Configuring Avaya Identity Engines Ignition Guest Tunneling

Release 9.1.1
NN47280-504
Issue 02.04
December 2015

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

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya 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 Avaya. End User agrees 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 websites referenced within this site or documentation 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 Avaya hardware and software. 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 website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means a hosted service subscription that You acquire from either Avaya or an authorized Avaya 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 Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, 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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 Avaya or an Avaya 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 Designated Processor that hosts 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 types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya 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 Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage

Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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 Avaya. All content on this site, the documentation, Hosted Service, and the product 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 unless expressly authorized by Avaya. 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.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya 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 Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. 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 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 AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA 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 AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA 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

Customer acknowledges and agrees that it is responsible 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 Avaya 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.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

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

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(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

Contents

Chapter 1: Introduction

Purpose

The *Configuration Avaya Identity Engines Ignition Guest Tunneling* explains how to install, configure, and manage Ignition Guest Tunneling (IGT).

Related resources

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

    Note:

    Videos are not available for all products.

Subscribing to e-notifications

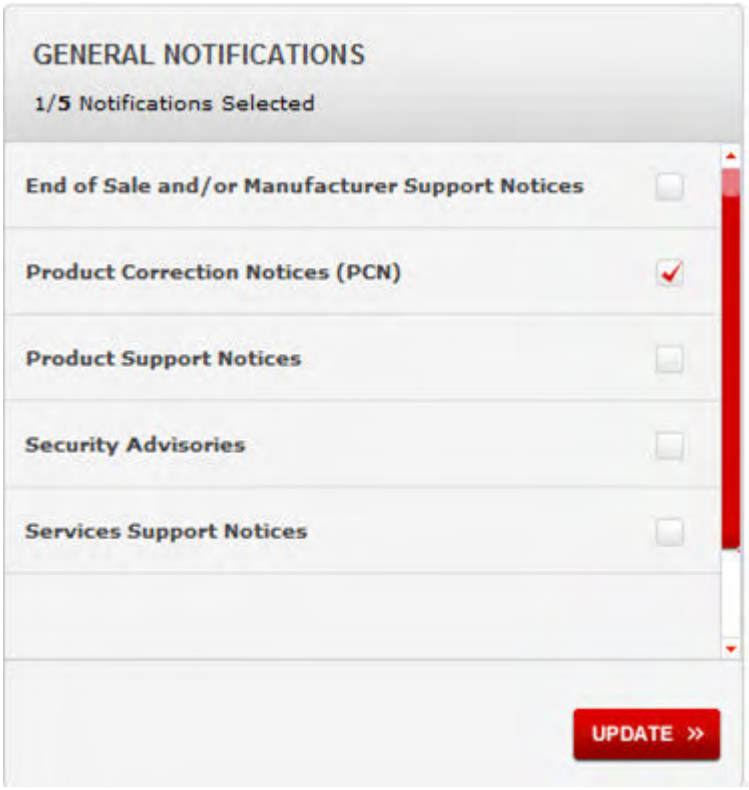
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

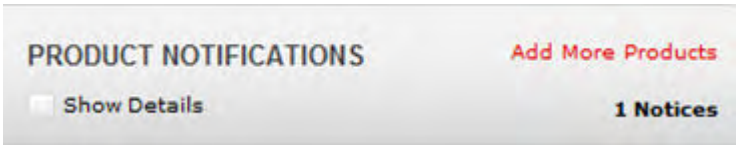
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services Platform 7000.

Procedure

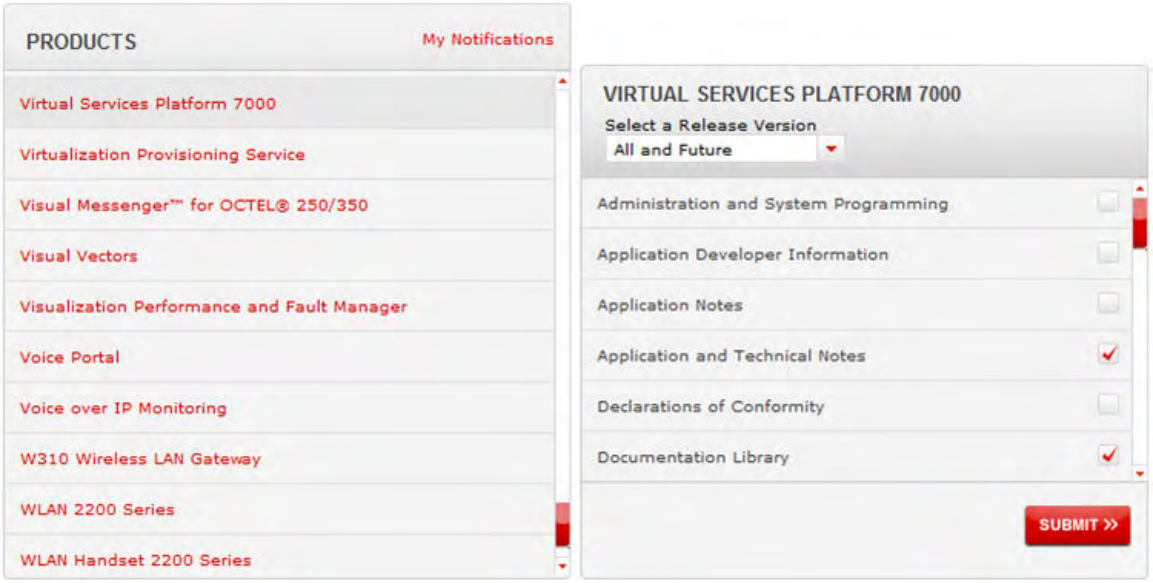
1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.



6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.



8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.



11. Click **Submit**.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.
3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks

- Include Comments

6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Support

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.

Chapter 2: New in this release

The following section detail what is new in *Configuring Avaya Identity Engines Ignition Guest Tunneling* for Release 9.1.1.

Ignition Guest Tunneling Enhancements

Following are the Ignition Guest Tunneling (IGT) enhancements for release 9.1.1.

- IGT is enhanced to support up to 300 WLAN 9100 APs and handle up to 5000 simultaneous clients per Virtual Machine instances.

Chapter 3: Introduction to IGT

Avaya Identity Engines Ignition Guest Tunneling (IGT) virtual appliance is an Avaya Identity Engines portfolio product which provides Wireless Local Area Network (WLAN) 9100 guest user traffic isolation solution using Generic Routing Encapsulation (GRE) tunneling technology.

Common Guest Network Isolation

Guest Network Isolation is a security requirement for network access control to separate the guest traffic from intranet and to separate intranet from guest traffic.

Common Guest Network Isolation steps includes:

- Mapping Service Set Identifier (SSID) and VLAN
- Tunneling from WLAN 9100 Access Point into the Demilitarized Zone (DMZ) part of enterprise network
- Enforcing through security policy and Firewall

Guest Network Isolation for IGT

IGT uses Guest Network Isolation to separate the guest traffic from intranet and to separate intranet from guest traffic.

Guest Network Isolation method for IGT includes:

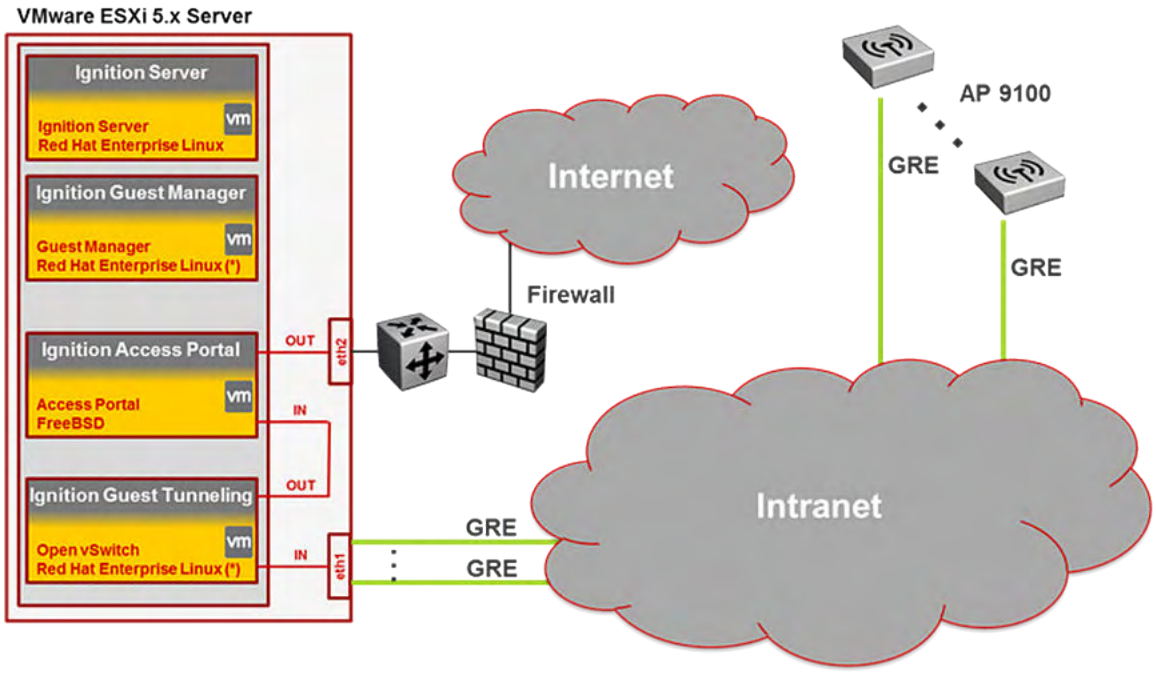
- Mapping SSID and VLAN
- Tunneling to IGT through the SSID and GRE tunneling

Use case examples

Following are the two use cases of GRE-based Guest Network isolation.

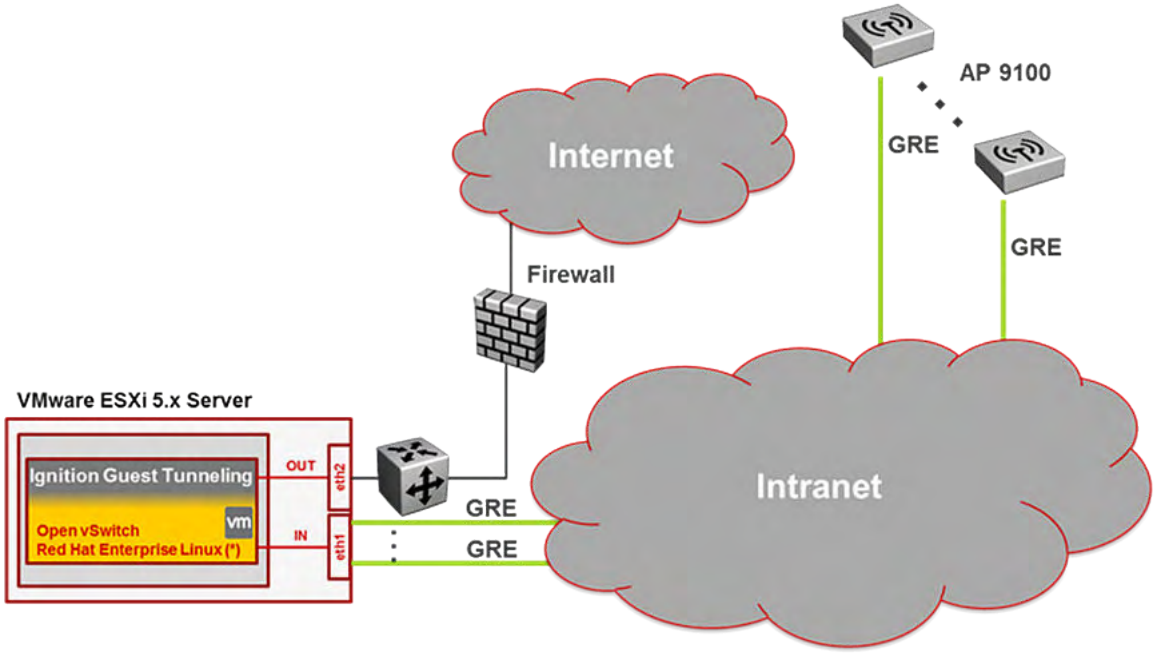
GRE-based traffic isolation for Ignition Captive Portal based authentication

GRE-based Guest Isolation Deployment deals with isolating guest traffic by making use of IGT and IDE Access Portal that acts as an external captive portal. The IGT's IN-interface is configured as the remote end point on the AP 9100. The AP tunnels the guest traffic to the IGT appliance. The appliance on receiving client traffic, decapsulates the packets and forwards it to the Access Portal. The Access Portal OVA can be deployed on the same server that hosts the IGT appliance. In this situation, the OUT interface of IGT is connected to the IN interface of the Access Portal. A Dynamic Host Configuration Protocol (DHCP) server can reside on the IN interface of the Access Portal. The OUT interface of Access Portal will be connected to the Internet or DMZ. Hence, guest traffic is routed from the AP to the guest tunneling appliance and later through the access portal. In case, the access point sends out client traffic on different VLAN, then IGT needs to be configured to strip the VLAN tag and forward the client traffic to the access portal as untagged.



