Avaya Identity Engines Release Notes
Software Release 9.0.1

1. Release Summary

Document Version:	03.03
Document Date:	June 2014
Purpose:	Identity Engines (IDE) software major release to introduce new Features, Enhancements, and to address customer found software issues.

2. Important Notes before Installing this Release

- Avaya provides the Identity Engines Ignition Server as a complete Virtual Appliance.
  - Do not install or uninstall any software components on this Virtual Appliance unless Avaya specifically provides the software and/or instructs you to do so.
  - Do not modify the configuration or the properties of any software components of the Ignition Server VM (including VMware Tools) unless Avaya documentation and/or personnel specifically instruct you to do so.
  - Avaya does not support any deviation from these guidelines.

- Avaya does not support upgrading the VMware Tools in the Ignition Server VMware VM. If you have already updated the VMware tools or unsure, stop the process and follow the procedure given below.

  - Take a backup of 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

Identity Engines Software Upgrade Requirements

Identity Engines release 9.0.1 requires deployment of a fresh new Ignition Server OVA. Upgrade from release 8.0.x to 9.0.1 (as well as from 9.0.0 to 9.0.1) is not available as the hardware system requirements for release 9.0.1 have changed compared to previous release(s).

If you are running release 8.0.x or 9.0.0 and would like to migrate to 9.0.1, take a configuration backup from 8.0.x or 9.0.1, deploy a new 9.0.1 VM and perform a configuration restore on the 9.0.1 VM. You will have to obtain new licenses for release 9.0.1.

Saved Configuration File Compatibility

In order to maximize configuration compatibility during upgrade, Identity Engines Ignition Server release 9.0.1 does not support performing configuration restore from release prior to 8.0.x. Please refer to Upgrade Procedure in section 8 of this document. If you are on a release prior to release 8.0.x, please refer to the Release Notes of release 8.0.x for upgrade procedure.

©2012-2014 Avaya Inc.

3. Platforms Supported

The following VMware ESXi platforms are supported with Identity Engines release 9.0.1:
VMware vSphere version 5.0
VMware vSphere version 5.1
VMware vSphere version 5.5

Please be aware that a VMware ESXi platform upgrade may be necessary as previous release 8.0.x supported VMware ESXi 4.0, 4.1 and 5.0.

IMPORTANT NOTE:
Note that VMware vMotion, VMware Player and VMware Workstation are not supported and cannot be used in conjunction with the Ignition Server.

4. Installation

File Names for Identity Engines release 9.0.1

File Name	Module or File Type	Comments
AIEIS_RHEL_6_3_LINUX-VM_09_00_01_026078_x86_64.ova	Ignition Server OVA files for vSphere 5.x environment	Ignition Server release 9.0.1. Used for fresh install of Ignition Server. No upgrade package available.
GuestManagerInstaller-9.0.0.25816.exe	Guest Manager Installer	Bug Fixes and compatibility with Ignition Server release 9.0.1
DashboardInstaller-9.0.1.26078.exe	Dashboard Installer	Dashboard Installer release 9.0.1 compatible with Ignition Server release 9.0.1
SSOServiceProviderAgent-9.0.0-25816.zip SSOServiceProviderAgent-9.0.0-25816.tar.gz	Service Provider Agent Package	Service Provider application and configuration utility for Identity Engines Web-based SSO

File Names of Identity Engines Release 8.x that are compatible for deployment in conjunction with Identity Engines Release 9.0.1

File Name	Module or File Type	Comments
AdminConsoleInstaller-1.0.0.22931.exe	CASE Manager Installer	CASE Manager release 1.0 is compatible with Ignition Server release 9.0.1
AccessPortal_01.00.00_022931_x86_32.mf AccessPortal_01.00.00_022931_x86_32.ovf AccessPortal_01.00.00_022931_x86_32.vmdk	Access Portal OVF files for vSphere 4.x and 5.x	Access Portal Release 1.0 is compatible with Ignition Server release 9.0.1

