenticator Import functionality doesn’t behave as expected. As a workaround, make sure that “Enable Radius Access” field in the CSV file is always populated with either TRUE or FALSE and if TRUE, all the RADIUS related fields are populated as well in the CSV file.

9.5. Important Application Notes

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

- **Ignition Server HA Sync:**
  - After HA is configured it takes few minutes (Based on the configuration) to sync across nodes. If admin wants to break the HA during this time, then admin may see the instability in secondary node.It is recommended to wait for sync operation to complete before you break the HA. If the system has gone into this inconsistent state, please restart the secondary node.
- **Guest & IoT Manager Support for TLS 1.2**
  - Note that the Guest & IoT Manager support for TLS 1.2 for communication with the Ignition Server dictates that Guest & IoT Manager 9.3.2 up is only compatible with Ignition Server 9.3.2 and up.

- **Guest & IoT Manager REST API**
  - The attribute “startTime” and “endTime” are now changed to “startDate” and “endDate” respectively. This change is applicable in Fetch Users/Devices (single and bulk) APIs and also Fetch Guests/Devices with Filter APIs

- **Network Analytics Internal Maintenance Tasks**
  - The Network Analytics application runs internal maintenance tasks on a time window basis between 00:00 to 1:00 AM (GMT) everyday, it is advised to not schedule any job during this period.

- Database purge will trigger at 00.15 AM (GMT) every day, which will remove DB records older than 3 months.

- **Network Analytics Configuration in HA setup**
  - In a HA setup if one of the node is down then Ignition Dashboard will not let the admin configure the IP Address of the Analytics server. Kindly ensure that both nodes of the HA configuration are up and running while specifying Analytics related details in the Ignition Dashboard.

- **Network Analytics Displaying 'User/Endpoint Device Trends'**
  - Displaying 'User/Endpoint Device Trends' statistics in Dashboard page takes time when total authentication records are more than 1 million, Sometimes user may get 'Failed to Retrieve Data for Access Trends' error message.

- **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 **& IoT** Manager
  - A password history is now maintained on Ignition Server and Ignition Guest & IoT 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 & IoT 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."

- **Ignition Server 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

- **Ignition Server 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 **& IoT** Manager 9.3.2 release. Support for HTTP is no longer available in IDR APP if it wishes to communicate with Guest **& IoT** Manager 9.3.2 release.

- **Ignition Server 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.

- **Ignition Server 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.x, 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.

- **Ignition Server enhancements in MS-CHAPv2 flow**
  - Starting from release 9.3.3, Ignition Server no longer uses SMBv1 for MSCHAPv2 authentication and need not be enabled on the Active Directory if it's disabled already. The 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

- **Ignition Server 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

- **Ignition Server 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 and up 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 9.3.2, 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".
  - Note that User logins via Social Media is sent from Ignition Server to Network Analytics as part of the regular Identity Engines Access Logs send via Syslog from Ignition Server to Network Analytics for statistic reporting.
  - Social Media user data as described above in section 9.1.3 is not included in Access Logs but rather may be configured separately by the administrator to be sent from Access Portal to any standard Syslog Server for data gathering and further processing and analysis. Note that if Social Media data is greater than standard UDP packet length then it is cut off at the UDP max length.

10. Upgrade Procedure

10.1. Ignition Server 9.3.3 - Pre-upgrade Checklist

Ignition Server Checklist

- By design, neither Software Upgrade flow nor Configuration Restore flow form 9.0.x to 9.3.3 is supported.
- If you are running 9.1.0, 9.2.x, 9.3.0, 9.3.1 or 9.3.2 you may perform Configuration Restore to 9.3.3 release.
- If you are running 9.1.0, 9.2.x, 9.3.0, 9.3.1 or 9.3.2 you may perform Software Package upgrade as follows:
  - If you are running 9.1.0, 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1 or 9.3.2 you may perform Software Upgrade directly to 9.3.3 release.
  - If you are running 9.2.3 or 9.2.4, you may perform Software Upgrade to 9.3.3 release via an intermediate 9.2.5 path (i.e. 9.2.3/9.2.4 to 9.2.5 then to 9.3.3)
- 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 9.3.3 includes a new Dashboard installer that must be installed. Ignition Server release 9.3.3 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. Ignition Server 9.3.3 - 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 9.3.3:
  - 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 9.3.3
    - Deploy a fresh new VM 9.3.3
    - Perform a configuration restore from 9.1.0 into 9.3.3
    - Perform a new backup of the 9.3.3 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 9.3.3 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.x, 9.3.0, 9.3.1 or 9.3.2 using fresh OVA install**
  If you are running Ignition Server 9.1.0, 9.2.x, 9.3.0, 9.3.1 or 9.3.2 and would like to migrate to release 9.3.3 using a new VM:
  - Take a configuration backup from your 9.1.0, 9.2.x, 9.3.0, 9.3.1 or 9.3.2
  - Deploy a fresh new VM 9.3.3
  - Perform a configuration restore from 9.1.0, 9.2.x, 9.3.0, 9.3.1 or 9.3.2
  - Perform a new backup of the 9.3.3 configuration
  - New perpetual licenses will be required. Send email request to datalicensing@avaya.com
  - Perform a new backup of the 9.3.3 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, 9.2.2, 9.3.0, 9.3.1 or 9.3.2 using Software Package File Upgrade process:**
  If you are running Ignition Server 9.1.0, 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1 or 9.3.2 and would like to migrate to release 9.3.3 using Software Package upgrade flow:
  - Take a configuration backup from 9.1.0, 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1 or 9.3.2
  - 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, 9.2.2, 9.3.0, 9.3.1 or 9.3.2 to 9.3.3 using the Package (pkg) file
  - Perform a new backup of the 9.3.3 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 9.3.3 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 a Software Package upgrade directly from 9.2.5 to 9.3.3 using the Package (pkg) file.
    - Perform a new backup of the 9.3.3 configuration
    - No new licenses are required.

- **Migrating from Network Analytics 9.3.0 or 9.3.2 to Network Analytics 9.3.3 using fresh OVA install**
  If you are running Ignition Network Analytics 9.3.0 or 9.3.2 and would like to migrate to release 9.3.3 using a new VM:

  Step 1: Back up existing configuration (System and Database)
    - Take a backup of the System Configuration from the current Network Analytics 9.3.0 or 9.3.2 running VM
    - Take a backup of the Database Configuration from the current Network Analytics 9.3.0 or 9.3.2 running VM
    - Shutdown Network Analytics 9.3.0 or 9.3.2 VM

  Step 2: Generate System Serial number and request for new License
    - Deploy the new Network Analytics 9.3.3 VM
    - Configure the IP address on the Admin interface
    - Obtain the System Serial Number of the Network Analytics installation from console using command show systemserialno
    - Send email request to datalicensing@avaya.com to transfer your existing Network Analytics license to the newly generated System Serial Number
    - Launch the browser using the above IP address as the URL
    - In the interim, obtain an Network Analytics Trial License from www.avaya.com/identitytrial
    - Install the Network Analytics Trial License
    - Perform System Configuration restore into Network Analytics 9.3.3 using the 9.3.0 or 9.3.2 System Configuration file. Make sure that the “Include License” checkbox is unchecked.
    - Perform Database Configuration restore into Network Analytics 9.3.3 using the 9.3.0 or 9.3.2 Backup Configuration file
    - Once you receive the transferred license Install the received license

  NOTE: In case you are migrating from **Network Analytics 9.3.0 to 9.3.3**, then you need to configure Data Source and Network Settings again from GUI and console respectively as these was not part of Configuration Export in previous release.

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.

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/