GRE-based traffic isolation direct authentication without IDE Captive Portal

In GRE-based Traffic Isolation Deployment there is no captive portal. The AP to guest tunneling appliance connectivity remains similar to the GRE-based Guest Isolation Deployment. The IGT instead of forwarding the guest traffic to the access portal after decapsulating, forwards it to the next hop switch that in turn forwards the packet to the internet or DMZ through a firewall similar to how the rest of traffic is forwarded. This scenario supports both tagged and untagged client traffic with suitable modifications on the ESXi server.



Chapter 4: Installing IGT

This chapter describes the procedure to install Ignition Guest Tunneling (IGT) as a virtual appliance on a VMware ESXi server.

Installing and Configuring IGT requires tasks that are performed on the ESXi Server (Hypervisor) and the IGT Virtual Appliance instance. Ensure that the ESXi Server (Hypervisor) side tasks are appropriately performed, which will require separate administrative access to the Server side IT administration in your organization.

Following are the ESXi Server (Hypervisor) side tasks required to be performed:

- Installing IGT VM - ESXi Hypervisor console tasks.
- Configuring VLANs on ESXi Server mapping to IGT IN or OUT interface when configuring VLANs for the GRE tunnels.

System requirements

The following table describes the minimum system requirements to install IGT:

Software	Software Compatibility	Comments
Ignition Guest Tunneling	• VMware ESXi versions 5.1 or 5.5 • Installation on a VMware ESXi server is done using an OVA file which already incorporates the OS Red Hat Enterprise Linux.	• The VM requires a x86_64 capable environment • Number of CPUs - minimum 2 Dual-core CPUs • Memory - minimum 4GB • Storage (HDD or Flash) - minimum 20GB (VMware thin provisioning is allowed) • Minimum 1 physical NIC (preferably 3 NICs. Management, IN and OUT) • See https://www.vmware.com/ for a list of supported hardware platforms for ESXi.

Warning:

Avaya provides Ignition Guest Tunneling as a Virtual Appliance. Do not install or configure any other software on the VM shipped by Avaya.

- Avaya does not support the installation of any VMware specific, Red Hat Enterprise Linux (RHEL) specific, or any third-party vendor package or Red Hat Package Manager (RPM) on its VM, other than what Avaya ships as a package, image, or OVA.
- Do not install or uninstall any software components 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 VMs (including VMware Tools) unless Avaya documentation and/or personnel specifically instructs you to do so. Avaya does not support any deviation from these guidelines.

Caution using VMware Tools

Avaya determines which VMware Tools to install and configure. When required, Avaya provides these tools as part of the installation package. VMware Tools configures the kernel and network settings and unless Avaya tests and approves these tools, Avaya cannot guarantee that the VM will work after the tool is installed and configured.

Note:

At this time, Avaya does not support installing VMware tools.

IGT Network Interface mapping with VMWare ESXi and Server

IGT has three virtual network interfaces - vSwitch Port Group instances:

- **Management Interface (br0)** is a vSwitch Port Group instance dedicated for management of the devices. All the devices used in IGT provides Web or CLI based administration. Hence, having dedicated interface for management provides more security and agility.
- **AP Interface (br1)** is a vSwitch Port Group instance dedicated for AP and Guest Tunneling GRE connectivity.
- **Mobility Interface(br2)** is a vSwitch Port Group instance dedicated for Wireless LAN clients. All wireless client IP addresses and Ignition Access Portal IN interface will be part of Mobility VLAN subnets.

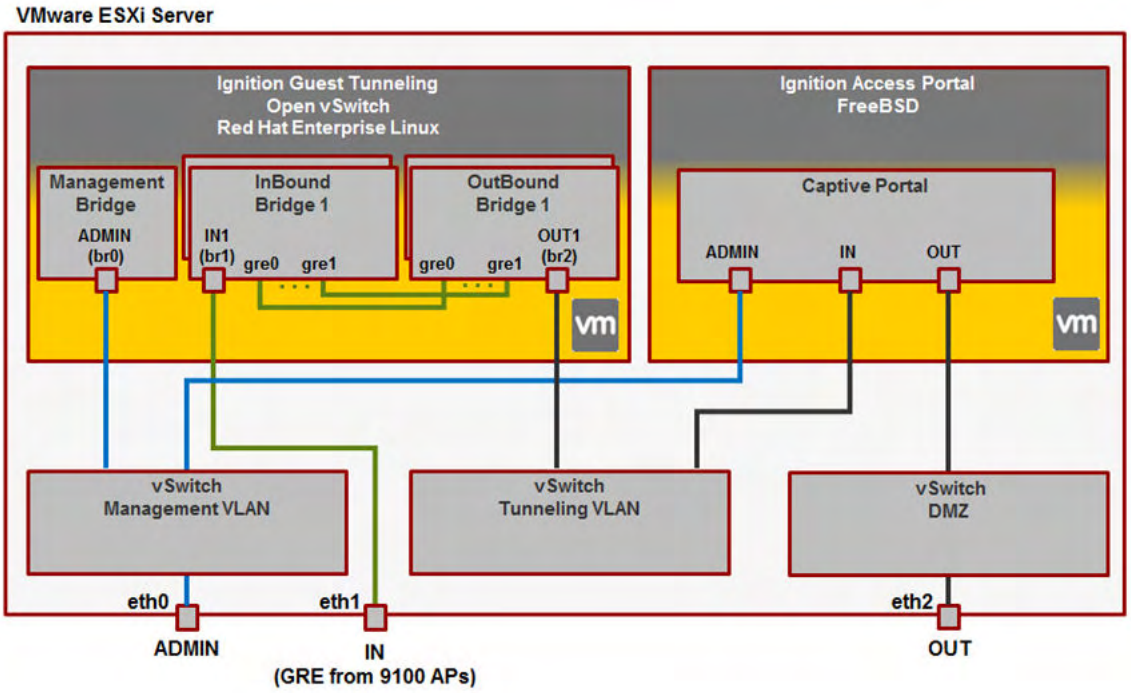


Figure 1: IGT Architecture

IGT interface shall be configured as shown below.

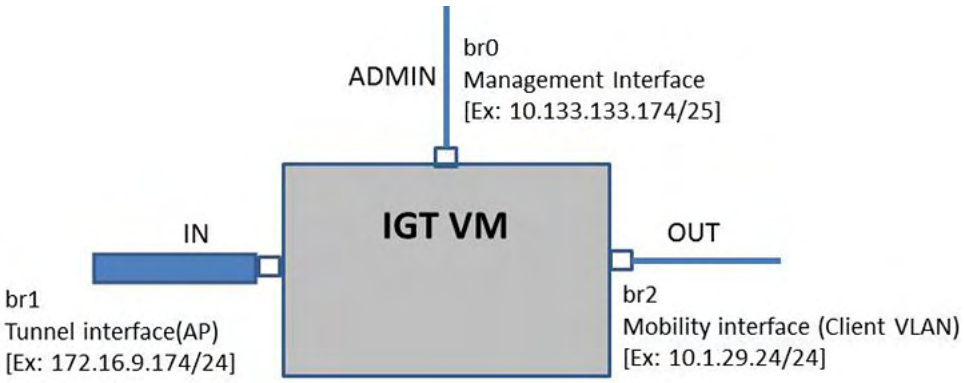


Figure 2: IGT interfaces configuration

IGT maps bridge interfaces (br0, br1 and br2) to linux interfaces (eth0, eth1 and eth2) respectively as shown below.

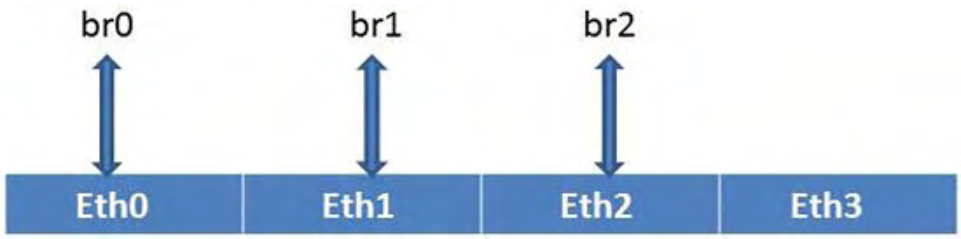


Figure 3: IGT interface mapping

Installation Overview

To setup IGT there are two types of configurations:

- Customizing ESXi Server Configuration - for IGT VM deployment
- IGT VM Configuration – Configuration made in IGT using IGT appliances.

Installing IGT VM - ESXi Hypervisor console tasks

Follow the below procedures in sequence to install and configure IGT:

1. Install IGT Virtual Appliance. For more information, see Installing IGT virtual appliance on page 18.
2. Initial Console settings of IGT. For more information, see Installing IGT – Console settings within IGT VM on page 20.
3. (Optional) Install WLAN 9100 Wireless Orchestration System (WOS) on the same Hypervisor as IGT. For more information, see Installing WLAN 9100 Orchestration System (WOS) on page 23.

Installing IGT virtual appliance

About this task

Avaya recommends that you use VMware vSphere Client to deploy the VM into your system. Start the VMware vSphere Client and log in to the ESXi server on which you want to install IGT.