System Requirements

Software	System Requirements	Comments
Ignition Server	• VMware ESXi versions 5.0 or 5.1 or 5.5 • Installation on a VMware ESXi server is done using an OVA file which already incorporates the OS Red Hat Enterprise Linux.	• The VM requires a x86_64 capable environment • Minimum 4 CPUs • Minimum 4 GB of memory • Minimum 260 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
Access Portal	• VMware ESXi versions 4.0* or 4.1* or 5.0 or 5.1 or 5.5 • Installation on a VMware ESXi server is done using an OVF file which already incorporates the OS FreeBSD.	• The VM requires 32-bit capable environment • • Minimum 2 CPUs • • Minimum 2 GB of memory • • Minimum 10 GB available disk storage • • Minimum 2 physical NIC (preferably 3 NICs). • • VMware lists on its site supported hardware platforms for • ESXi: http://www.vmware.com
Ignition Dashboard	• Windows XP sp3 (32 bit)** • Windows 7 (32 bit or 64 bit) • Windows 8 (32 bit or 64 bit) • Windows Server 2003 (32 bit or 64 bit) *** • Windows Server 2008 (32 bit or 64 bit) ****	• Minimum 2GB RAM memory • US English Windows
Guest Manager	• Windows XP sp3 (32 bit) ** • Windows 7 (32 bit or 64 bit) • Windows 8 (32 bit or 64 bit) • Windows Server 2003 (32 bit or 64 bit) *** • Windows Server 2008 (32 bit or 64 bit) ****	• Minimum 2GB RAM memory • US English Windows
CASE Manager	• Windows XP sp3 (32 bit)** • Windows Server 2003 (32 bit) *** • Windows Server 2008 (32 bit and 64 bit) **** • Microsoft IE version 6.0 or later • Firefox version 1.5 or later	• Minimum 2GB RAM memory • US English Windows
Analytics	• Windows XP sp3 (32-bit)***** • Windows Server 2003 (32-bit)****** • Windows Server 2008 (32-bit)******* • Windows must have NTFS file system partition • 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 for iPad release 1.2	• Compatible with Identity Engines R9.0 SSO
Avaya System Manager	Avaya SMGR release 6.2 FP3	• Compatible with Identity Engines R9.0 SSO
Service Provider Agent	Apache Tomcat 6.x	• Compatible with Identity Engines R9.0 SSO • Any servlet container compliant with the Servlet API specifications version 2.4 or higher will work, like Tomcat 6.x, JBoss or Websphere

Notes for Identity Engines OVA/OVF VMware ESXi versions
* Release 9.0.1 is last release to support Access Portal on ESX 4.x versions

Notes for Dashboard/CASE Manager/Guest Manager Windows versions
** Release 9.0.1 is last release to support Dashboard/CASE Manager/Guest Manager on Windows XP versions
*** Release 9.0.1 is last release to support Dashboard/CASE Manager/Guest Manager on Windows 2003 versions
**** Release 9.0.1 is last release to support Dashboard/CASE Manager/Guest Manager on Windows 2008 32-bit

Notes for Analytics Windows versions
***** Release 9.0.1 is last release to support Analytics on Windows XP versions
****** Release 9.0.1 is last release to support Analytics release 8.0.0/8.0.1 on Windows 2003 (32-bit)
******* Release 9.0.1 is last release to support Analytics release 8.0.0/8.0.1 on Windows 2008 (32-bit)
Please note that Analytics with support for Windows 7 (64-bit) and 2008 (64-bit) versions is planned

5. Version of Previous Releases

Identity Engines Software release 8.0.2, Release Date – May, 2013

6. Compatibility

Identity Engines Ignition Server release 9.0.1 software can only be managed with Avaya Ignition Dashboard release 9.0.1.

