Identity Engines Release Notes

Software Release 9.4.0

NN47280-400
Issue 16.01
December 2017

1. Document Summary

Document Version: 16.01
Document Date: December 2017
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
16.01	First published Release Notes for IDE 9.4.0	

2. Important General Notes

- Extreme Networks provides the Identity Engines Ignition Server as a complete Virtual Appliance.
  - Do not install or uninstall any software components on this Virtual Appliance unless Extreme Networks 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 Extreme Networks documentation and/or personnel specifically instruct you to do so.
  - Extreme Networks does not support any deviation from these guidelines.

- Extreme Networks 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 Ignition Server using the OVA supplied by Extreme Networks.
  - 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 9.1.x then please be aware that Software Package upgrade from Ignition Server release 9.1.x to Ignition Server release 9.4.0 is **not** supported.

- If you are running Ignition Server release 9.1.x then please also note that configuration restore of the backup from Ignition Server 9.1.x to 9.4.0 is **not** supported.

- Should you want to restore your Ignition Server 9.1.x configuration, then first install a fresh Ignition Server 9.3.3 VM using trial licenses and then restore the configuration from 9.1.x into that instance of 9.3.3. Post that you can either upgrade to 9.4.0 or take a backup and then restore the configuration on a fresh 9.4.0 instance.

- If you are running Ignition Server release 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1, 9.3.2 or 9.3.3 and would like to migrate to 9.4.0, you have two options:

    - Option 1: Take an Ignition Server configuration back up from 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1, 9.3.2 or 9.3.3, deploy a fresh Ignition Server 9.4.0 VM and perform a configuration restore on the 9.4.0 VM. Updated licenses will be required.
    - Option 2: Perform a Software Package upgrade directly from Ignition Server 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1, 9.3.2 or 9.3.3 to 9.4.0 using the PKG (Package) file. No updated licenses will be required.

- If you are running release Ignition Server 9.2.3 or 9.2.4 and would like to migrate to 9.4.0, you have two options:

    - **Option 1**: Take an Ignition Server configuration backup from 9.2.3 or 9.2.4, deploy a fresh new Ignition Server 9.4.0 VM and perform a configuration restore on the 9.4.0 VM. Updated licenses will be required.
    - **Option 2**: Perform a software upgrade from Ignition Server 9.2.3 or 9.2.4 to an intermediate 9.2.5 version using the special purpose PKG (Package) file supplied by Extreme Networks and then upgrade from 9.2.5 to 9.4.0. No updated licenses will be required. Note that the 9.2.5 intermediate package file is included in the zip file of the 9.4.0 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.
    - Request trial licenses for transitional upgrade process from datalicensing@extremenetworks.com

- 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 9.4.0:

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

IMPORTANT NOTE:

The 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 9.4.0:

File Name	File Type	Comments
AIEIS_RHEL_6_5_LINUX-VM_09_04_00_32956_x86_64.ova	Ignition Server 9.4.0 OVA for VMware ESXi	This file is used for fresh VM install.
LINUX-VM_09_04_00_32956_server_complete.pkg	Ignition Server 9.4.0 Software Package file	This file is used for Software Package upgrade.
DashboardInstaller-9.4.0.32956.exe	Dashboard Installer 9.4.0	Compatible with Ignition Server 9.4.0
AIGM_RHEL_6_5_LINUX-VM_09_04_00_32986_x86_64.ova	Guest & IoT Manager 9.4.0 OVA for VMware ESXi	Compatible ONLY with Ignition Server 9.4.0

5.2. Previous Identity Engines software files compatible with Release 9.4.0:

File Name	File Type	Comments
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 9.4.0

File Name	File Type	Comments
		IMPORTANT: **IDR 9.2 can communicate with Guest & IoT Manager 9.4.0 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.x or 9.4.0**

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 9.4.0	-	9.4.0	-	9.2.0 9.2.1 9.3.2	9.3.0 9.3.2
Guest & IoT Manager 9.4.0	9.4.0	-	9.2.0	9.2.0 9.2.1 9.3.2	9.3.0 9.3.2
Android IDR App 9.2	-	9.3.0(1) 9.3.2(1) 9.4.0	-	-	-
Access Portal 9.3.2	9.3.2 9.3.3 9.4.0	9.3.0 9.3.2 9.4.0	-	-	9.3.0 9.3.2
Network Analytics 9.3.2	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	FROM Ignition Server 9.1.x
Ignition Server 9.4.0	Not Supported	Not Supported	Not Supported

TO	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 9.3.0/9.3.1/9.3.2/9.3.3
Ignition Server 9.4.0	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 9.4.0	9.2.x 9.3.x	---	---	---
Guest & IoT Manager 9.4.0	---	9.2.x 9.3.x	---	---
Access Portal 9.3.2	---	---	9.2.0 9.2.1	---
Network Analytics 9.3.2	---	---	---	9.3.0