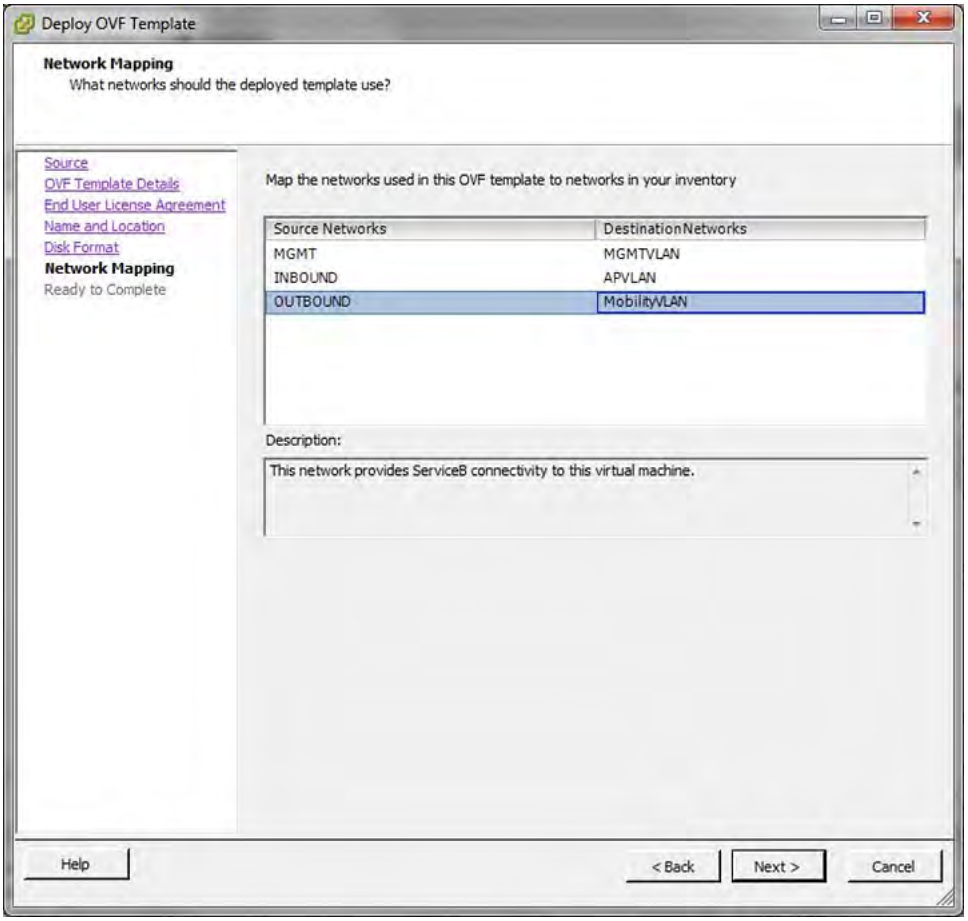
Procedure

1. Select **File** > **Deploy OVF Template** from the vSphere Client.
2. Click **Browse** to select the location to import the IGT virtual appliance and click **Next**.
3. Click **Accept** to accept the license and click **Next**.
4. Enter a **Name** for the virtual machine and click **Next**.
5. Select one of the following format to store the virtual disks and click **Next**.
   - **Thick Provision Lazy Zeroed** : Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created.
   - **Thick Provision Eager Zeroed**: A type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. This format takes longer time to create disks than to create other types of disks.

- **Thin Provision**: For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the disk size. Uses only as much datastore space as the disk needs for its initial operations.

By default, **Thick Provision Lazy Zeroed** format is selected.

6. Associate the IGT network interfaces to the correct VM network, based on site configuration.



For example, see IGT Network Interface mapping with VMWare ESXi and Server on page 16to know how to map IGT network interface with VMWare ESXi Server.

7. Review your settings. Click **Finish** to start the import.

Note:

Ensure that the **Promiscuous mode** is set to **Accept** for the newly created OUT interface.

By default, a guest operating system's virtual network adapter only receives frames that are meant for it. Because, IGT is acting as a tunneling server for the wireless clients, it has to check for packets that are meant to the wireless clients. Placing the guest's network adapter in promiscuous mode causes it to receive all frames passed on the virtual switch that are allowed under the VLAN policy for the associated port group.

8. Set the **Promiscuous Mode** to **Accept** for the newly created network. For more information, see Setting Promiscuous Mode for newly created network on page 20
9. Select the VM created from the tree on the left side of the **vSphere Client** window.
10. Start IGT by clicking the **Power on the virtual machine** link in the **Getting Started** tab.

    You can see the Avaya Ignition Guest Tunneling summary in the **Summary** tab.

Setting Promiscuous Mode for newly created network

About this task

Set the Promiscuous Mode to Accept for the newly created OUT interface.

Procedure

1. Click **VMware ESXi** IP address on the left of the **vSphere Client**.
2. Navigate to **Configuration** tab.
3. In the **Hardware** section, click **Networking**
4. Click **Properties** of the **Standard Switch: vSwichx**.
5. Select the new network created and click **Edit**.
6. Select the **Security** tab.
7. Select the **Promiscuous Mode** check box.
8. Select **Accept** from the drop-down list and click **OK**.

   In the vSwitchx Properties window in the **Effective Policies** section, you can see the Promiscuous Mode changed to **Accept**.
9. Click **Close** to close the vSwitchx Properties window.

Installing IGT – Console settings within IGT VM

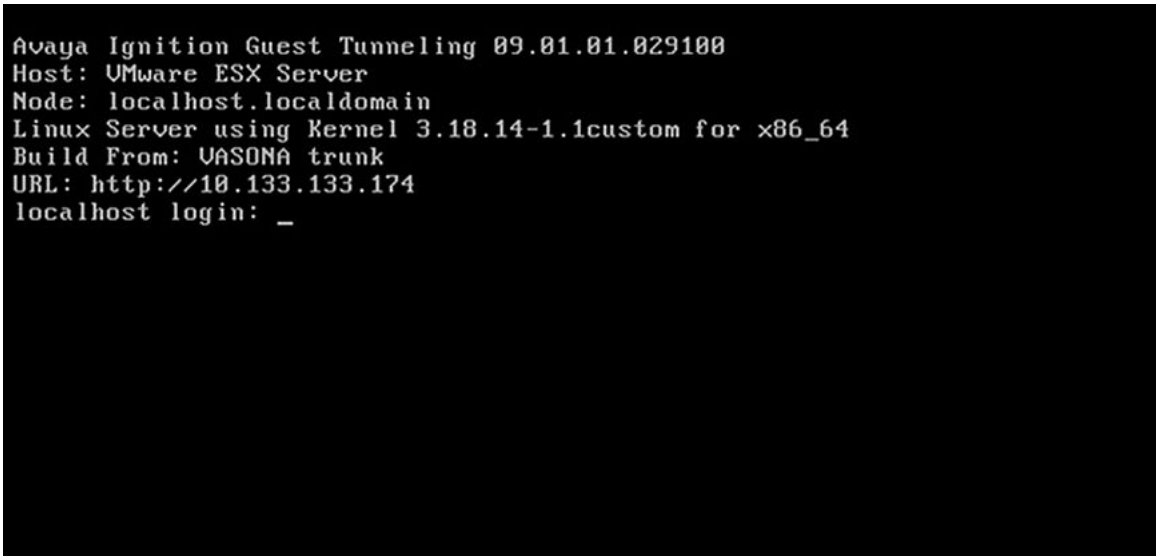
About this task

After you power on the IGT VM, configure the VM settings to start Ignition Guest Tunneling.

Procedure

1. Power on the VM and launch the Ignition Guest Tunneling console.

2. Enter the **username** and **password**. The default **username** and **password** is `admin` and `admin`.



3. Configure the management interface:

   `interface br0 ipaddr <IP Address>/<netmask>`

4. Configure the inbound interface:

   `interface br1 ipaddr <IP Address>/<netmask>`

5. Configure the outbound interface:

   `interface br2 ipaddr <IP Address>/<netmask>`

6. Configure the default route for the inbound interface:

   `route add <subnet>/<prefix> <gateway>`

   Note:

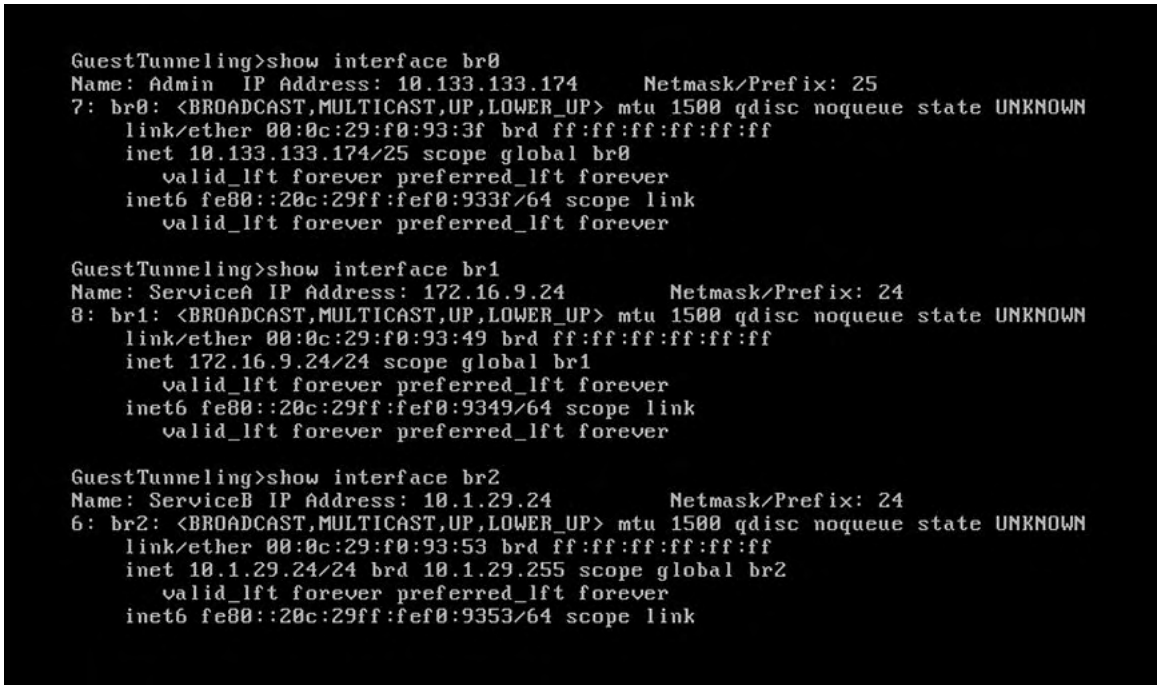
   - Setting a default route to bridge interface is optional. Ensure that the network connectivity with AP is Up.
   - Ensure that br0 bridge interface should not be configured with the default route. Because, packets that do not belong to br1 and br2 will get routed over br0 interface. This can cause leakage of traffic into the br0 network.
   - Promiscuous mode should be enabled only on br2 interface and it should be marked as **Reject** on other interfaces.
   - All the interfaces must be configured to a separate subnet and br2 interface must be in the same IP subnet range of the wireless client.

7. Configure the static route for the management interface:

   `route add <subnet>/<prefix> <gateway>`

Example

Following is the example to configure IGT interfaces.



IGT Network Configuration Checklist

The following table lists all the check points for IGT network configuration.

Check if all the listed points are TRUE, if any of the points are FALSE, see Troubleshooting Frequently Asked Questions on page 52.

No.	Task	✔
1.	The command **Show Interface** displays the bridges (br0, br1, and br2) created by default.	
2.	Bridges (br0, br1 and br2) are configured in different IP subnets.	
3.	br0 IP address is reachable from the PC used for accessing the IGT WebUI.	
4.	Access Point IP address reachable from IGT using source address as br1 IP address.	
5.	br2 IP address configured is in the wireless clients' IP subnet range.	
6.	br2 IP address is reachable from Access Portal IN interface.	

(Optional) Installing WLAN 9100 Orchestration System (WOS)

As an option, you can choose to install WLAN 9100 Wireless Orchestration System on the same server where IGT VM is installed.

For more information about using the WOS, see *Using the Avaya Wireless Orchestration System*, NN47252-103.