7. Changes in This Release

New features in This Release

Enterprise-Level Administration

The Enterprise Level Administration of Identity Engines Ignition Server offers more granularities in terms of the administration. The Enterprise Administration introduces RBAC (Role Based Access Control) approach to IDE. By associating a role to a user, IDE can qualify different types of administrators and map them to the functionality that is pertinent to their administration interest for a given IDE instance.

All prior Dashboard releases included one centralized administrative login account. The user of this account is the equivalent of a super-user on Dashboard. This account has no restrictions with regards to configuration or monitoring of the IDE.
As network administration grows in complexity there becomes an increasing need to limit or define the capabilities of specific types of administrators for an IDE Server.

There are four pre-defined roles for Dashboard Administration

- System Administrator
- Configuration Administrator
- Trouble Shooting Administrator
- Monitoring Administrator

One admin can focus on system monitoring while another can focus on system management (upgrading images, saving configurations, etc). This approach creates boundaries for administrators to work autonomously from one another. It will also prevent admins from touching parts of the system that they may not be truly interested in.

Identity Engines Single-Sign-On (SSO)

With the Single-Sign-On (SSO) feature, IDE becomes a full-fledged Identity Management System that not only controls the network access for a user but also provides granular policy based access control to the resources (application servers) contained within an enterprise network. Proprietary identity requirements, complex password policies, forgotten passwords, and high help desk costs for password resets are just a few of the sign-on challenges for modern enterprises.

With IDE SSO architecture, enterprises can enable ubiquitous SSO for users. This not only simplifies secure access, but also results in lower operational costs for enterprises, leading to stronger enterprise security. Identity Engines SSO provides standards based SSO capabilities and allows various application servers (sites) to make informed authorization decisions for individual access of protected online resources in a privacy- preserving manner.

The IDE SSO architecture provides two SSO workflows to take into account different modes of client access:

- Web-based SSO targeted for browser-based client access or thin clients
- ECP-based SSO targeted for thick clients or intelligent clients

Identity Engines SSO consists of the following architectural components.

Identity Provider
The Identity Assertion Provider (IdP) is an authentication module that authenticates the user within a security realm and then issues a security token, which can be used by the client to get access to protected resources within that security realm without having to authenticate again.

An IdP is hosted on the Ignition Server as a licensable service. This IdP uses all of the IDE Ignition Server's capabilities to enforce XACML-based policies and integration with various directory services.

Realm Mapper
In Avaya Aura environment, Aura login credentials are different from Enterprise credentials and hence do not directly support Single-Sign-On. Realm Mapper service running on the Ignition Server provides mapping between user's enterprise credentials and their Aura identity. Aura services first contact the Ignition Server Realm Mapper for validating user's enterprise credentials and then use the response from Realm Mapper to validate the Aura credentials automatically without the user being prompted for Aura credentials.

Note: In Release 9.0, Aura Flare Experience 1.2 for iPad supports IDE SSO capabilities.

Service Provider
Service Provider is an entity that protects application services. It intercepts access requests and redirects the user to IdP for validating the credentials. Upon successful authentication, Service Provider gets an assertion from the IdP and then uses it to grant access to the user based on the local policies.

Identity Engines R9.0 includes a Service Provider package that can be integrated with Enterprise's web applications for SSO support. This Service Provider can work with any Web Server that complies to Servlet API specification version 2.4 or higher, like Apache Tomcat 6.x, JBoss etc.

Identity Engines supports the following authentication methods for Single-Sign-On:

- Kerberos based authentication using SPNEGO for domain joined devices
- Basic authentication
- Form-based Login for browsers

Note: Kerberos based Single-Sign-On authentication is limited to Microsoft Active Directory environments in IDE R9.0.

Licensing Requirements for SSO feature

Single-Sign-On (SSO) is a licensed feature. Users must install the Ignition Aura SSO license (also known as SAML license) to enable the Identity Engines SSO feature support on the Ignition Server.

The Ignition Aura SSO license requires at a minimum an Identity Engines Ignition Server Base license of any size (for example: Ignition Server Base LITE, SMALL or LARGE license). A single Identity Engines Aura SSO license is required for either a standalone deployment of the Ignition Server or a High Availability (HA) deployment of a pair of Ignition Servers.