7. System Requirements

Software	Software Compatibility	Comments
Ignition Server Release 9.4.0	• VMware ESXi versions 5.5, 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 9.4.0 software can only be managed with Ignition Dashboard release 9.4.0.	• The VM requires a x86_64 capable environment • 4 CPUs • Minimum 4 GB of memory • Minimum 250 GB available disk storage (thin provisioning is allowed) • Minimum 1 physical NIC (preferably 3 NICs) • 3 Logical NIC cards

Software	Software Compatibility	Comments
		• VMware lists on its site supported hardware platforms for ESXi: http://www.vmware.com
Ignition Dashboard Release 9.4.0	• 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 • **This is the last release supporting Windows 2008 Server**
Ignition Guest & IoT Manager Release 9.4.0	• VMware ESXi versions 5.5, 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 52 - 57 • 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 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 52 - 57 • 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 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 9.3.2	• 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 52 - 57 • 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	Not Supported	
Avaya System Manager	Not Supported	

Software	Software Compatibility	Comments
Citrix XenMobile MDM	Citrix XenMobile MDM 8.7 and 9.0	• Compatible with Ignition Server R9.4.0
AirWatch MDM	AirWatch MDM v8.4.3.0	• Compatible with Ignition Server R9.4.0
Infoblox	Infoblox DDI 8.2.1	• Compatible with Ignition Server R9.4.0
Microsoft Active Directory	Windows Server 2008 & 2008 R2 Windows Server 2012 & 2012 R2	• Compatible with Ignition Server R9.4.0

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"

- Identity Engines Software release 9.3.3, Release Date – August 2017
  File name "NN47280-400_15_01_IDEngines_9_3_3_Release_Notes.pdf"

9. New and Changes in this Release

9.1. Overview of New and Enhanced Features in 9.3.x and 9.4.0 Releases

9.1.1 Summary of Select New and Enhanced Features in Releases 9.3.x

- **Ignition Server & Ignition Dashboard 9.3.x**

  - **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**

    - 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 Extreme 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.

- **Certificate Enhancements**

  - 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.

- **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 FA Client APs, you need to change the VLANs and ISIDs that service a set of APs. Using this new feature, you simply apply a filter to select the desired set of 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.

- **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

- **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.

- **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.

- **Display Filters for Authenticators**

  - Customers with large number of Authenticators can now filter the display out on:
    - Authenticator Name
    - Authenticator IP Address

  Example :

- **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

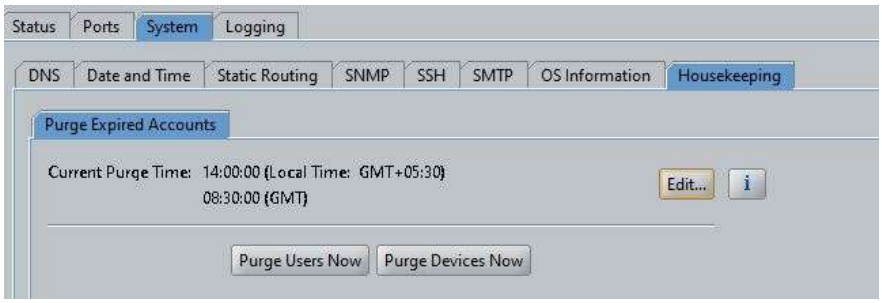
- **Clone Outbound Value**

  - 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.

- **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:



- **Ignition Server RFC 4675**
  - Enhanced Ignition Dashboard configuration of RFC 4675 Outbound attribute
- **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.
- **Ignition Server Quick Add MAC Address**
  - Added ability to add MAC address of user device from the Actions of user authentication logs
- **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*.

Guest & IoT Manager 9.3.x

- **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.
- **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.

- **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 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 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
- **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 xyz
- **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
- **Option to exclude Network Configuration 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.

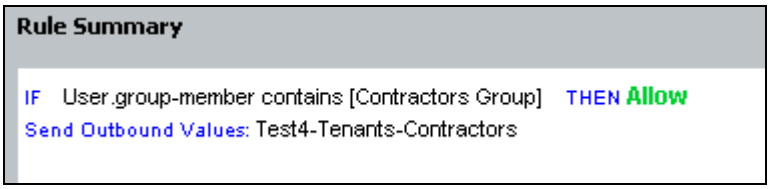
- This feature allows guests to receive again their password in case was forgotten
- The workflow is also available to Self-Service guest and may be enabled or disabled by admin to be available to the self-service guest