Chapter 5: Configuring GRE Tunnels in IGT and WLAN 9100

This chapter describes the procedures to configure GRE Tunnels in IGT and WLAN 9100.

WLAN 9100 GRE Tunnel Configuration

GRE Tunnel configuration on WLAN 9100 access points can be done through WLAN 9100 WOS and Access Point Web Management Interface (WMI).

WLAN 9100 WOS is a management application used to manage multiple access points. For more information about configuring GRE tunnel on WLAN 9100 WOS, see GRE Tunnel Configuration on WLAN 9100 Orchestration System on page 24.

Access Point WMI is a GUI used to manage a single access point. For more information about configuring GRE tunnel on WLAN 9100 WMI, seeGRE Tunnel Configuration on WLAN 9100 Web Management Interface on page 29.

GRE Tunnel Configuration on WLAN 9100 Orchestration System

Use the following procedure in sequence to configure GRE tunnel on WLAN 9100 Orchestration System.

1. Launching WLAN 9100 Orchestration System. For more information, see Launching WLAN 9100 Orchestration System on page 25.
2. Configuring SSID. For more information, see Configuring SSID using WLAN 9100 Orchestration System on page 25.
3. Configuring GRE tunnel. For more information, see Configuring GRE tunnel on WLAN 9100 Orchestration System on page 26.
4. Associating the GRE tunnel to SSID. For more information, see Associating the GRE tunnel to SSID on page 27.
5. Exporting WLAN Access Point configuration. For more information, see Exporting WLAN Access Points configuration on page 28.

Launching WLAN 9100 Orchestration System

About this task

Launch WLAN 9100 Orchestration System to configure tunnel.

Procedure

1. In a supported web browser, enter the IP address of the WOS (https://<*WOS IP Address*>).

2. Enter the **Username** and **Password**. The default **Username** and **Password** is `admin` and `admin`.

Configuring SSID using WLAN 9100 Orchestration System

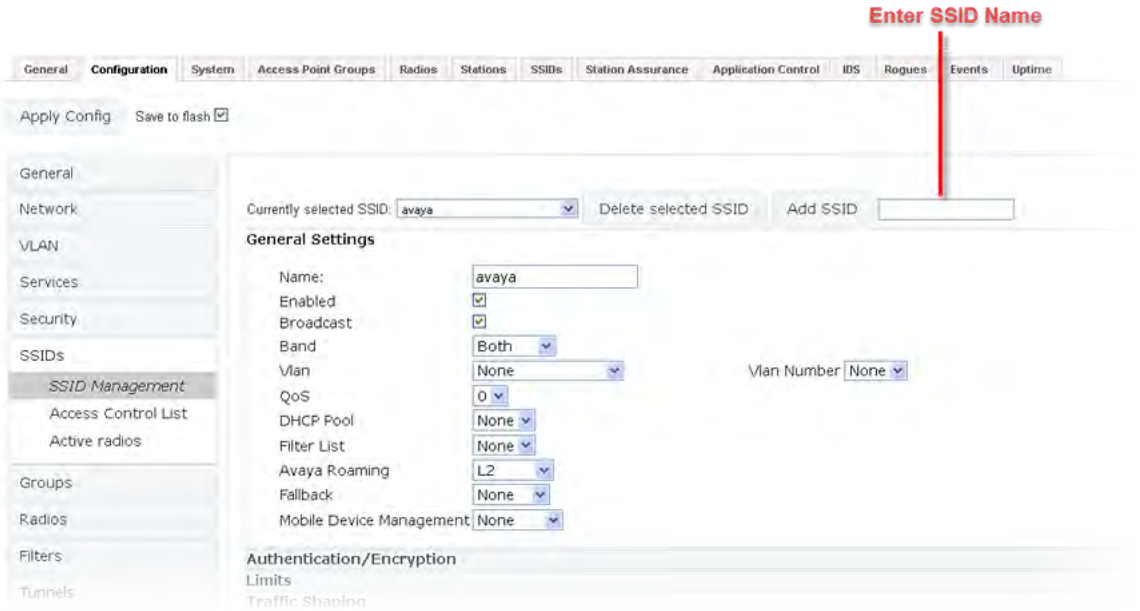
About this task

Configure SSID on AP using WLAN 9100 Orchestration System.

Procedure

1. Go to **Monitor** > **Access Points** > **<*AP instance*>** > **Configuration**.
2. Click **SSIDs** > **SSID Management**.

3. Enter the **Name** of SSID that you want to add.



4. Click **Add SSID**.
5. Click **Apply Config** to save the configuration.

Configuring GRE tunnel on WLAN 9100 Orchestration System

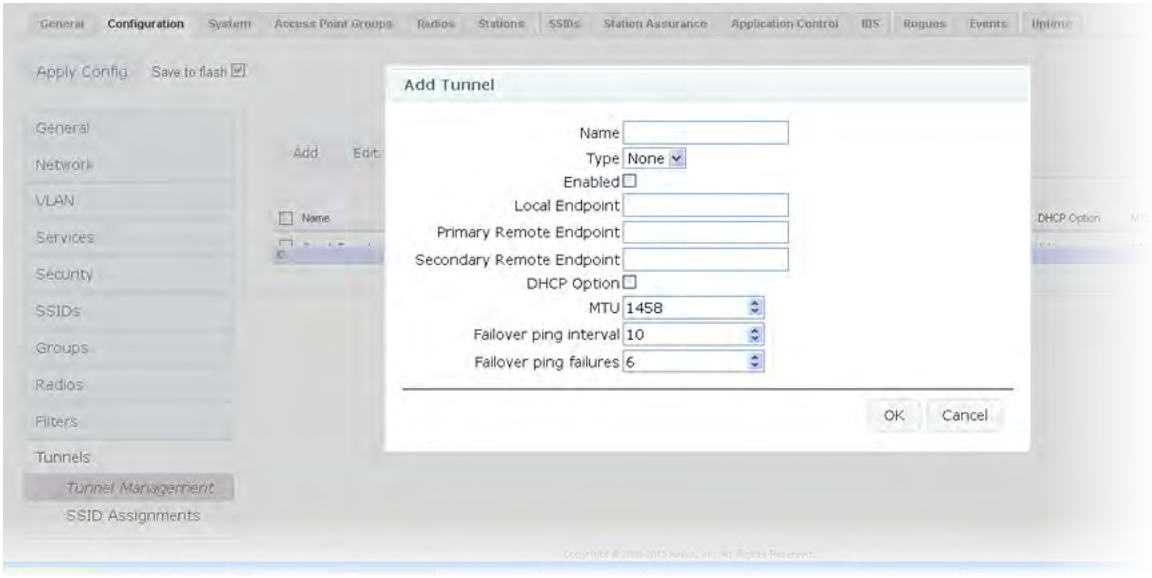
About this task

Configure GRE tunnel on AP using WLAN 9100 Orchestration System.

Procedure

1. Go to **Monitor** > **Access Points** > **<*AP instance*>** > **Configuration**.
2. Click on **Tunnels** > **Tunnel Management**.

3. Click **Add**. The Add new tunnel window displays.



To edit existing tunnel information, select the tunnel and click **Edit**.

4. Select **Type** as `gre` from the drop-down list.
5. Enter the **Local EndPoint** IP address (Access Point address).
6. Enter the **Primary Remote EndPoint** IP address (IGT inbound interface IP).
7. **(Optional)** Enter the **Secondary Remote EndPoint** IP address, for failover and redundancy purposes.
8. Click **Add**.
9. Click **Apply Config** to save the configuration.

Associating the GRE tunnel to SSID

About this task

Associate the GRE tunnel to SSID using WLAN 9100 Orchestration System.

Procedure

1. Go to **Monitor** > **Access Points** > **<*AP instance*>** > **Configuration**.
2. Click **SSID Assignments**.

3. Select the **SSID check box** to associate the GRE tunnel to SSID.

4. Click **Apply Config** to save the configuration.

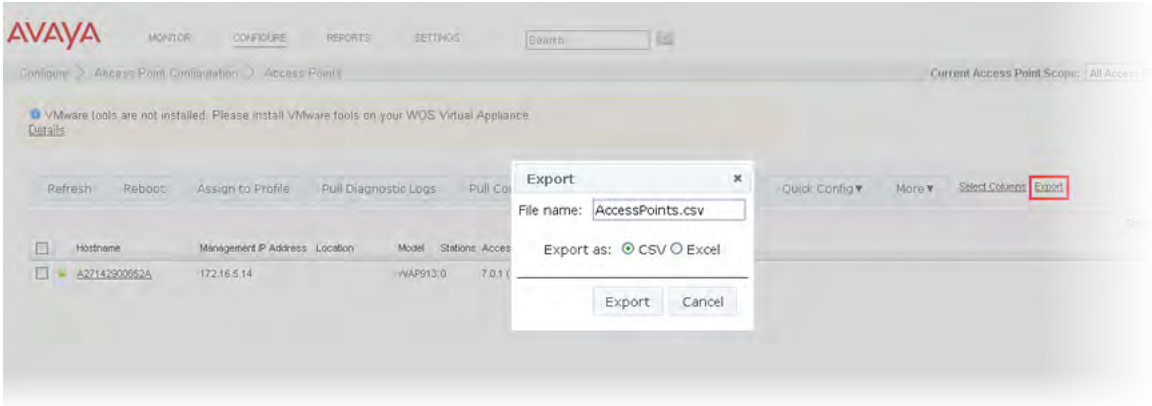
Exporting WLAN Access Points configuration

About this task

Export the Access Points configuration in .csv format.

Procedure

1. Go to **Configure** > **Access Point Configuration** > **Access Points**.
2. Click **Export link**.



3. Browse and select the .csv file.
4. Click **Export**.

GRE Tunnel Configuration on WLAN 9100 Web Management Interface

Use the following procedure in sequence to configure GRE tunnel on WLAN 9100 Web Management Interface (WMI).

1. Launching the WLAN 9100 WMI. For more information, see Launching WLAN 9100 Web Management Interface on page 29.
2. Configuring SSID. For more information, see Configuring SSID on Avaya WLAN 9100 WMI on page 30.
3. Configuring GRE tunnel. For more information, see Configuring GRE tunnel on Avaya WLAN 9100 WMI on page 30.
4. Associating GRE tunnel to SSID. For more information, see Associating the GRE tunnel to SSID on page 31.

Launching WLAN 9100 Web Management Interface

About this task

Launch WLAN 9100 Web Management Interface to configure tunnel.