Avaya Product Licensing and Delivery System (PLDS) support

Avaya Identity Engines currently supports the Keycode Retrieval System (KRS) based licensing model.
Starting with Identity Engines R9.0, Identity Engines supports the Avaya PLDS licensing model in addition to KRS.

The Avaya Product Licensing and Delivery System (Avaya PLDS) provides customers, Business Partners, distributors, and Avaya Associates with easy-to-use self-service tools for managing asset entitlements and electronic delivery of software-related licenses. Using PLDS, you can perform activities such as license activation, license de-activation, license re-host, and software downloads.

For a period of time, Identity Engines will support the dual licensing to accommodate current install base customers who do not have yet access to the Avaya PLDS system.

Other Enhancements

Identity Routing based on Machine Names

In machine authentication, a PC will provide its machine name as identity. A machine name does not include realm info and therefore identity routing based on realm does not apply. In a multi-domain environment, machine authentication has to rely on fall-through mechanism to find appropriate directory service if there are multiple directory services.

Identity routing based on machine name provides a direct guide to the directory service that will efficiently process machine authentication. If the machine name itself is constructed including the machine name and the realm, Identity Engines Identity Routing policy can now be configured to look for realm information in the username attribute and route to the appropriate Directory service.

SHA-2 based Certificates

Avaya Identity Engines now ships the default self-signed certificates based on the SHA256 signature algorithm. If the user restores 8.0.x configuration, then both SHA128 and the new SHA256 certificates will co-exist.

SHA256 bit ciphers are also added to the cipher list that can be selected in the authentication policy.

OPERATIONAL NOTE:

- Ignition Server R9.0 has new default server certificates based on SHA256 algorithm
- Dashboard includes appropriate root CA to connect with the Ignition Server
- Dashboard cannot build the keystore from previous installation if one already exists on the PC that Dashboard is running on
- Take the following actions and delete the keystore manually by deleting the following directories
  - Win XP -- C:\Documents and Settings\<user id>\Application Data\Avaya\security
  - Win 7 -- C:\Users\<user id>\AppData\Roaming\Avaya\security
  - Win 8 -- C:\Users\<user id>\AppData\Roaming\Avaya\security
  - Note that these folders may be hidden folders

Hierarchical Certificates

Hierarchical certificate authority deployments use a subordinate client certificate authority (CA). This client certificate CA (also known as an Intermediate CA) is spawned from a parent CA in order to isolate and minimize exposure of its parent root certificate. The root CA is kept offline to avoid compromise.

The client certificate CA is used to generate server and client certificates. It is this same subordinate client certificate CA that may revoke client certificates and publish CRLs (Certificate Revocation Listings).

Starting from this release, CRL checks can be performed at the certificate issuing CA level as well as at the root CA level, depending on configuration via CLI.

Authorization Policy based on User Certificate Attributes
In TLS-based user authentication, the supplicant will provide user certificate to Identity Engine. Certificate attributes such as common name, locality, organization, organization unit, state, country code, and email could be used in authorization policy.

Enhanced Group cache support
For LDAP based directory services (including Active Directory), the Ignition Server maintains an internal cache of the group hierarchies and attributes schemas of the directory services.

IDE R9.0 now allows disabling this caching by clearing the Enable Group Caching check box.

By default, Ignition Server looks for groups starting at the Directory Root DN. This behavior can be changed by specifying Group Search Base DNs. This is useful in case of huge AD deployments, where starting at the root DN can take up a substantial amount of time.

In addition the Re-sync Duration for the group cache is customizable now. The range is between 1 to 168 hours. The cache is automatically refreshed based on this setting.

Support to retain licenses across restore
With IDE releases prior to R9.0, while performing restore of backup configuration, any licenses that users may have installed on the system will be overwritten by the licenses in the backup file. If the backup was from another VM, the license data in the backup will not be applicable to this node. After restore, user would have to re-install the new license.