- **Localized Characters in Provisioner Username**

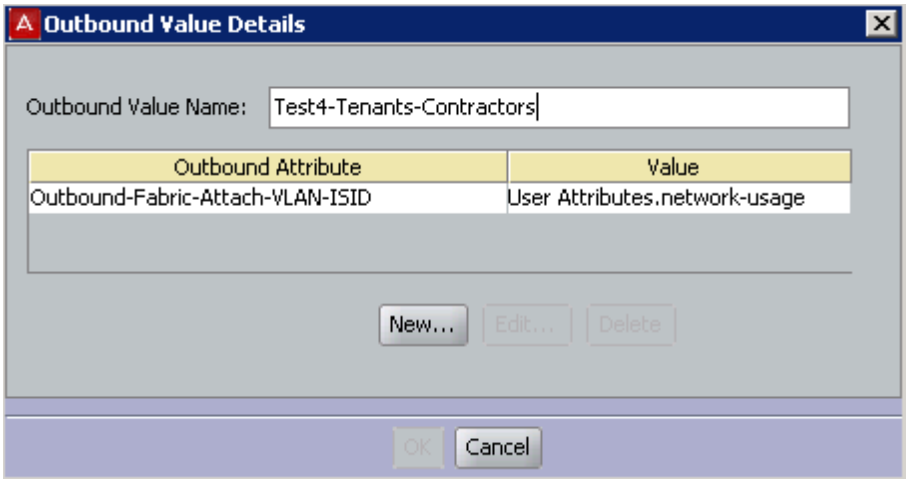
  - Allow AD authentication of Provisioners whose username/Password contains Localized characters.

- **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.

- **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

9.1.4 New and Enhanced Features in Releases 9.4.0

- **Ignition Server & Dashboard 9.4.0**

  - **Identity Routing for MAC Authentication**

    Prior releases in Ignition Server the Identity Routing concept was available only for RADIUS User Authentication flow and not available for MAC Authentication flow. The lookup of the MAC address of the Devices was done against the Local Store. Now we can define Device Set in addition to User Set in Directory Sets and that Device Set can be used in Identity Routing for MAC Auth Access Policy. Note that currently Device lookup supports external service from Infoblox and internal service to the local store.

  - **Ignition Server Integration with Infoblox**

    Identity Engines now support Infoblox which is primarily a DNS, DHCP and IP address management application that can also act as the device repository. It helps to discover / monitor the network and record all the various entities / devices that are on the network at any given point of time. Infoblox lookup is currently available for MAC authentication only.

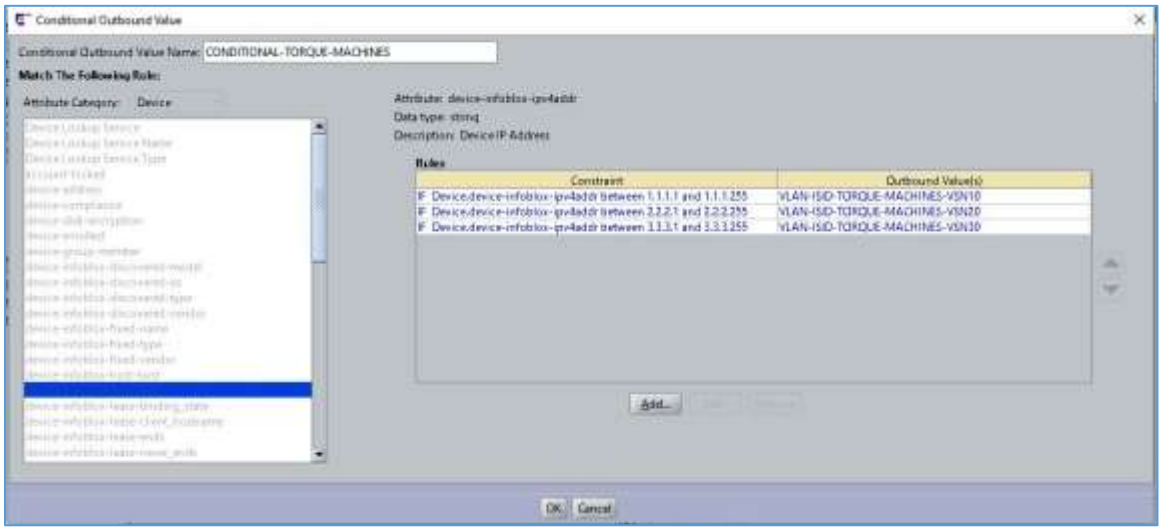
Example:

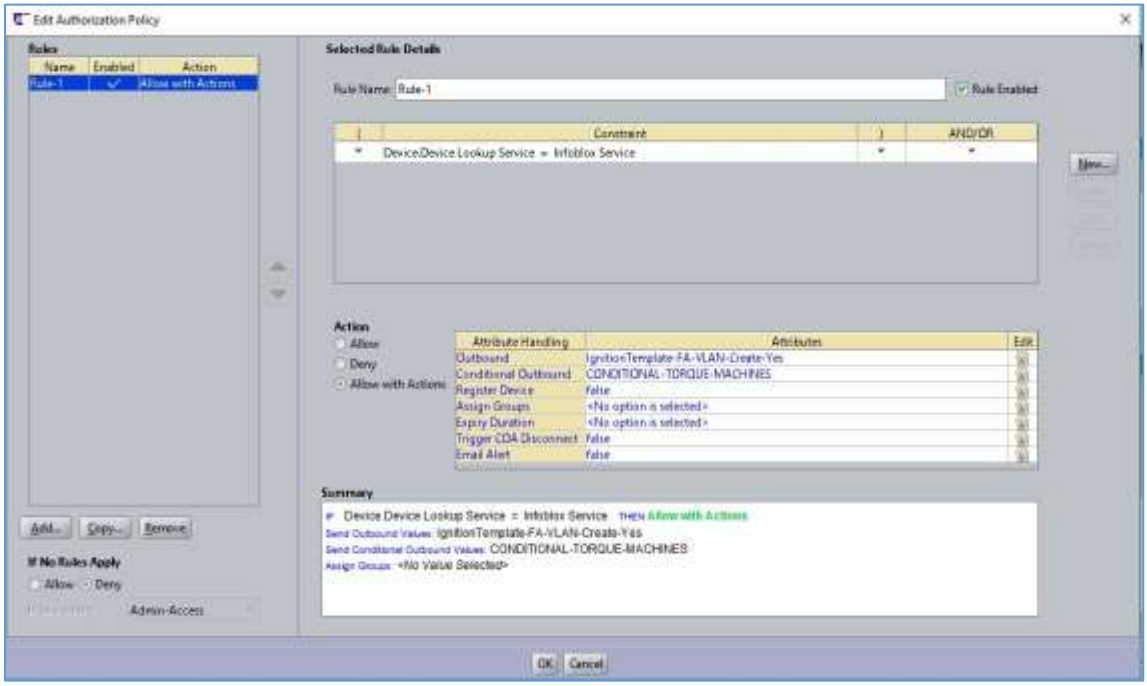
- **Conditional Outbound Values (COV)**

  In the previous releases, one can send one or more outbound values based when a rule is met in the Authorization policy. And to add another condition/constraint, a new rule must be defined. And if similar rules were defined in multiple policies, one must update all the policies separately.

  In release 9.4, we introduced a new feature called 'Conditional Outbound Value (COV)' wherein you can group multiple rules/constraints into a single COV. The processing of this COV still happens similarly to any other constraint match. But the advantage of this approach is that this COV can then be re-used in multiple Access Policies. And any updates to the COV will automatically get reflected in all the associated policies without the need for the administrator to manually.

Example:





- **Online Certificate Status Protocol (OSCP)**

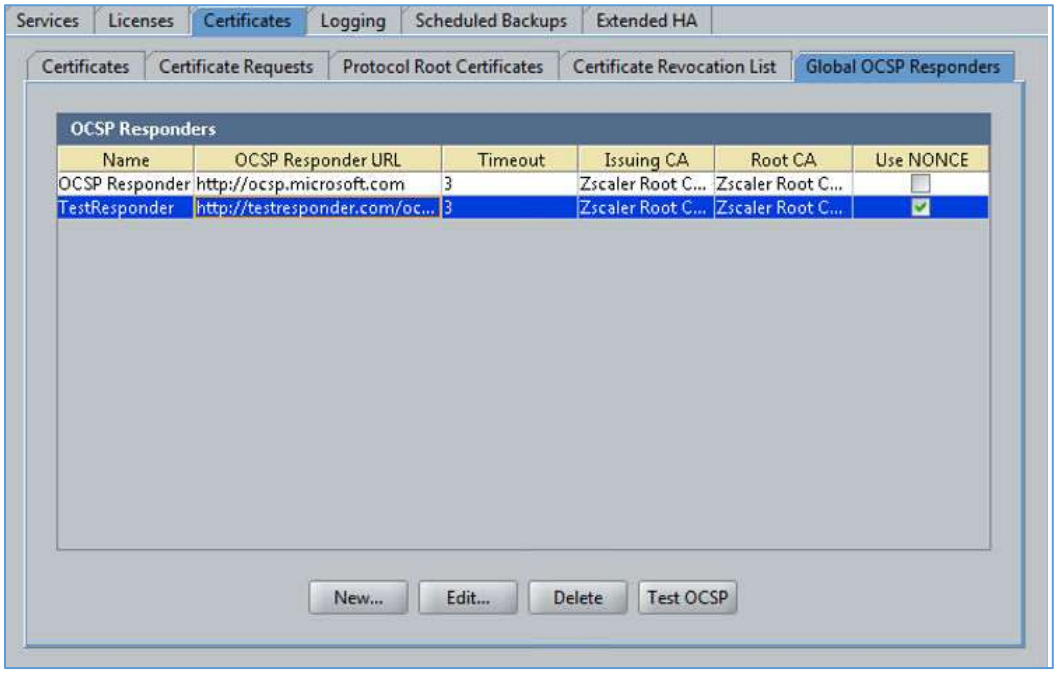
  Up until now, Ignition Server supported checking the revocation status of client certificates through CRL method. In this method, the client certificate revocation is checked against a periodically published CRL list which is downloaded onto the Ignition Server at certain time intervals.