Procedure

1. In a supported web browser, enter the IP address of the AP (https://<*AP IP Address*>).

2. Enter the **Username** and **Password**. The default **Username** and **Password** is `admin` and `admin`.

Configuring SSID on Avaya WLAN 9100 WMI

About this task

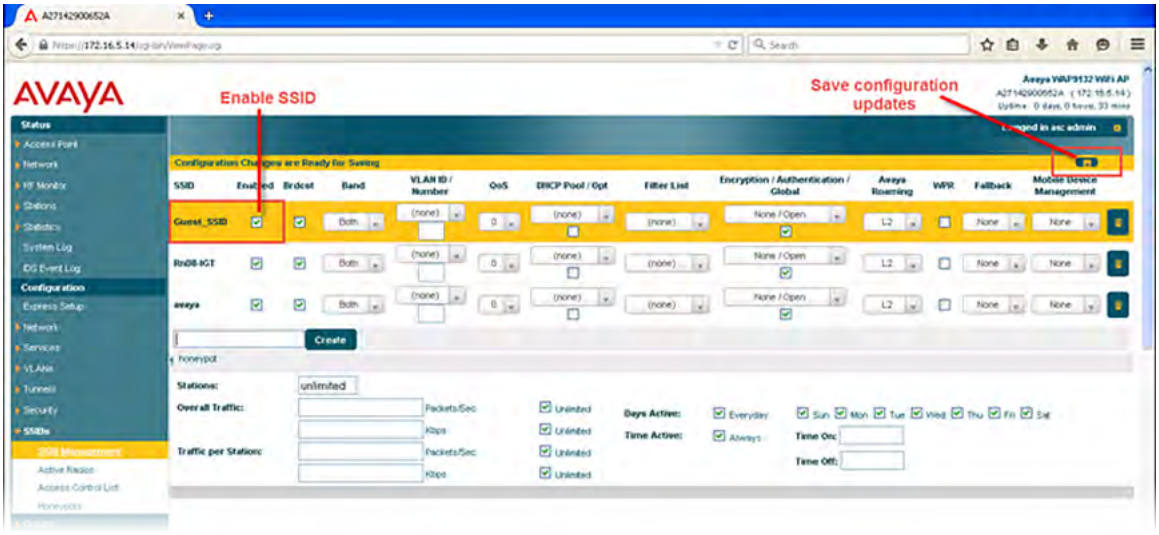
Configure SSID on AP using Avaya WLAN 9100 Web Management Interface.

Procedure

1. Go to **Configurations** > **SSIDs** > **SSID Management**.
2. Enter the **Name** of the SSID.
3. Click **Create**.

   A message box is displayed with the following note:

   “Note: New SSID created is disabled. Enable after configuration.”
4. Click **OK**.
5. Select the **Enabled** check box.
6. Click **Save** icon on top right corner below the **Logged in as: username**.



Configuring GRE tunnel on Avaya WLAN 9100 WMI

About this task

Configure GRE tunnel on AP using WLAN 9100 Web Management Interface.

Procedure

1. Go to **Configuration** > **Tunnels** > **Tunnel Management**.
2. Enter the **New Tunnel Name** and click **Create**.

   A message box is displayed with the following note:

   “Note: New tunnel created is disabled. Enable after configuration”.
3. Click **OK**.

4. Select the **Enabled** check box.
5. Select the **Type** to `gre` from the drop-down list.
6. Enter the following endpoints.
   - **Local Endpoint** (the AP address).
   - **Primary remote Endpoint** (the Ignition Guest Tunneling inbound interface IP).
   - **Secondary remote Endpoint** for failover and redundancy purposes.
7. Click **Save** icon on the right-top corner.

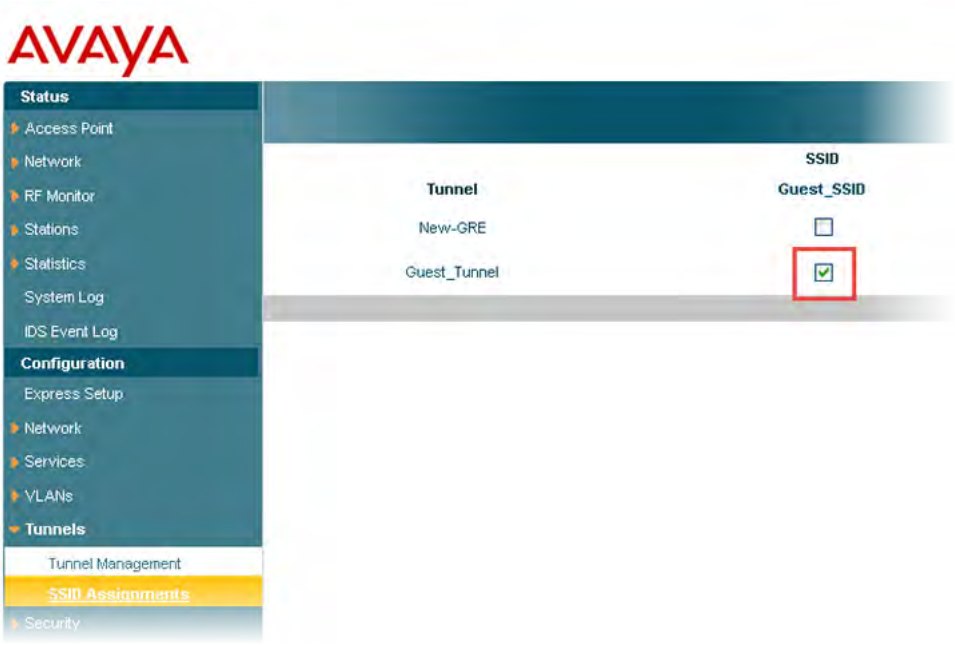
Associating the GRE tunnel to SSID

About this task

Associate the GRE tunnel to SSID using Avaya WLAN 9100 Web Management Interface.

Procedure

1. Go to **Configuration** > **Tunnels** > **SSID Assignments**.
2. Select the **SSID** check box to associate it with the GRE tunnel.



3. Click **Save** icon on the right-top corner.

IGT GRE Tunnel Configuration

Follow the below procedures in sequence to configure IGT GRE Tunnel in the IGT appliance and WLAN 9100.

1. Launch IGT Web User Interface to import, export the GRE Tunnel configuration .csv or .tar file, add, display or delete the GRE Tunnel in the IGT appliance. For more information, see IGT Web User Interface on page 32.
2. Configuring the IGT GRE tunnel VLAN to untag the VLAN traffic. For more information, see IGT Web User Interface on page 32.

IGT Web User Interface

Launch IGT Web User Interface to import, export the GRE Tunnel configuration .csv or .tar file, add, display or delete the GRE Tunnel in the IGT appliance.

Follow the below steps to configure and manage IGT GRE tunnel:

- Add GRE Tunnel. For more information, see Adding GRE tunnel on page 32.
- Display GRE Tunnel Status. For more information, see Displaying Guest Tunneling Status on page 33.
- Import GRE Tunnel. For more information, see Importing GRE tunnel on page 34.
- Export GRE Tunnel. For more information, see Exporting GRE Tunnel on page 34.

Adding GRE tunnel

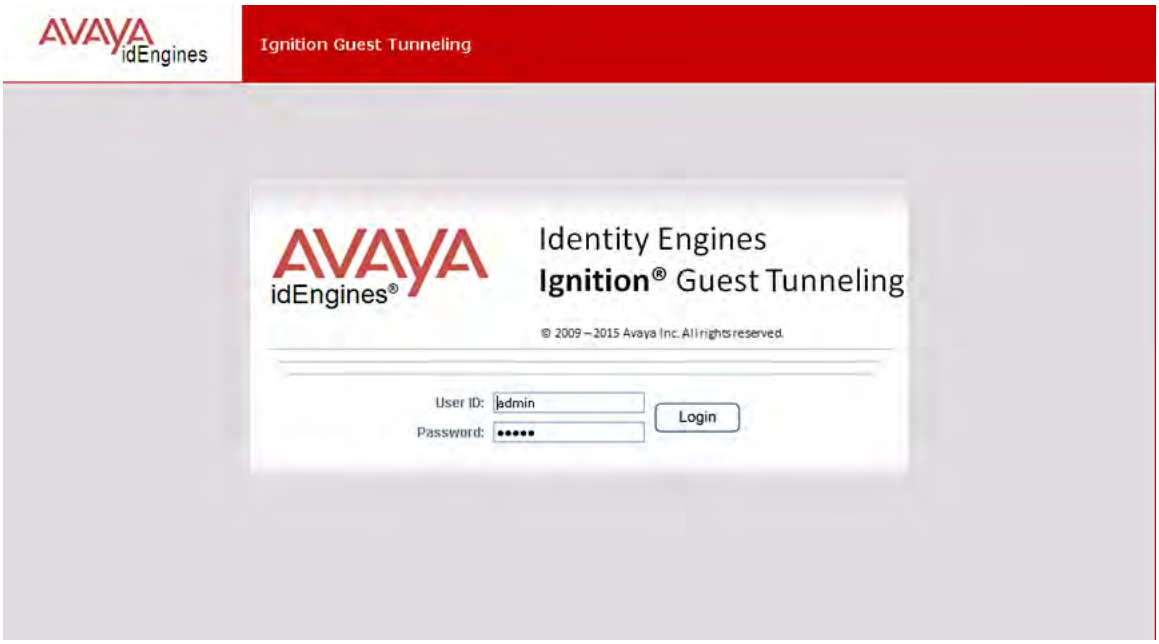
About this task

Add individual GRE tunnel into IGT.

Procedure

1. In a supported web browser, enter the IP address of IGT Appliance management (https://<*IGT Appliance mgmt IP address*>).

2. Enter **User ID** and **Password**. The default **User ID** and **Password** is `admin` and `admin`.



3. In the **Tunnel** menu, click **Add** to add new GRE tunnel.
4. Enter the tunnel remote endpoint.
5. Click **Add** to save the new GRE tunnel.

   The user interface adds the tunnel remote endpoint into IGT and displays the success message.

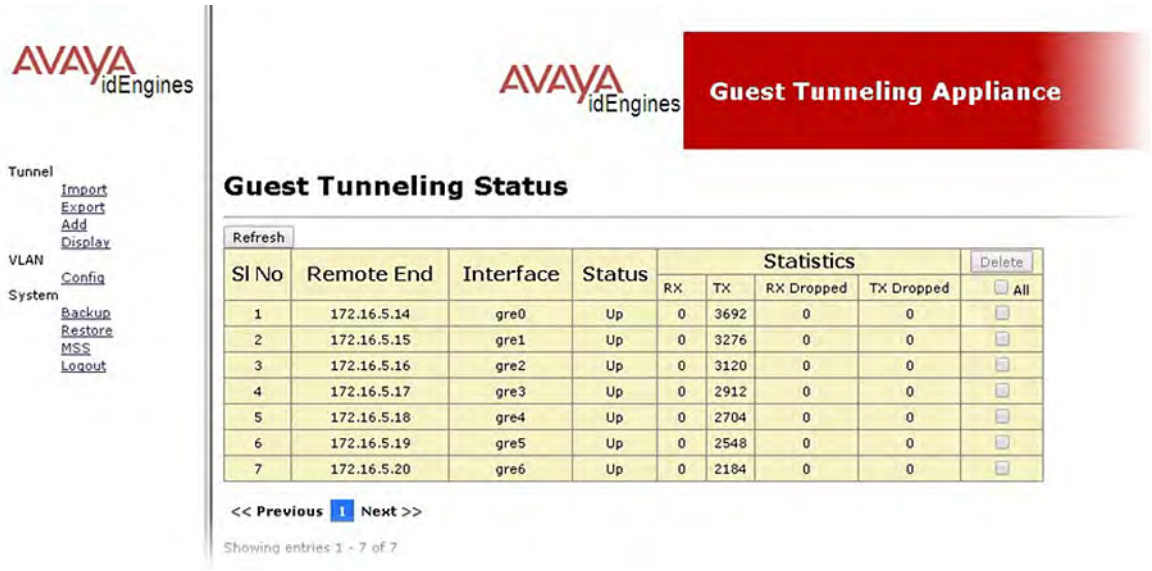
Displaying Guest Tunneling Status

About this task

Display the status of Guest Tunneling.

Procedure

1. In the **Tunnel** menu, click **Display** to display the status of Guest Tunneling.



   The Display Guest Tunneling Status window appears listing all the Guest Tunneling information.

2. **(Optional)** To remove a Tunnel, select the required tunnel check box and click **Delete**.
3. **(Optional)** Click **Refresh** to refresh the **Guest Tunneling Status** table.