With IDE R9.0, users can now choose whether to retain existing licenses during restore or overwrite the existing licenses with the data from backup file. A new option 'License configuration' is now included in the restore dialog which will determine whether to restore the license or keep the existing licenses.

7.1. Problems Resolved in This Release

Work item Number	Description
wi01097935	**Ignition Dashboard still shows includes DST calculation when running in Moscow Time zone.** Ignition Dashboard R9.0 now ships with JRE 7 update 45 which has fixes for Moscow DST changes
wi01046457	**While installing release 8.0.x dashboard on Windows 7 with UAC enabled machine, there is no logs folder.** Dashboard release 9.0.1 logs folder will be created in C:\Users\<user>\AppData\Roaming\Avaya\logs\ Ignition Dashboard 9.0.1.26078 folder
wi01046138/ wi01042106/ wi01040618	**In HA setup, multiple issues were seen in previous releases. Some of the issues were,** - **Secondary node was stuck in "Synching Config" while creating HA,** - **Failed to sync the following on node <x.x.x.x.> error message on** - **Dashboard** - **Unable to update radius/soap/tacacs configuration error message on Dashboard**

	R9.0 now provides enhanced HA stability by upgrading the underlying platform which includes fixes to memory leaks seen during HA synchronization operations.
wi01047698	**Occasionally, disabling HA/Service ports from Dashboard does not update the actual physical port status in the system correctly.** In R9.0, event mechanism has been enhanced which now reliably sends any configuration change event to all the listener process and the configuration is applied correctly on the system.
wi00977909	**While restoring large database in a HA setup, restore status on the 2nd node may be stuck at 'syncing config…'** R9.0 now provides enhanced HA stability by upgrading the underlying platform which includes fixes to memory leaks seen during HA synchronization operations.
wi01141333	**Add display of GMT time on Dashboard node status tab** Ignition Server always runs under GMT time zone. When the user is connected via Dashboard, the logs are shown with the time stamp converted to the local time zone. To make it more clear to the user, Dashboard now displays the time both in GMT time zone as well as the local time zone on which the Dashboard is running under Configuration -> <node> -> Status tab
wi01141330	**Add a new CLI command to display the time of Ignition Server** R9.0 now includes a new CLI command 'show time' to display the current time of Ignition Server which always runs under GMT time zone
wi01136871	**Special characters in the authorization policy rule causes authentication failure** A validation has been added in release 9.0 which correctly checks for any special characters at the time of rule creation
wi01081205	**Identity Engines release 8.0.1 admin password cannot be over 8 characters in release 8.0.1** The maximum password length has been changed to 36 characters and minimum to 5 characters in R9.0
wi01007904	**Add support for new default vendor definitions** R9.0 now includes new Vendor/VSA definitions for the following vendors: - Brocade - Aerohive Networks - Ruckus Wireless
wi00998636	**By default, Access Portal MAC based authentication recognized as user authentication** R9.0 now includes a new device template under Avaya->avaya-ignition-access-portal' which has the right attribute definitions for Access Portal MAC authentication.
wi00991616	**Expired Guest Accounts with 'Delete upon expire' setting enabled are not cleared quickly** The expired guest accounts purge interval is now changed from 7 days to 24 hours in R9.0
wi01123453	**In large customer deployments with huge no. of AD groups, the group cache operation takes a long time to complete and makes the system slow** In some customer deployments, they have huge no. of AD groups, but Ignition Server doesn't need to cache all the groups. R9.0 now includes two new enhancements to the group cache behavior. - The group cache now be completely turned off or the cache interval can be configured. - Also added a support to select base DN from which the group information is read as well as specify a group search filter
wi01086386	**Create a Device Template on Ignition Server for another Ignition Server acting as a RADIUS Proxy** In a Radius Proxy setup where Ignition Server is acting as a forwarding proxy, it needs to be added as an authenticator on the Remote Radius Server that may be another Ignition Server itself. This authenticator can be defined with the device template as 'Avaya > avaya-ignition-server' template
wi01150440	**Unreachable CRL link causes Certificate Manager to fail initialize properly** While adding a CRL, Ignition Server will first check if the URL is reachable. If not, adding