  Starting from release 9.4, Ignition Server can now dynamically check the client certification revocation status using OCSP. Whenever a client presents its certificate for authentication, Ignition Server can read the client certificate to see if there's any OCSP responder is present in the certificate itself. If present, then it'll check against that OCSP responder.

Alternatively, administrator can also specify one or more global OCSP responders and Ignition Server can validate against that if no OCSP responder info is present in the client certificate.

Note: The original CRL based validation is still available. If NO OCSP responder information is present nether in the client certificate nor in the global OCSP responder configuration, Ignition Server can continue to check the client certificate revocation status against the CRL.

Example:



- **RBAC Changes for Configuration Administrator**

  In the previous releases of Ignition Server, if multiple Configuration Administrators try to log in to the Dashboard, then only the first logged in Configuration Administrator is allowed with read / write permissions. All other config admin logins are disallowed. In this release, if one Configuration Administrator is already logged in to the Dashboard, the subsequent Configuration Administrator login will still be allowed but the permissions are lowered to a Troubleshoot Administrator role. The role lowered information will be indicated in RED color at the bottom of the Dashboard main window.

- **CLI Changes for RBAC**

  Ignition Server now allows the System Administrator to configure the Idle and Session time-out values through CLI commands.

- **Extended HA Changes**

Configuring both “Extended-HA Import” and “Extended-HA Export” schedule on the same node is now supported. This is especially useful if there’s double fail-over and both pairs are active at some point of time and synching only in direction wouldn’t aggregate the guest accounts correctly.

However, administrator can configure only one import and one export per site. If the Back-up configuration from previous release have multiple scheduled Import or Export, then in current version during restore an warning message will be displayed as “System is configured with more than one Extended HA export and / or import schedule(s). Only one Extended HA export and import schedule should be configured. Please remove any additional Extended HA import and / or export schedule(s)”.

- **Bulk Authenticator Operation Enhancements**

  Various bulk Authenticator operations are supported in this release. These include enabling / disabling the authenticator(s) and changing the COA / RADIUS shared secret.

- **RADIUS VSA Support for Extreme Wireless**

  New support for RADIUS Vendor-Specific Attributes Support for ExtremeWireless and ExtremeWireless-WiNG.

  The full set of RADIUS Vendor-Specific Attributes have been added to the default database on the Ignition Server to provide seamless integration with the ExtremeWireless and ExtremeWireless-WiNG product suites. Administrators can create inbound/outbound attributes for these VSAs and utilize them in the Authorization Policies as needed.

Guest & IoT Manager 9.4.0

- **IOT Onboarding and Administration**

  Guest and IoT Manager Application now allows Provisioners to manage Non-Guest and IoT Manager (non-GIM) devices that are created through Guest and IoT Manager application. New field **All Non-GIM Devices** is available in the **Devices** tab for Administrator to allow Provisioners belonging to this Provisioning Group to manage Non-Guest and IoT Manager devices. It also provides an optional Static group selection to further limit the access of the Provisioner managing these devices.

  Provisioners can now use Bulk Modify feature to view / edit Non-Guest and IoT Manager devices. New field **Bulk Modify** is available when logged in as **Provisioner** > **Device** > **View** , and selecting the Provisioning group that contains Non-Guest and IoT Manager devices from the **Provisioned by** drop-down field.

- **CSV Device Import Flow Changes**

  - **Override Duplicate MAC Entries:**
    Provisioner can now Import Devices from a CSV File which contain MAC entries that are already present in the Ignition Server **Override Duplicate Records** field is available in *Load Devices* screen.

- **Group Assignment of Devices from CSV File:**
  Provisioners can now Import Network Access Groups from the GUI or CSV file, if the Provisioning Group selected has access to modify Network Access Rights of a Device. **Group Assignment (Input from)** field with **CSV** and **GUI** option is available in the *Load Device* screen.