Importing GRE tunnel

About this task

Import the GRE tunnel configuration .csv file from WLAN 9100 Orchestration server.

Procedure

1. In the **Tunnel** menu, click **Import**.
2. Browse and select the .csv file from your local hard disk.

   The .csv is exported from the WOS to configure the GRE Tunnels on IGT. For more information see, Exporting WLAN Access Points configuration on page 28
3. Click **Import** to import the .csv file.

   The user interface parses the .csv file and import only tunnel information into the IGT .

   After parsing, it displays a success message with the count of tunnels added.

Exporting GRE Tunnel

About this task

Export GRE tunnel from IGT.

Note:

Ensure to take backup of the GRE Tunnels before making any config changes, because when IGT VM is upgraded it replaces it with a new VM.

Procedure

1. In the **Tunnel** menu, click **Export**.

   The Export tunnel remote endpoint window appears.

2. Click **Export** to export the GRE tunnel.

   The Save as window appears.

3. Select the location in your local hard disk to save the .tar file.

Configuring IGT GRE Tunnel VLAN

About this task

Configure the IGT GRE tunnel VLAN to untag the VLAN traffic.

Procedure

1. In the **VLAN** menu, click **Config**.

   The Guest VLAN Untagging Configuration window appears.

2. Enter the **Guest VLAN ID** for which you want the IGT to untag the VLAN traffic and forward.

   Enter **VLAN ID** range between 1 and 4095.

3. Click **Untag VLAN**.

   The VLAN ID entered gets configured as **Guest Tunnel VLAN**.

Chapter 6: Managing IGT GRE Tunnel System

This chapter describes the procedure to manage the IGT GRE Tunnel System and to migrate IGT to new version.

Managing IGT GRE Tunnel

Use the following procedures to backup system configuration, restore it, configure Maximum Segment Size (MSS) and logout of the appliance.

- Backup System Configuration. For more information, see Taking Backup of IGT System Configuration on page 36.
- Restore System Configuration. For more information, see Restoring IGT System Configuration on page 37.
- TCP MSS Value Configuration. For more information, see Configuring TCP MSS value on page 37.
- Logout. For more information, see Logging out of Guest Tunneling Appliance on page 38.

Taking Backup of IGT System Configuration

About this task

Take Backup of IGT system configuration.

Note:

- The IGT system backup does not contain Tunnel and VLAN configuration. For more information on exporting tunnel configuration, see Exporting GRE Tunnel on page 34
- Ensure to take backup of the IGT system configuration before making any configuration changes, because when IGT VM is upgraded it replaces it with a new VM.

Procedure

1. In the **System** menu, click **Backup**.
2. Click **Export**.

The Save as window appears.

3. Select the location in your local hard disk to save the .tar file.
4. Click **Save** to save the .tar file.

Restoring IGT System Configuration

About this task

Restore the IGT system configuration.

Procedure

1. In the **System** menu, click **Restore**.
2. Click **Browse** to select the **Backup** .tar file from your local hard disk.
3. Click **Import** to restore the system configuration.

   Note:

   System will reboot automatically after import.

Configuring TCP MSS value

About this task

Configure TCP Maximum Segment Size (MSS) value to change the default value 1350 bytes.

Procedure

1. In the **System** menu, click **MSS**.
2. Uncheck the **Use Default** check box and enter the **TCP MSS** value (TCP MSS value ranges between 577 and 1422 bytes).

3. Click **Save**.

   MSS value gets saved and displays a success message.

Logging out of Guest Tunneling Appliance

About this task

Logout from Guest Tunneling appliance.

Procedure

In the **System** menu, click **Logout**.

The **Guest Tunneling Appliance** login page is displayed.

Migrating IGT to new version

About this task

Migrate IGT VM instances to new version.

Before you begin

- Take a backup of the System Configuration of your current version. For more information, see Taking Backup of IGT System Configuration on page 36.
- Take a backup of the Tunnel Configuration of your current version. For more information, see Exporting GRE Tunnel on page 34.

Procedure

1. Login to the ESXi Server to shut down the IGT current version.
2. Expand vSphere Client IP address and click IGT VM.
3. In the **Getting Started** tab, click **Power Off the virtual machine**.
4. After shutting down the IGT VM, deploy the new version IGT VM. For more information, see Installing IGT virtual appliance on page 18.
5. Restore the System Configuration. For more information, see Restoring IGT System Configuration on page 37.

   Restore the System Configuration using the previous version System Configuration backup file.
6. Restore the Tunnel Configuration. For more information, see Importing GRE tunnel on page 34.

   Restore the Tunnel Configuration using the previous version Tunnel Configuration backup file.

Chapter 7: Configuring AP 9100 and IGT to support VLANs

The AP 9100 supports VLAN tagging. After configuring the AP 9100, it sends encapsulated client traffic through transport VLAN (tunnel VLAN) to IGT. The IGT decapsulates the packets received on the GRE tunnel, removes the tagging on the VLAN and forwards the untagged packet to the Ignition Access Portal.

Configuring VLAN on ESXi Server mapping to IGT IN-interface

About this task

Configure VLAN on VMware ESXi Server for IGT IN-interface.

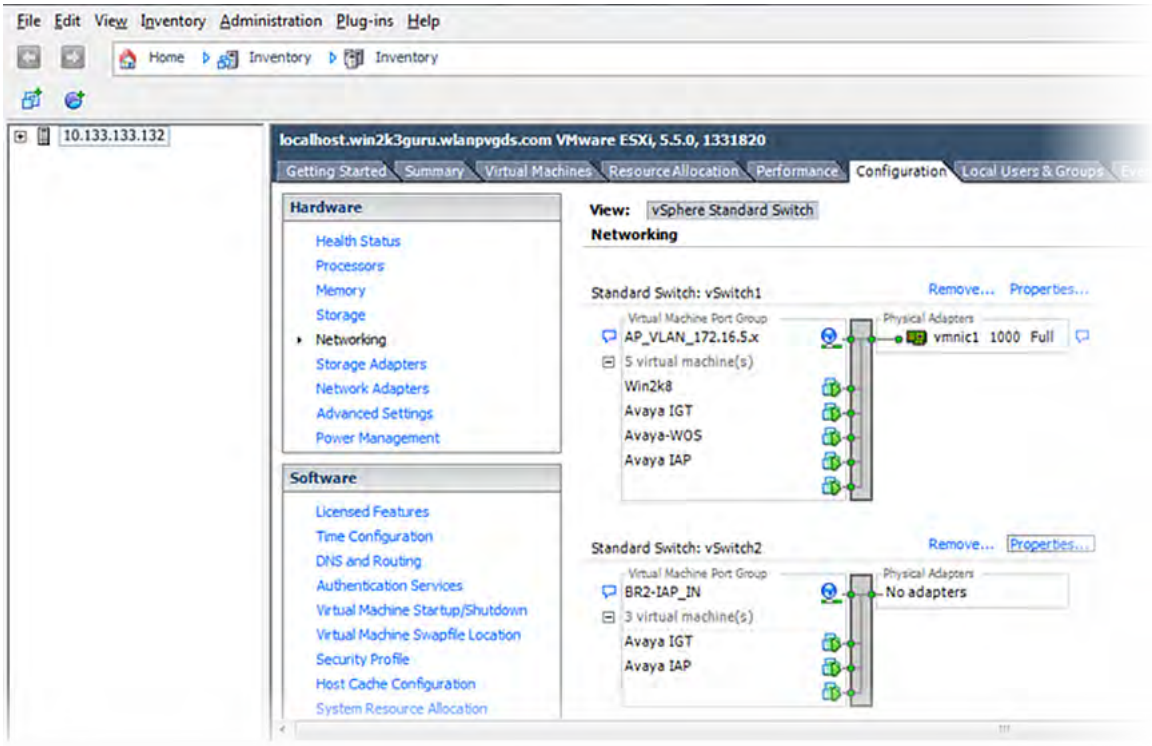
Before you begin

Install the Ignition Guest Tunneling appliance. For more information, see Installing IGT on page 15.

Procedure

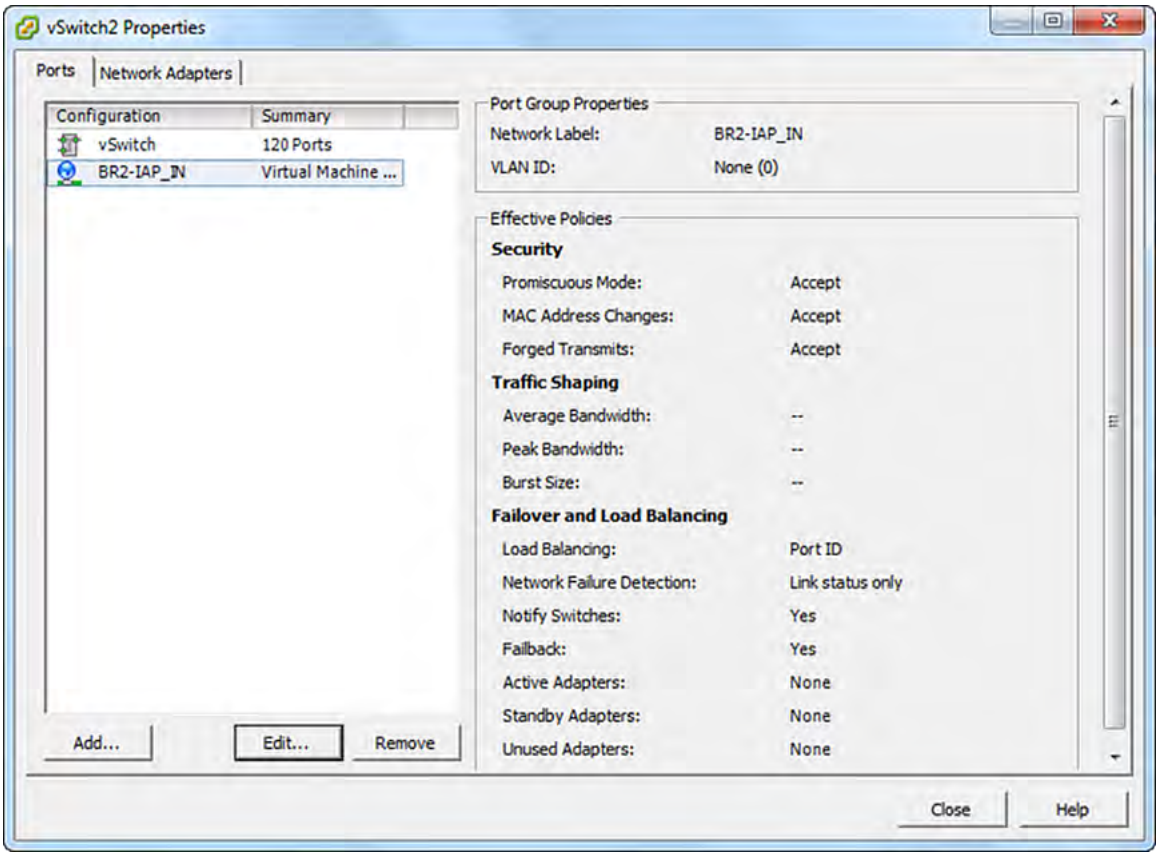
1. Navigate to **Configuration** tab in **vSphere Client**.
2. Click **Networking** in the **Hardware** section.

   The vSphere Standard Switch Structure displays.