	of CRL itself will fail. However, it's possible that the CRL may become unreachable after some time or if the CRL information is taken from a backup file whose link is not available anymore. In this case, any unreachable CRL causes failure in Certificate Manager initialization. This issue is now fixed in R9.0.
wi01165651	**OpenSSL "Heartbleed" Vulnerability (CVE-2014-0160)** 9.0 includes updated OpenSSL library from Red Hat which addresses the OpenSSL "Heartbleed" Vulnerability (CVE-2014-0160).

7.2. New Outstanding Issues

Work item Number	Description
wi01155908	**When the connection between Dashboard sys-admin session and Ignition Server is lost, sys-admin cannot login to dashboard again** With multi-administrators support in R9.0, only one sys-admin user can login at any time. If the logged in sys-admin has not gracefully closed the Dashboard session and the connection between the Ignition Server and the Dashboard sys-admin session is lost for any reason (like network failure or the machine from the Dashboard is running is shut down), another sys-admin cannot login to the system. As a work around, • login to console or open an SSH connection to Ignition Server and run 'show sessions' command • Note down the 'Id' of the session entry for sys-admin • Run 'session delete id <id>' to clear the stale session and the sys-admin can now login to the Dashboard
wi01151857	**Not able to associate internal users with internal devices** While adding internal users to the Ignition Server, internal devices could also be mapped to each user which can then be used in the authorization policies. However, this operation although shows successful, the mapping is lost when we try to view the user details. As a work around, the same association can be mapped by associating the internal device with the internal user.
wi01126383	**In a deployment where Guest Manager and an Enterprise Web Server application using the Identity Engines Service Provider package for SSO are installed on the same server, user not able to add Guest Manager server configuration on the IDE** Typically, Guest Manager application which ships with its own Tomcat Web Server will be deployed on separate machines from the Enterprise web application servers. But if the user wants these two applications to co-exist on the same Tomcat server, first deploy the Guest Manager application on the server and then deploy your Enterprise web application and the Identity Engines Service Provider package for SSO next. After installing these applications, first configure the Guest Manager server details first on the IDE and then add the Service Provider details for SSO.
wi00852520	**One node IP address was truncated after breaking and creating HA multiple times from Dashboard** This issue is seen occasionally after breaking and creating HA multiple times. This issue does not affect any functionality. As a work around, users can logout and re-login to the Dashboard to fix the issue

7.3. New Known Limitations

Work item Number	Description
wi01121113	**In Form-based SSO authentication where a client trying to access a protected resource is redirected to the Ignition Server IdP, If IdP hostname contains special character like underscore, IdP login page shows unspecified service provider** Underscore is not considered a valid character for DNS hostname. Only following characters are allowed for DNS hostnames: • Alphabets, Numeric, Hyphens
wi01119478	**IdP summary shows two entries in HA even though SAML service is bound to VIP** In HA, if DNS configuration is not valid or not reachable on either of the HA nodes, then SSO configuration will not be valid. **Note: SSO feature requires a valid DNS configuration to be added to each IDE in HA which can then use it to resolve hostname to the interface IP address (or VIP) to which the SAML service is bound to.**
wi01127410	**While restoring large configuration, system takes additional 4-5 minutes for all the SSO services to come up** While restoring large config which contains many Directory services and large group cache information, Ignition Server will try to establish connectivity with the Directory services for group cache and service account creation. If any of these Directory services are unreachable, Ignition Server will keep trying to connect to them until time out. Eventually, the entire configuration will be loaded and the applications will come online. Users can make use of 'System Health' and 'Directory Service Status' tabs until 'monitor' to make sure all the services are up and running
wi01155806	**After session timeout triggers from Dashboard, session is not cleared from Ignition Server side immediately. It will take 30sec to 1 minute to clear** Each Dashboard connection will have a session time out after which the session is automatically disconnected. Though the session is closed from the Dashboard, it'll take 30-60 seconds for the session to be cleared from the Ignition Server side. If any user tries to login within this short interval (30-60 seconds), the login will not be allowed with an error saying 'session already exists'. Ignition Server session cleanup process runs every 60 seconds to clear any timed out sessions.