- **Customizing Guest User Notification Template**

  Administrator can now customize Guest User Notification email template selecting **Email Charset** options available in the **Create Provisioning Group Notification** tab. Administrator can select **HTML Charset** or **Plain Charset** for the contents of the Guest User email. HTML Charset allows to select Font family, Size and Color to customize the Guest User Notification Email Contents and the Plain Charset will send an email with plain characters without any standard custom-tailoring to the content. The Terms of Use/Additional Information can now be appended in the Guest User Notification template.

- **Creating Permanent Guest User Accounts**

  The Administrator can now allow a Provisioner to create Permanent Guest User Accounts.

  Permanent (Yes / No) option alongside **Max Validity Duration** option beneath **Account Validity Duration** option in **Guest User** tab is available to the Administrator, if the Account Validity duration cannot be edited by the Provisioner.

- **Sponsor URL Multiple Interfaces Support**

  Administrator can now select the required interface to allow a sponsor to have access to a certain network to approve or deny received requests.

  The **Select Interface** drop-down field is available in the **Sponsor** tab.

- **Modify Random Password Special Characters**

  Administrator can now set the password complexity by selecting the alphanumeric check boxes: lower case, upper case, number, and special character along with the required number of characters condition.

  If **Random Generated Password** option is selected in **Guest User** tab, then the system generates a random password and send an email to the Guest User containing special characters similar to an Admin password while the provisioner creates a guest user.

- **Special Characters in Provisioning Group Name**

  Administrator can now create a provisioning group name using alphanumeric / special characters and space in between words. For example, use only these special characters: # =()_-.! [].

- **Providing Passphrase for Key**

  Administrator can now generate private key for the certificate with passphrase and provide the passphrase while binding the certificate and chain. Ensure that the valid passphrase is provided, so that the bind does not fail and result in HTTPD restart failure. The **Passphrase** field is available *Bind Certificate and Key* pop up window and *Bind Chain* pop up window.

9.2. Issues Resolved in this Release

Item Number	Description
JUPITER-3878	Active Directory may return STATUS_PIPE_EMPTY response code during authentication workflow. This is a Windows Server defect in legacy SMBv1. Ignition 9.3.3 now uses RPC over TCP transport and is no longer SMBv1 dependent.
JUPITER-4099	CertMgrServer process may restart while importing a duplicate certificate or a certificate with no CN (CommonName) specified.
JUPITER-4231	Support has been added for new gTLDs (generic top level domains) in Guest Manager provisioner / self-provisioner.
JUPITER-4273	Adding Ignition server's capability to display New User's group association under Dashboard / Syslog Audit logs. This mimics existing logging behavior for New Device logging.
JUPITER-4310	Attempting to edit an existing AirWatch MDM may fail if another AirWatch MDM service uses a different Server URL but same GroupID.
JUPITER-4311	CVE-2003-1418 Apache Tomcat HTTPD Server ETag Header Information Disclosure Vulnerability resolved in Guest Manager.
JUPITER-4348	An empty username or password in EAP-TLS/TTLS requests may cause RADIUS service to restart.
JUPITER-4349	Ignition Dashboard SMTP Authentication is broken for BASIC authentication dialect.
JUPITER-4546	Ignition Dashboard now correctly validates the format of the AirWatch MDM Server URL field.
JUPITER-4451	If Ignition Analytics is enabled, syslog messages are incorrectly mirrored to the system messages file. This is resolved.
JUPITER-4578	In prior Guest Manager releases, self-service users/devices were considered 'temporary' and would always 'Delete On Expire' regardless of provisioner policy configuration. It is now possible via provisioner policy to toggle this option.

9.3. Outstanding Issues

Item Number	Description
JUPITER-3597	NTP Skew May Cause Bootup Delay. Ignition may experience a delay during startup if configured to synchronize with a NTP clock source. If the clock source is at a time in the past compared to the Ignition appliance this problem may occur. Extreme recommends configuring Ignition to synchronize time with its hypervisor in lieu of NTP and configure the hypervisor to synchronize its time with the NTP clock source.
JUPITER-4132	Unexpected HAPBServer Core Triggered HA/Zdb ReElection
JUPITER-4302	Network Analytics: Email validation on scheduler page is not complete.
JUPITER-4313	ZdbServer Core "Queue is Full" 9.3.1_31472
JUPITER-4452	Disabling Ignition Analytics Logging In Dashboard Deletes Server IP Address

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-4126	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	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	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.
JUPITER-4334	Unable to get `systemserialno` while configuring admin interface IP other then /24 subnet If the admin interface IP is configured with a subnet other than /24 then there are some issues generating the system serial number information. As a workaround, please make sure to configure the admin interface IP with a /24 subnet. Note that this workaround is only meant for admin interface. The service interface IP can be assigned a subnet (other than /24) as per requirements.