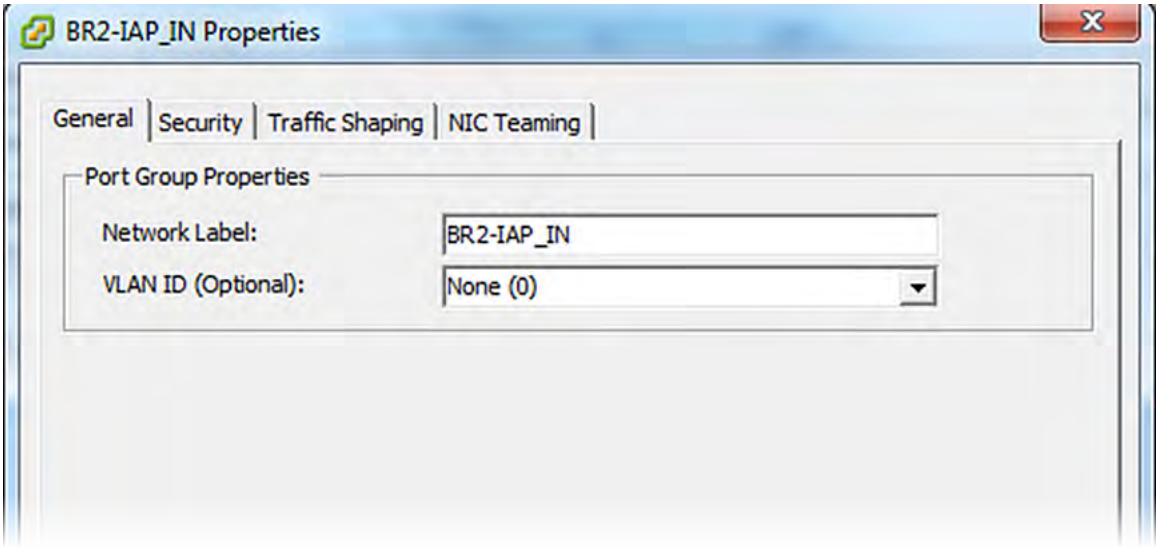
3. Create a virtual machine port group for the vSwitch to which the **IN** interface of the IGT appliance is mapped.
4. Click **Properties**.

5. Select the network interface mapped to the vSwitch and click **Edit**.



The interface properties window displays.

6. Enter the VLAN ID of the Tunneling VLAN and click **OK**.



After the virtual machine port group is created, the network interface assigned to the VM instance expects the tagged VLAN traffic with the VLAN ID to be same as the tunneling VLAN present on the AP.

Configuring VLANs on WLAN 9100

About this task

Configure client VLANs on AP 9100.

Procedure

1. In a supported browser, enter the IP address of the AP (https://<*AP IP Address*>).
2. Enter the **Username** and **Password**. The default **Username** and **Password** is `admin`.
3. Go to **Configuration** > **VLANs** > **VLAN Management**.
4. Enter the **New VLAN Name** and **Number**.
5. Click **Create**.

   Create two VLANs, one for client traffic and another for tunneling.
6. **(Optional)** Add an interface IP in case a static IP address is being assigned.
7. **(Optional)** Select the **DHCP** check box, in case an external DHCP server is configured to grant an IP for these VLANs.
8. **(Optional)** Select the **Management** check box to enable Management, in case management traffic needs to flow on these VLANs.
9. Create a new SSID and enable it. For more information, see Configuring SSID on Avaya WLAN 9100 WMI on page 30.

   Assign the created guest VLAN to the SSID that is being used for guests to connect.
10. Select the VLAN to the SSID from **VLAN ID / Number** drop-down list, in the **SSID Management** page.
11. Create a GRE tunnel to associate with the SSID you created. For more information, see Configuring GRE tunnel on Avaya WLAN 9100 WMI on page 30.

    Note:

    When you create a GRE tunnel on the AP, ensure that the tunnel's local end point IP address is same as the Tunnel VLAN that is created.
12. Click **Save** icon on the right-top corner.

Configuring Tunnel VLANs on WLAN 9100

About this task

Configure tunnel VLAN on AP 9100.

Procedure

1. Create GRE tunnel. For more information, see Configuring GRE tunnel on Avaya WLAN 9100 WMI on page 30.
2. Go to **Configuration** > **VLANs** > **VLAN Management**.
3. Enter **New VLAN Name** and **Number**.
4. Click **Create**.

   The newly created tunnel VLAN list appears.
5. **(Optional)** Add an interface IP in case a static IP address is being assigned.
6. **(Optional)** Select the **DHCP** check box, in case an external DHCP server is configured to grant an IP for these VLANs.
7. **(Optional)** Select the **Management** check box to enable Management, in case management traffic needs to flow on these VLANs.
8. Enter the **IP Address**.

   Ensure that the GRE tunnel's **Local Endpoint** and Tunnel VLAN **IP Address** should be the same.
9. Enter the **Subnet Mask**.
10. Click **Save** icon on the right-top corner.

Configuring VLANs on IGT

About this task

Configure VLAN on IGT using Guest Tunneling Appliance.

Procedure

1. In a supported web browser, enter the IP address of the IGT (https://<*IGT IP Address*>).
2. Enter the **Username** and **Password**. The default **Username** and **Password** is `admin`.
3. Navigate to **VLAN** > **Config** to configure guest tunnel VLAN.

   The **Guest VLAN Untagging Configuration** window displays.
4. Enter the **Guest VLAN ID** and click **Untag VLAN**.
5. Configure the IGT appliance GRE tunnel, to configure GRE tunnel see Adding GRE tunnel on page 32.

Chapter 8: Multiple VLAN Support for IGT GRE Tunneling

In multiple VLAN support scenario, IGT does not untag the multiple VLAN IDs from AP. IGT forwards the packet to OUTBOUND interface with a tag and rely on the adjacent switch to untag the VLAN IDs.

Figure 4: Topology diagram of multiple VLAN support in IGT

Configuring VLAN on ESXi Server for IGT OUT interface

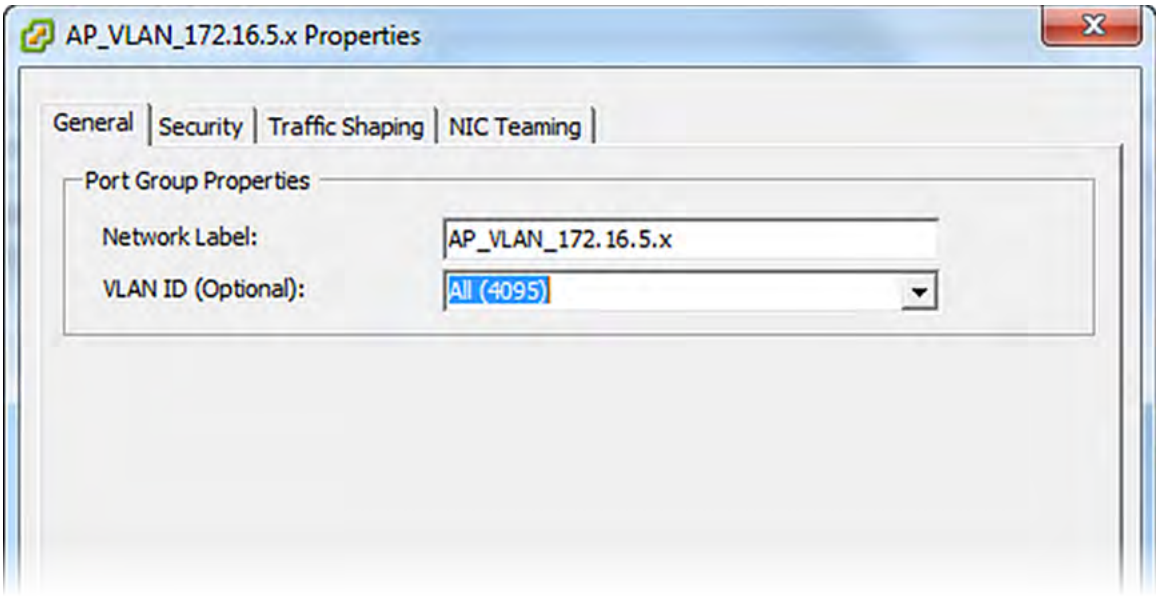
About this task

Configure VLAN on ESXi Server for IGT OUT interface.

Procedure

1. Navigate to **Configuration** tab in **vSphere Client**.
2. Click **Networking** in the **Hardware** section.
3. Create a virtual machine port group for vSwitch that is mapped to the **OUT** interface of IGT appliance.
4. Click **Properties**.
5. Select the network interface mapped to the vSwitch and click **Edit**.

6. Select the **VLAN ID (Optional)** to (All) 4095 from the drop-down list.



Configuring Multiple VLANs on WLAN 9100

About this task

Configure multiple VLANs on AP 9100.

Procedure

1. In a supported web browser, enter the IP address of AP (https://<*AP IP Address*>).
2. Enter the **Username** and **Password**. The default **Username** and **Password** is `admin` and `admin`.
3. Go to **Configuration** > **VLANs** > **VLAN Management**.
4. Create tunneling VLAN, for more information see Configuring Tunnel VLANs on WLAN 9100 on page 42.
5. Create multiple VLANs, create multiple SSIDs and map to respective VLANs and create GRE tunnel and assign to SSID on AP 9100.

   Ensure that the Local Endpoint and Tunnel VLAN IP address is the same.

Configuring Tunnel VLANs on WLAN 9100

About this task

Configure tunnel VLAN on AP 9100.

Procedure

1. Create GRE tunnel. For more information, see Configuring GRE tunnel on Avaya WLAN 9100 WMI on page 30.
2. Go to **Configuration** > **VLANs** > **VLAN Management**.
3. Enter **New VLAN Name** and **Number**.
4. Click **Create**.

   The newly created tunnel VLAN list appears.
5. **(Optional)** Add an interface IP in case a static IP address is being assigned.
6. **(Optional)** Select the **DHCP** check box, in case an external DHCP server is configured to grant an IP for these VLANs.
7. **(Optional)** Select the **Management** check box to enable Management, in case management traffic needs to flow on these VLANs.
8. Enter the **IP Address**.

   Ensure that the GRE tunnel's **Local Endpoint** and Tunnel VLAN **IP Address** should be the same.
9. Enter the **Subnet Mask**.
10. Click **Save** icon on the right-top corner.

Configuring Dynamic Client VLAN assignment through IDE Server

About this task

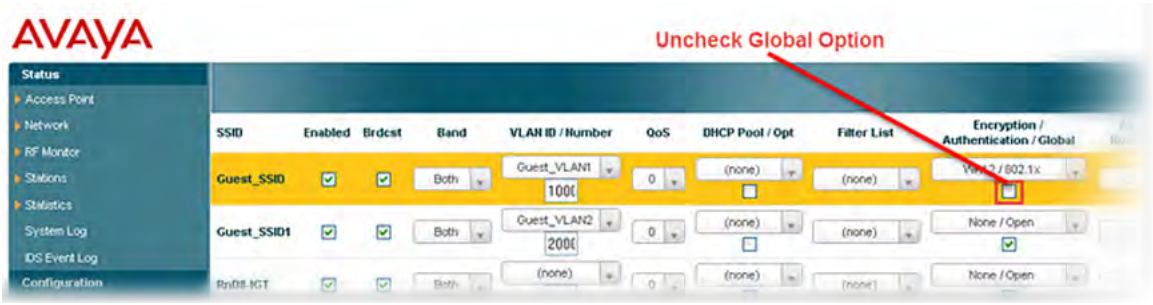
This section describes the procedure to configure Dynamic Client VLAN assignment through IDE Server.

In this scenario AP 9100 is configured with only one SSID. The SSID will have the authentication type as 802.1X with the IDE server configured as the external radius server. After user authenticates, the IDE server maps the user on the specific VLAN and the traffic flows on the GRE tunnel to the IGT appliance.

Procedure

1. Create an SSID on the AP. For more information, see Configuring SSID on Avaya WLAN 9100 WMI on page 30.
2. Select **Encryption / Authentication / Global** type as `WPA2/802.1X`.

3. Uncheck the **Encryption / Authentication / Global** check box.



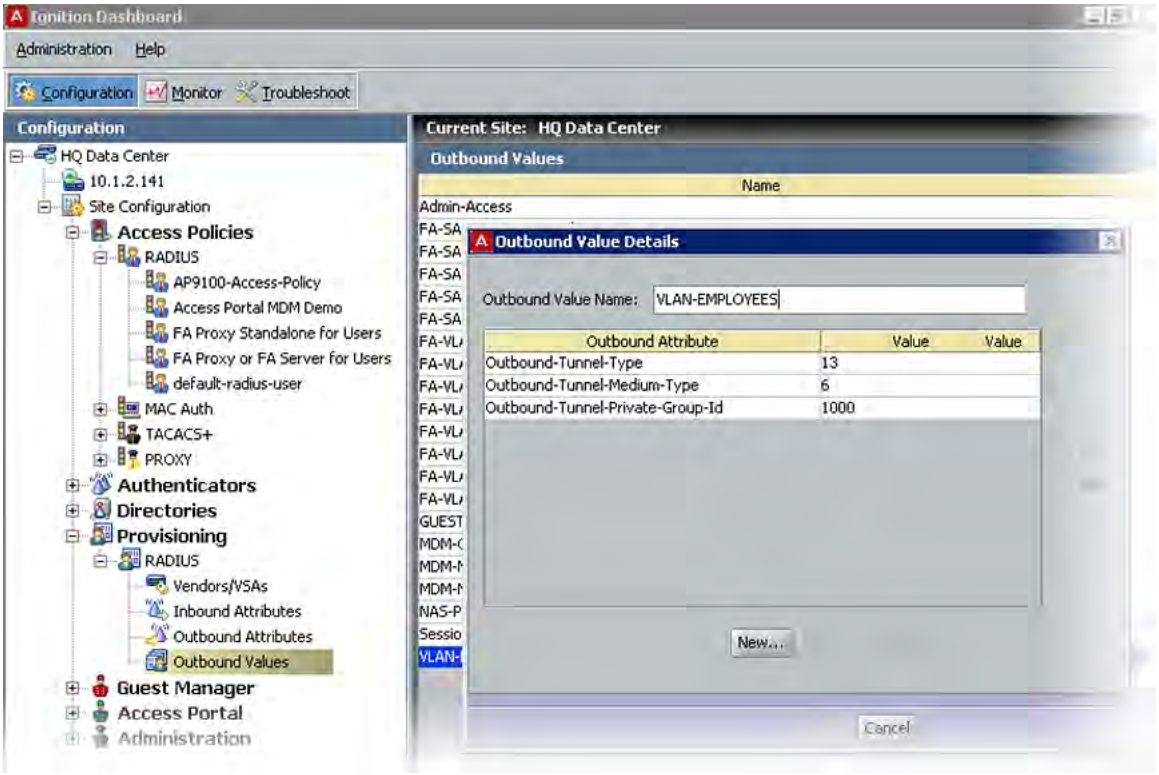
The **Authentication Service Configuration** displays for the SSID.

4. Configure the Ignition Server as the external radius server by entering the **Primary Host / IP Address** and **Shared Secret** for the ports 1812 and 1813.
5. Configure VLAN. For more information, see Configuring VLANs on WLAN 9100 on page 42.

   Note:

   Do not associate any VLAN ID with the SSID.

6. Configure the Ignition server to authenticate user and push a RADIUS outbound attribute with the Guest VLAN ID as shown in the following screenshots. For more information on configuring IDE server, see *Administering Avaya Identity Engines Ignition Server*, NN47280–600.



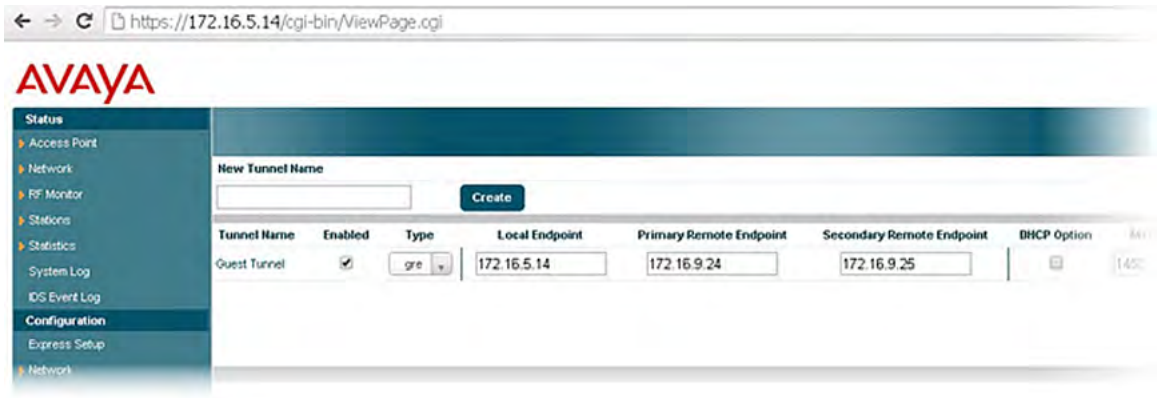
7. To configure multiple VLANs on ESXi Server. For more information, see Configuring VLAN on ESXi Server mapping to IGT IN-interface on page 39.

Chapter 9: IGT High Availability

IGT High Availability is delivered by running two IGT virtual instances, which acts as primary and secondary servers.

The redundancy is achieved through the 9100 AP functionality. AP keeps checking for the availability of the GRE tunnel on primary server. If GRE tunnel on primary server does not respond, the packets are sent to GRE tunnel on secondary server.

Example



Chapter 10: IGT Troubleshooting

This chapter provides answers to common questions and describes what to do if you encounter error while using Avaya Identity Engines Ignition Guest Tunneling.

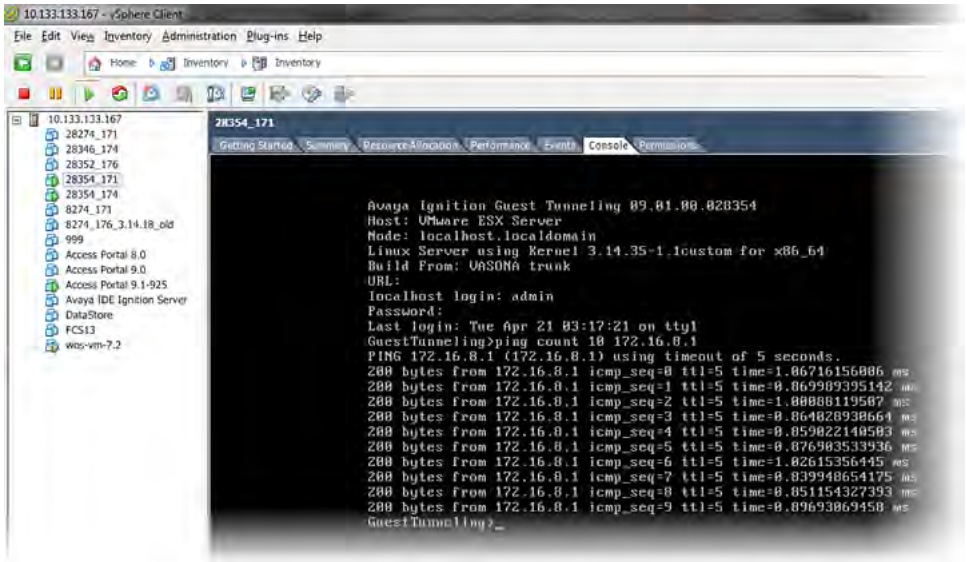
Verifying the connectivity for IGT appliance

Ping functionality can be used to verify the network connectivity for IGT appliance.

`Ping <TTL / Count> <IP Address>`

For example,

1. `ping 20.20.20.1`
2. `ping ttl 10 20.20.20.1`
3. `ping count 10 20.20.20.1`



Tunnel is not responding

- Ensure that SSID to tunnel mapping is correct on the AP.
- Ensure that local IP configured on the AP is same as tunnel remote endpoint configured on the IGT.
- Check the network connectivity.

Issue with wireless client getting an IP address

- Ensure that **Promiscuous** mode is configured as **Accept** on br2 interface.
- Ensure that the configuration of ESXi vSwitch and DHCP server is correct.

Client getting an IP address in the management VLAN

- Ensure that tunnel configuration is correct.
- Ensure that tunnel status is Up.

Debugging issues using tcpdump

Use following procedure to capture packets using tcpdump.

1. Login to IGT console using root or debug user.
2. Capture packets on all interfaces of IGT.

```
tcpdump -texieth0 -w /tmp/eth0.cap &
tcpdump -texibr0 -w /tmp/br0.cap &
tcpdump -texieth1 -w /tmp/eth1.cap &
tcpdump -texibr1 -w /tmp/br1.cap &
tcpdump -texieth2 -w /tmp/eth2.cap &
tcpdump -texibr2 -w /tmp/br2.cap &
```

Stop packet capture

Use the following command to stop all the tcpdump.

```
killall tcpdump
```

Checking CPU and memory status

Use the following commands to check the CPU and memory usage.

```
top -b -n 1
vmstat
ovs-dpctldump-flows -m
ovs-dpctlshow -s
arp
tar czvfopenswitch_log.tgz /var/log/openvswitch/ /var/log/messages
dmesg
```

Collecting running configuration

Use the following commands to collect the OVS configuration and OVS system configurations.

- OVS configuration

  ```
  ovs-vsctlshow
  ovs-vsctlfind Interface
  ```

- OVS system configurations

  ```
  ifconfig -a
  netstat-nr
  uname-a
  tar czvfoperational.tgz /operational/
  tar tmp_arch.tgz /tmp/
  ```

Packet capture on AP using WOS

Use the following procedure to capture packet on AP using WOS.

1. Go to **Monitoring** > **Access Points** > ***<Access Point>*** and click **Packet Capture**.
2. Select **Capture source** as `Network`.
3. Select **Interface** as `Gig1`.
4. Specify **Capture time** and click **OK**.

Troubleshooting Frequently Asked Questions

The following section answers the frequently asked questions to troubleshoot the common issues.

Q1: **Bridges are not created by default (`show interface` does not show any bridges created)**.

A1:

1. Restart IGT VM.
2. If restarting IGT VM does not show bridges, then redeploy the IGT.

Q2: **Unable to ping IGT br0 interface from management network hosts**.

A2:

1. Add specific route in IGT to reach the management network.
2. Check network configuration.
3. Verify ESXi vSwitch configuration has a vNIC assigned to the br0 interface.

Q3: **Unable to access IGT Web UI**.

A3:

1. Add specific route in IGT to reach management network.
2. Check network configuration.
3. Verify ESXi vSwitch configuration has a vNIC assigned to the br0 interface.

Q4: **Unable to reach Access Point IP address**.

A4:

1. Verify network configuration to ensure br1 IP address has a route to reach the subnet of the Access Point IP address.
2. Verify 9100 AP configuration.

Q5: **Tunnel Tx or Rx packet stats are not incrementing**.

A5: Verify remote tunnel endpoint IP address in AP9100 is set to the br1 address of IGT.