8. Upgrade procedure

Pre-upgrade Checklist for Ignition Server

- Note that by design, users cannot upgrade an existing 8.0.x or earlier VM nor an existing 9.0.0 to 9.0.1 VM using software upgrade procedure

- Alternatively, existing configuration can be migrated to 9.0.1 using the backup & restore functionality. Restore of configuration data on 9.0.1 release can only be performed from the following versions:
  - Backup of 8.0.x (or 9.0.0) configuration data
  - If you're running version older than 8.0.x and would like to upgrade to release R9.0, first perform an incremental upgrade to 8.0.x release and then use backup & restore functionality to migrate your existing configuration to 9.0.1 VM
  - Please contact Avaya support if you will need temporary licenses for IDE R8.0 for this process of incremental migration of your configuration to IDE release 9.0.1.

- IDE R9.0 also includes a new Dashboard installer that must be installed. Ignition Server release 9.0.1 cannot be managed from any previous versions of Dashboard

- IDE R9.0 includes new SHA256 based default certificates. If you're installing the new Dashboard release 9.0.1 over an existing Dashboard, you'll notice SSL validation errors that could cause connectivity issues with the Ignition Server.

Dashboard keeps the cached keystore of these certificates at following locations:

Win XP
C:\Documents and Settings\<user id>\Application Data\Avaya\security

Win 7
C:\Users\<user id>\AppData\Roaming\Avaya\security

Win 8
C:\Users\<user id>\AppData\Roaming\Avaya\security

Delete these directories from your system before launching the new Dashboard

Note that these folders may be hidden folders.

- IDE R9.0 also includes a new Guest Manager installer and must be installed. Ignition Server release 9.0.1 is not compatible with any previous versions of Guest Manager

- If you're installing the new Guest Manager release 9.0.0 over an existing Guest Manager, you'll notice SSL validation errors that could cause connectivity issues with the Ignition Server.

  Guest Manager keeps the cached keystore of this certificate and it cannot build a new keystore if one already exists from previous installation.

  Delete the keystore manually by deleting the following under Tomcat configuration:

  C:\Program Files\Apache Software Foundation\Tomcat 6.0\conf/idEngines\gm_ks

- No new upgrade software packages available for Access Portal, CASE Manager and Analytics applications. Existing 8.0.x release software continues to be compatible with 9.0.1 release for these applications.

- Users should never update VMware Tools or modify the configuration or the properties of Avaya provided Virtual Appliances which include Ignition Server. Avaya does not support upgrading of VMware tools or any other software components unless the upgrade package is provided by Avaya.

- If you have already updated VMware tools or unsure, stop the upgrade and follow the procedure given below.

  - Take a backup/snapshot of configuration from your existing VM's
  - Deploy a new Ignition Server using the OVA
  - Restore the configuration
  - Install the necessary licenses

Software Upgrade Procedure

There's no software upgrade of 8.0.x VM to 9.0.1 release. If you're running an existing 8.0.x deployment and would like to migrate to 9.0.1 release, follow the instructions given below:

- Deploy a new Ignition Server 9.0.1 VM using the OVA

- Obtain and install necessary 9.0.1 licenses

- Once above tasks are completed:

- Take a backup of the policy configuration data of your 8.0.x VM or 9.0.0 VM
- Perform configuration restore of 8.0.x backup on the 9.0.1 VM

9. 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.

© 2014 Avaya Inc. All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support

Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software.

Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding

distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/