9.5. Important Application Notes

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

- **Ignition Dashboard User Preferences**
  - With Identity Engines 9.4.0 release, the applications logs, user preferences and certs / keystore and location at a different location indicated below. Kindly make a note of the same:

    C:\Users\<user id>\AppData\Roaming\Extreme Networks

- **System-Admin Session Timeout**
  - Identity Engines 9.4.0 release introduces a new feature by which the system-admin's Dashboard Session and Idle timeout can be specified by a CLI.
  - If administrator is using a Site Group concept in Ignition Dashboard then please make sure that the Session and Idle timeout configured for all the nodes are the same else Ignition Dashboard may not behave accurately for these settings.

- **Guest & IoT Manager Cache**
  - After deploying Guest & IoT Manager 9.4.0, please make sure the browser cache and cookies are cleared before logging in as Admin or Provisioner. In the absence of this step, some stale references and preferences are carried over from earlier release. Same needs be done after config import.

- **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

- **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 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 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.

10. Upgrade Procedure

10.1. Ignition Server 9.4.0 - Pre-upgrade Checklist

Ignition Server Checklist

- By design, neither Software Upgrade flow nor Configuration Restore flow form 9.0.x/9.1.x to 9.4.0 is supported.
- If you are running 9.2.x, 9.3.0, 9.3.1, 9.3.2 or 9.3.3 you may perform Configuration Restore to 9.4.0 release.
- If you are running 9.2.x, 9.3.0, 9.3.1, 9.3.2 or 9.3.3 you may perform Software Package upgrade as follows:
    - If you are running 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1, 9.3.2 or 9.3.3 you may perform Software Upgrade directly to 9.4.0 release.
    - If you are running 9.2.3 or 9.2.4, you may perform Software Upgrade to 9.4.0 release via an intermediate 9.2.5 path (i.e. 9.2.3/9.2.4 to 9.2.5 then to 9.4.0)
- As best practice, always perform the following before any upgrade or restore
    - Take a backup of your Ignition Server configuration
    - Take a VMware snapshot of the Ignition Server Virtual Machine while the VM is in **shutdown state**.
- SSO Reminder
    - Please be reminder that Ignition Server 9.3.3 onwards does not support SSO feature. If you are migrating from any earlier supported release and have SAML access policies configured then the Software Upgrade or Configuration Restore flow will no longer work.
    - You **must** delete any SAML access policy configured in the system before initiating a Software Upgrade or Configuration restore to 9.4.0 release.

10.2. Ignition Server 9.4.0 - Software Upgrade Procedure

- **Migrating from IDE 9.1.x**

  If you are running Ignition Server release 9.1.x and would like to migrate to Ignition Server release 9.3.3:
    - First step migrate to 9.2.0
        - Take a configuration backup from 9.1.x
        - Deploy a fresh new VM 9.2.0
        - Perform a configuration restore from 9.1.x into 9.2.0
        - Perform a new backup of the 9.2.0 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.
    - Second step migrate 9.2.0 to 9.4.0
        - Deploy a fresh new VM 9.4.0
        - Perform a configuration restore from 9.2.0 into 9.4.0
        - Perform a new backup of the 9.4.0 configuration as a safety precaution step
        - New perpetual licenses will be required. Send email request to datalicensing@extremenetworks.com
        - Perform a new backup of the 9.4.0 configuration once the perpetual licenses are installed
        - **NOTE:** Until you receive your new perpetual licenses from Extreme Networks, you may request temp licenses by sending a request to datalicensing@extremenetworks.com

- **Migrating from IDE 9.2.x, 9.3.0, 9.3.1, 9.3.2 or 9.3.3 using fresh OVA install**

  If you are running Ignition Server 9.2.x, 9.3.0, 9.3.1, 9.3.2 or 9.3.3 and would like to migrate to release 9.4.0 using a new VM:
  - Take a configuration backup from your 9.2.x, 9.3.0, 9.3.1, 9.3.2 or 9.3.3
  - Deploy a fresh new VM 9.4.0
  - Perform a configuration restore from 9.2.x, 9.3.0, 9.3.1, 9.3.2 or 9.3.3
  - Perform a new backup of the 9.4.0 configuration
  - New perpetual licenses will be required. Send email request to datalicensing@extremenetworks.com
  - Perform a new backup of the 9.4.0 configuration once the perpetual licenses are installed
  - **NOTE:** Until you receive your new perpetual licenses from Extreme, you may use temp licenses by sending a request to datalicensing@extremenetworks.com

- **Migrating from IDE 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1, 9.3.2 or 9.3.3 using Software Package File Upgrade process:**
  If you are running Ignition Server 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1, 9.3.2 or 9.3.3 and would like to migrate to release 9.3.3 using Software Package upgrade flow:
  - Take a configuration backup from 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1, 9.3.2 or 9.3.3
  - In case of Ignition Server Standalone
    - Power down Ignition Server
    - Take a VMware Snapshot of the VM
    - Power up Ignition Server
  - In case of Ignition Server HA
    - Power down Ignition Server #1
    - Take a VMware Snapshot of VM #1
    - Power up Ignition Server #1
    - Power down Ignition Server #2
    - Take a VMware Snapshot of VM #2
    - Power up Ignition Server #2
  - Perform Software Package upgrade directly from 9.2.0, 9.2.1, 9.2.2, 9.3.0, 9.3.1, 9.3.2 or 9.3.3 to 9.4.0 using the Package (pkg) file
  - Perform a new backup of the 9.4.0 configuration
  - No new licenses are required

- **Migrating from IDE 9.2.3 or 9.2.4 using Software Package File Upgrade process:**

  If you are running Ignition Server 9.2.3 or 9.2.4 and would like to migrate to release 9.4.0 using Software Package upgrade flow:
  - In case of Ignition Server Standalone
    - Power down Ignition Server
    - Take a VMware Snapshot of the VM
    - Power up Ignition Server
  - In case of Ignition Server HA
    - Power down Ignition Server #1
    - Take a VMware Snapshot of VM #1
    - Power up Ignition Server #1
    - Power down Ignition Server #2
    - Take a VMware Snapshot of VM #2

        - Power up Ignition Server #2
    - Perform an intermediate Software Package upgrade from 9.2.3 or 9.2.4 to 9.2.5 using the intermediate Package (pkg) file.
    - Take a configuration backup from 9.2.5
    - In case of Ignition Server Standalone
        - Power down Ignition Server
        - Take a VMware Snapshot of the VM
        - Power up Ignition Server
    - In case of Ignition Server HA
        - Power down Ignition Server #1
        - Take a VMware Snapshot of VM #1
        - Power up Ignition Server #1
        - Power down Ignition Server #2
        - Take a VMware Snapshot of VM #2
        - Power up Ignition Server #2
    - Perform a Software Package upgrade directly from 9.2.5 to 9.4.0 using the Package (pkg) file.
    - Perform a new backup of the 9.4.0 configuration
    - No new licenses are required.

- **Migrating from Network Analytics 9.3.0 to Network Analytics 9.3.2 using fresh OVA install**

  If you are running Ignition Network Analytics 9.3.0 and would like to migrate to release 9.3.2 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 running VM
    - Take a backup of the Database Configuration from the current Network Analytics 9.3.0 running VM
    - Shutdown Network Analytics 9.3.0 VM

  Step 2: Generate System Serial number and request for new License
    - Deploy the new Network Analytics 9.3.2 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@extremenetworks.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 by sending a request to datalicensing@extremenetworks.com
    - Install the Network Analytics Trial License
    - Perform System Configuration restore into Network Analytics 9.3.2 using the 9.3.0 System Configuration file. Make sure that the “Include License” checkbox is unchecked.
    - Perform Database Configuration restore into Network Analytics 9.3.2 using the 9.3.0 Backup Configuration file
    - Once you receive the transferred license Install the received license

  Note: 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. Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

- Current Product Documentation : www.extremenetworks.com/documentation/
- Archived Documentation (for previous versions and legacy product) : ww.extremenetworks.com/support/documentation-archives/
- Release Notes : www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

Product purchased from Avaya

If you purchased your product from Avaya, use the following support contact information to get help. Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Extreme Networks, Inc. assumes no liability for any errors. Extreme Networks, Inc. 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

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks' 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

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks 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. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks' standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: http://www.extremenetworks.com/support under the link "Policies" or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

"Hosted Service" means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS, INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS

CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS 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 EXTREME NETWORKS, INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE ("EXTREME NETWORKS").

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Extreme Networks or an Extreme Networks Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks 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 unless expressly authorized by Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Extreme Networks' website at:http://www.extremenetworks.com/support/policies/softwarelicensing or such successor site as designated by Extreme Networks. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software.

The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A

CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Extreme Networks product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Security Vulnerabilities

Information about Extreme Networks' security support policies can be found in the Global Technical Assistance Center Knowledgebase at https://gtacknowledge.extremenetworks.com/

Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: http://documentation.extremenetworks.com, or such successor site as designated by Extreme Networks.

Contact Extreme Networks Support

See the Extreme Networks Support website: http://www.extremenetworks.com/support for product or Hosted Service notices and articles, or to report a problem with your Extreme Networks product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Extreme Networks Support website: http://www.extremenetworks.com/support/contact/ (or such successor site as designated by Extreme Networks), scroll to the bottom of the page, and select Contact Extreme Networks Support.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks