Configuring Avaya Identity Engines Ignition Guest Tunneling

Release 9.3
NN47280-504
Issue 03
April 2017

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 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. 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 or on the express behalf of 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 an Avaya 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 ONLY IF YOU PURCHASE AN AVAYA 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.

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 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 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

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 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, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

The *Configuring Avaya Identity Engines Ignition Guest Tunneling* guide 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

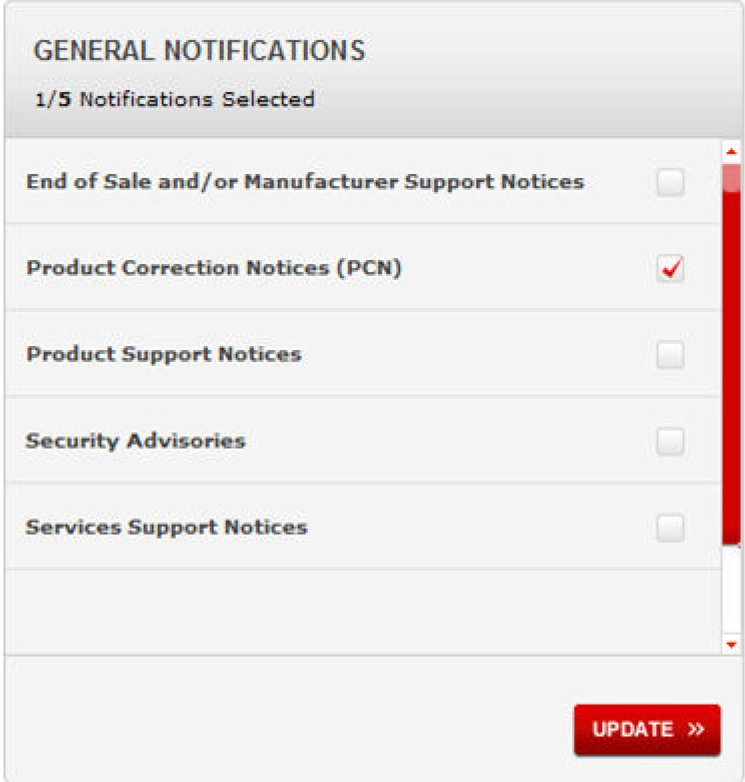
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

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 Ethernet Routing Switch 5000 Series.

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**.



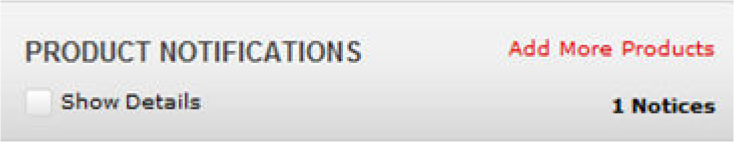
GENERAL NOTIFICATIONS

1/5 Notifications Selected

- End of Sale and/or Manufacturer Support Notices □
- Product Correction Notices (PCN) ☑
- Product Support Notices □
- Security Advisories □
- Services Support Notices □

UPDATE »

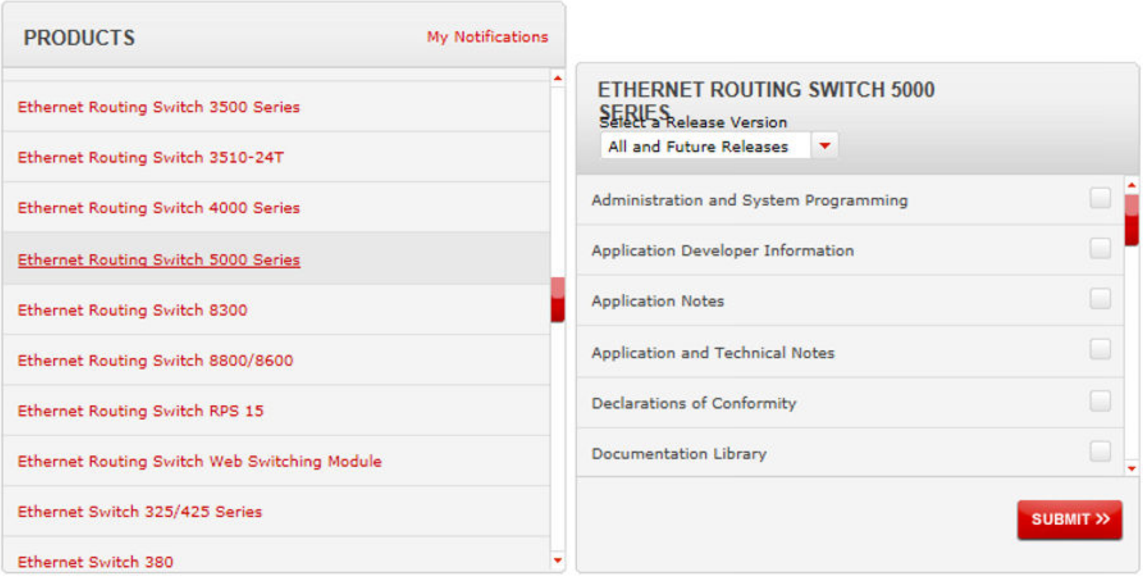
6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.



PRODUCT NOTIFICATIONS Add More Products

□ Show Details 1 Notices

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.



PRODUCTS
My Notifications
Ethernet Routing Switch 3500 Series
Ethernet Routing Switch 3510-24T
Ethernet Routing Switch 4000 Series
Ethernet Routing Switch 5000 Series
Ethernet Routing Switch 8300
Ethernet Routing Switch 8800/8600
Ethernet Routing Switch RPS 15
Ethernet Routing Switch Web Switching Module
Ethernet Switch 325/425 Series
Ethernet Switch 380
ETHERNET ROUTING SWITCH 5000 SERIES
Select a Release Version
All and Future Releases
Administration and System Programming
Application Developer Information
Application Notes
Application and Technical Notes
Declarations of Conformity
Documentation Library
SUBMIT »

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*, NN47280–504 for Release 9.3.

Features

This section describes features introduced in the current release.

Tunnel Grouping

Release 9.3 introduced Tunnel Grouping feature which allows an Administrator to group set of tunnels and perform operations over group such as enable, disable and delete. For more information, see Tunnel Grouping on page 41.

Static VLAN

Release 9.3 introduced configuring Static VLAN feature which helps an administrator to statically configure VLAN(s) on a tunnel on the system to allow the traffic related to the configured VLAN(s) to pass through the tunnel. For more information, see Configuring Static VLANs on page 85

Troubleshoot Enhancements

Release 9.3 introduced Trouble Ticket and Packet Capture mechanism to identify any problem in the IGT system for easy troubleshooting by Avaya Support Engineer. Perform this procedure to collect logs and data, and to capture packets. For more information, see Troubleshooting Guest Tunneling Appliance on page 71.

License

Release 9.3 introduced Licensing mechanism for Avaya Identity Engines Ignition Guest Tunneling application. It supports the Keycode Retrieval System (KRS) based licensing model. For more information, see Licensing Overview on page 57

Certificates

Release 9.3 introduced Certificates feature which allows a user to import and use custom certificate for secure (https) web management connection to Ignition Guest Tunneling application. For more information, see Certificate Management on page 62

Syslog

Release 9.3 introduced Syslog feature which allows an administrator to configure IGT to log system messages to external syslog servers. For more information, see Syslog on page 63

Display Tunnel Status Enhancements

Release 9.3 introduced new display tunnel status enhancements like filters on remote end IP address and Tunnel status. For more information, see Display Guest Tunneling Status on page 37.

Guest Tunneling System Summary and Status

Release 9.3 introduces a new summary page on the Web interface to view the IGT system configuration and status. This includes information about the system version, uptime, interface configuration, status details, DNS server settings, and static route configurations. The system status window shows detail about server processes, active admin sessions, and system resource summary. For more information, see Viewing Guest Tunneling System Summary and Status on page 69.

Reboot option using Web UI

Release 9.3 allows you to perform system restart using the Web UI. Reboot option will restart IGT VM. For more information, see Rebooting Guest Tunneling Appliance on page 78.

IGT System Configuration

Release 9.3 introduces a new System Configuration option to restrict the Web and Secure Shell (SSH) access. The option allows you to restrict the Web and Secure Shell (SSH) access only on the management interface. For more information, see Configuring Guest Tunneling Appliance on page 67.

Loop Prevention

GRE ingress packets are blocked on the OUT (br2) interface to prevent possible loops.

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:

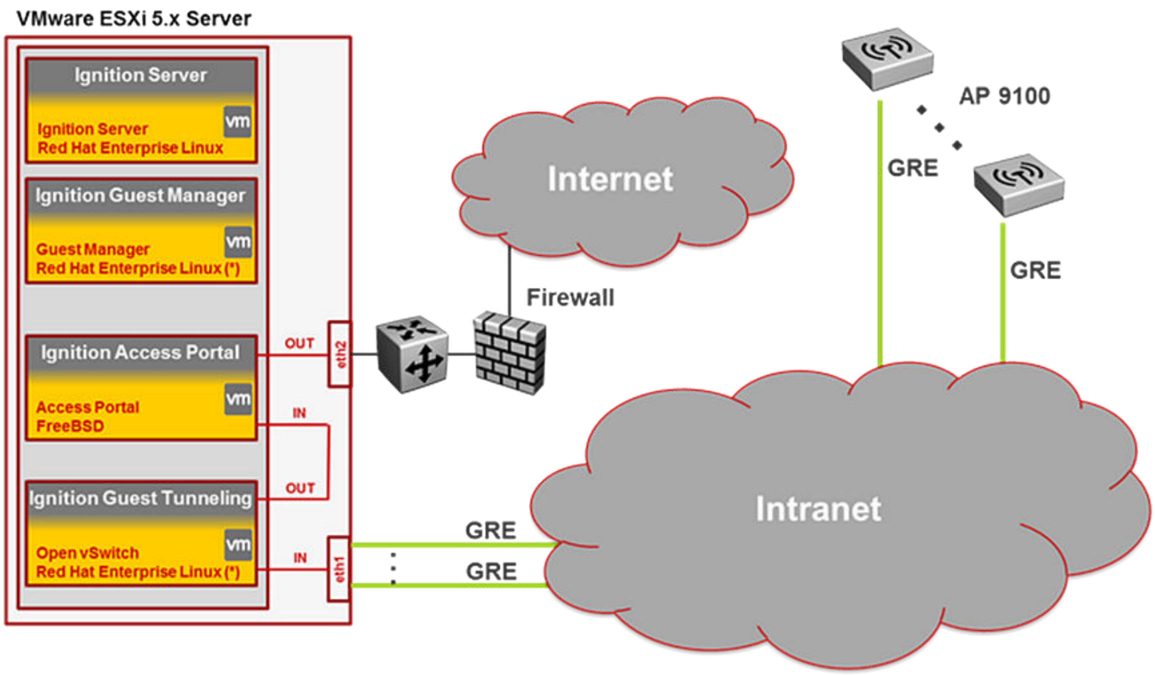
- Mapping SSID and VLAN
- Tunneling to IGT through the SSID and GRE tunneling

Use case examples

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

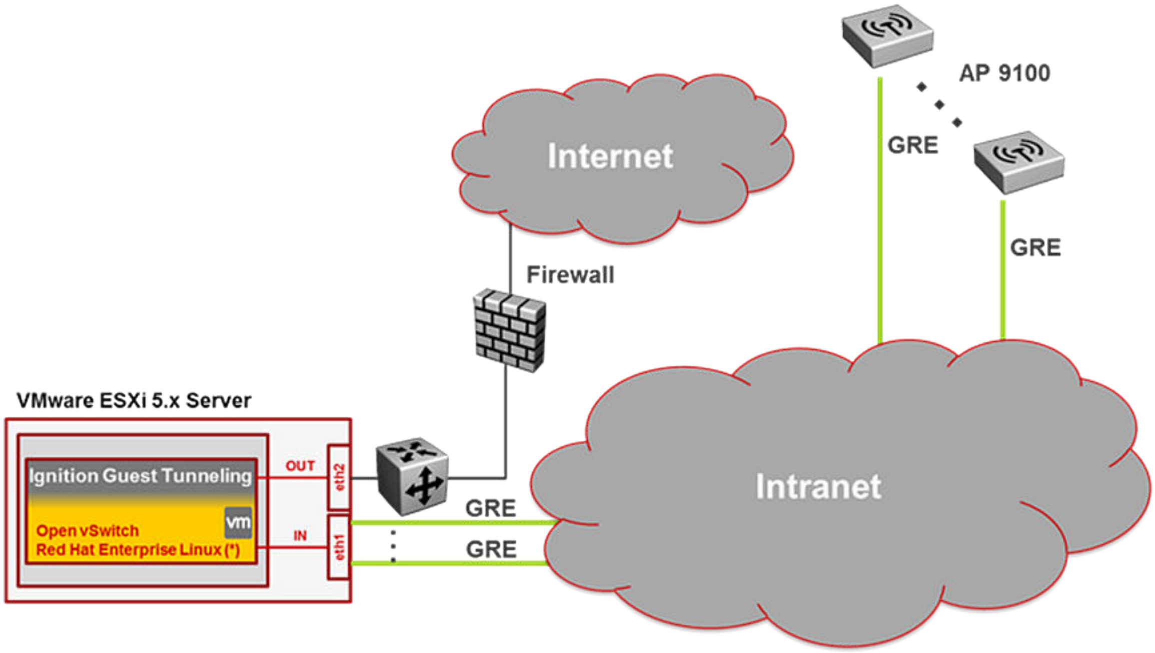
GRE-based traffic isolation for Ignition Captive Portal based authentication

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 is configured to send tagged client traffic, 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, 5.5 and 6.0 • 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.

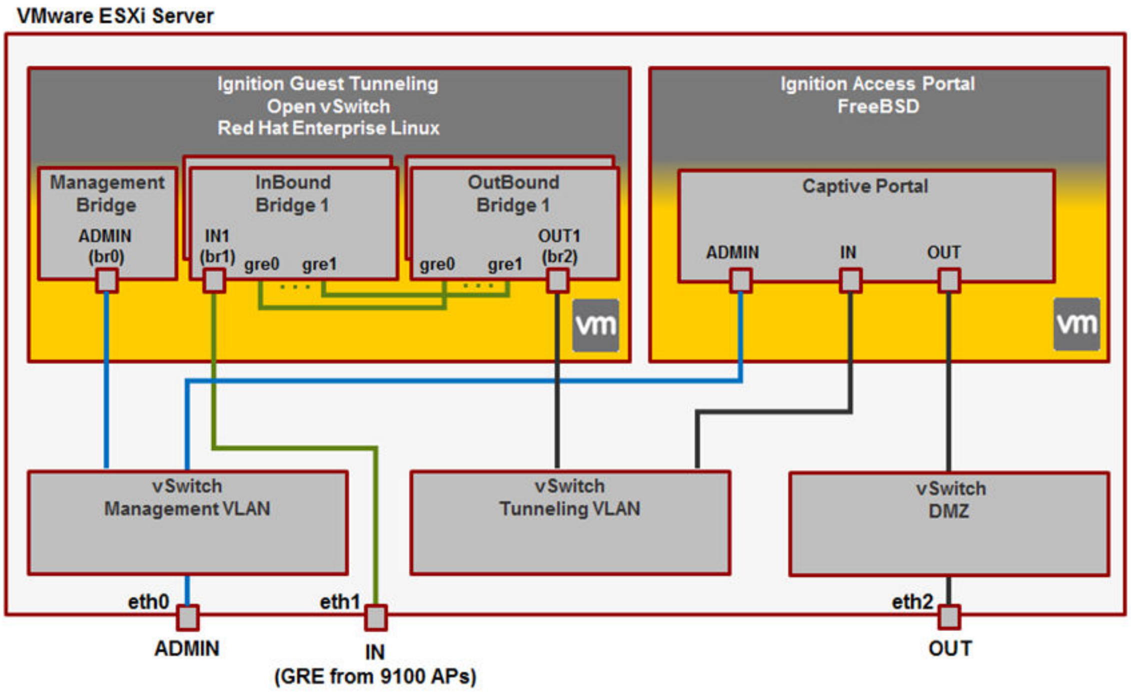


Figure 1: IGT Architecture

IGT interface shall be configured as shown below.

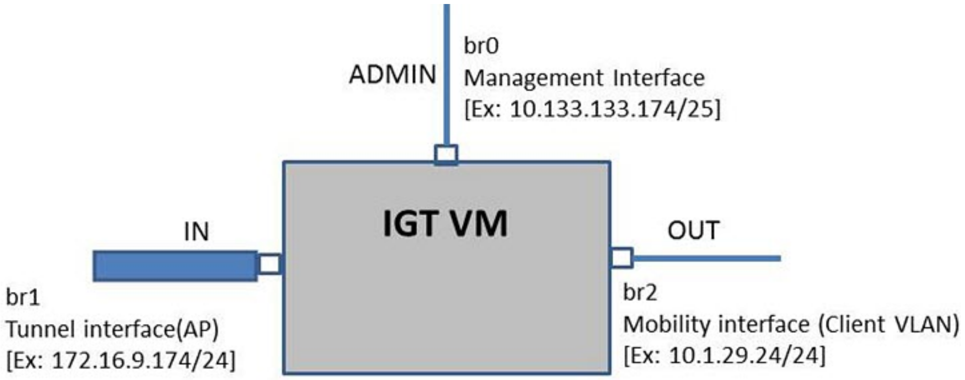


Figure 2: IGT interfaces configuration

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

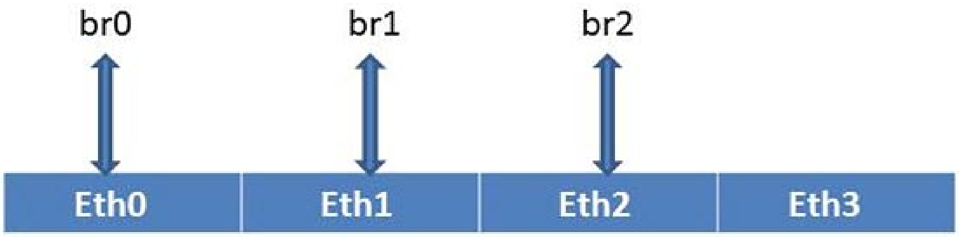


Figure 3: IGT interface mapping

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.

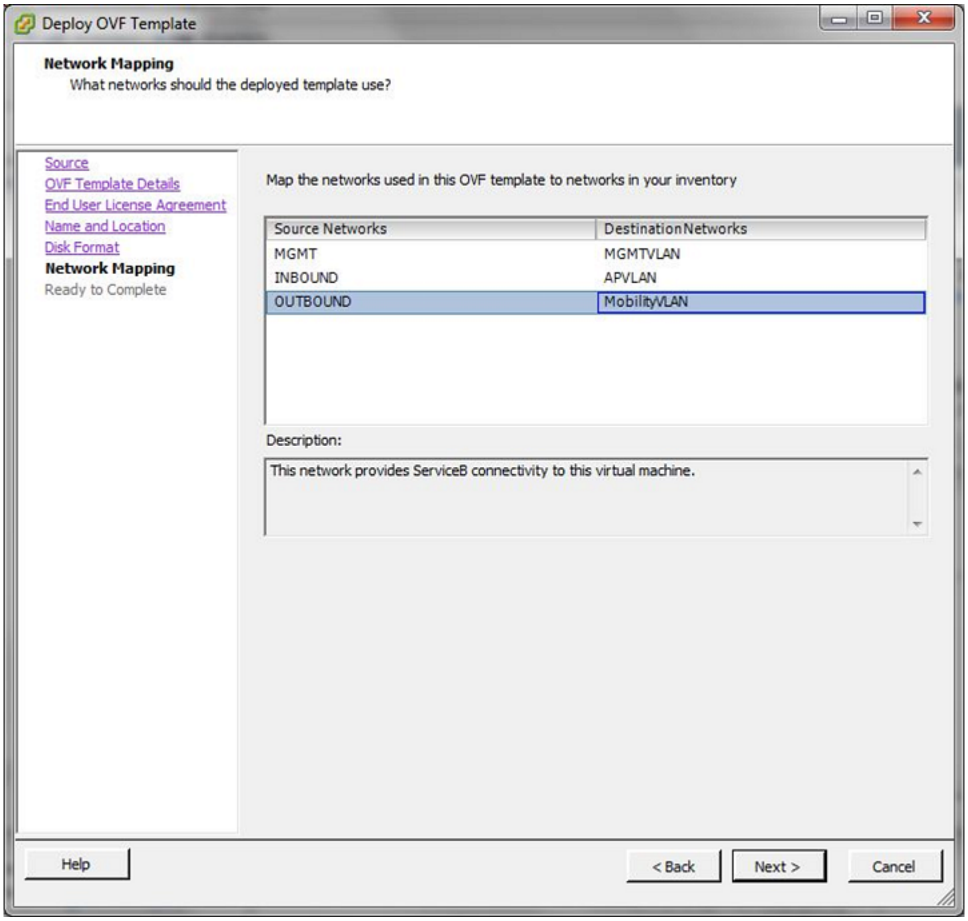
Procedure

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.



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	DestinationNetworks
MGMT	MGMTVLAN
INBOUND	APVLAN
OUTBOUND	MobilityVLAN

Description:

This network provides ServiceB connectivity to this virtual machine.

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

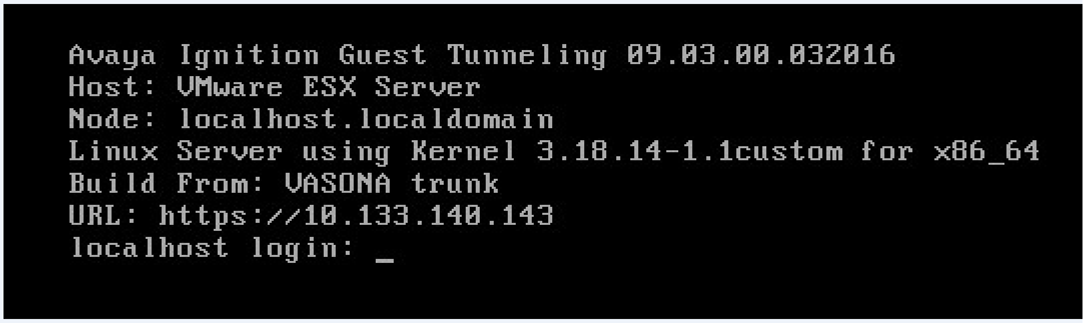
About this task

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**.



```
Avaya Ignition Guest Tunneling 09.03.00.032016
Host: VMware ESX Server
Node: localhost.localdomain
Linux Server using Kernel 3.18.14-1.1custom for x86_64
Build From: VASONA trunk
URL: https://10.133.140.143
localhost login: _
```

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:

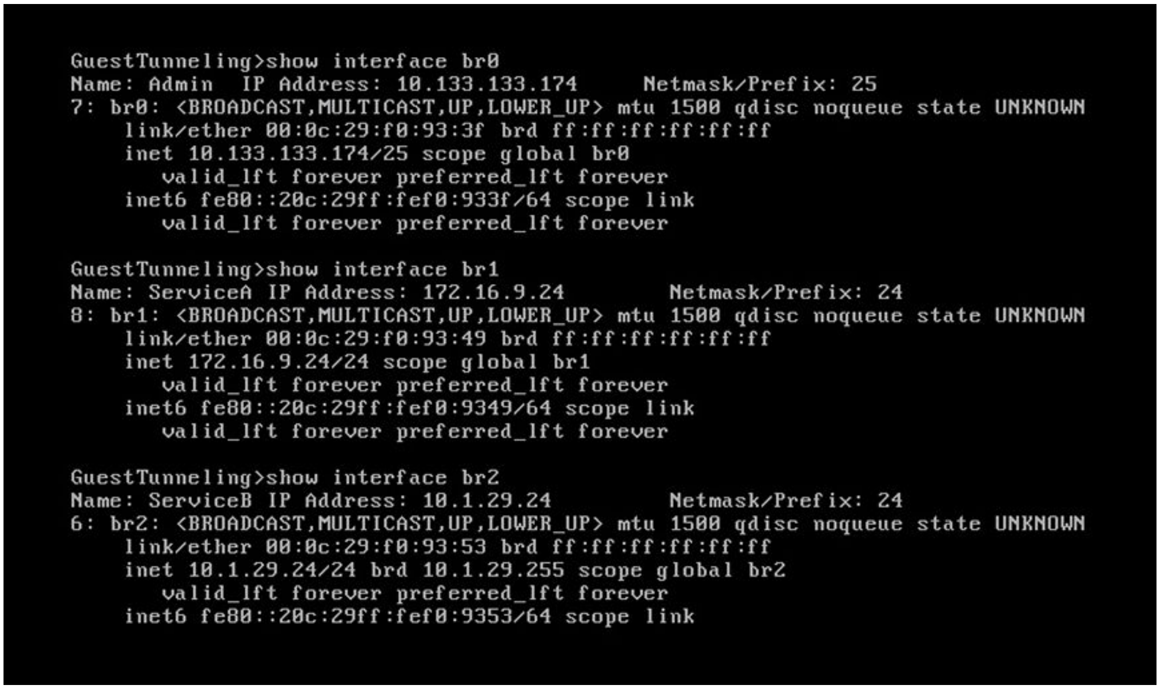
   - Setting a default route to bridge interface is optional. Ensure that the network connectivity with AP is Up.
   - To avoid spillage of user traffic into the management network, IGT has been enhanced to block user traffic from entering the ADMIN interface (br0).
   - Ensure that br0 bridge interface 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.



```
GuestTunneling>show interface br0
Name: Admin  IP Address: 10.133.133.174     Netmask/Prefix: 25
7: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 00:0c:29:f0:93:3f brd ff:ff:ff:ff:ff:ff
    inet 10.133.133.174/25 scope global br0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef0:933f/64 scope link
       valid_lft forever preferred_lft forever

GuestTunneling>show interface br1
Name: ServiceA IP Address: 172.16.9.24        Netmask/Prefix: 24
8: br1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 00:0c:29:f0:93:49 brd ff:ff:ff:ff:ff:ff
    inet 172.16.9.24/24 scope global br1
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef0:9349/64 scope link
       valid_lft forever preferred_lft forever

GuestTunneling>show interface br2
Name: ServiceB IP Address: 10.1.29.24         Netmask/Prefix: 24
6: br2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 00:0c:29:f0:93:53 brd ff:ff:ff:ff:ff:ff
    inet 10.1.29.24/24 brd 10.1.29.255 scope global br2
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef0:9353/64 scope link
```

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 98.

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.

✱ **Note:**

IGT supports WOS version 8.0 and above, and AP OS version 8.0 and above.

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

Configuring NIC teaming support on ESXi server

Before you begin

- Ensure that you have installed IGT Virtual Appliance. For more information, see Installing Guest Tunneling virtual appliance on page 18.
- Click **VMware ESXi** IP address on the left of the **vSphere Client** and navigate to **Configuration** tab.

About this task

Use this procedure for configuring NIC teaming, also known as load balancing and failover (LBFO), on an ESXi server. NIC teaming feature allows multiple network adapters on a vSwitch to be placed into a team for the following purposes:

- Load Balancing
- Traffic failover to prevent connectivity loss in the event of a network component failure

✱ **Note:**

You can perform the following procedure for configuring NIC teaming on both IN and OUT interfaces.

Procedure

1. In the **Hardware** section, click **Networking**.
2. Click **Properties** of the **Standard Switch: vSwitchx**.

   ✱ **Note:**

   By default, vSwitchx is selected.
3. On the **vSwitchx** properties window, click **Network Adapters** tab.

   The system displays list of Network Adapters.
4. Click **Add** and on the Add Adapter Wizard window add more network adapters, click **Next** > **Finish**.

5. On the **vSwitchx** properties window, click **Ports** tab.

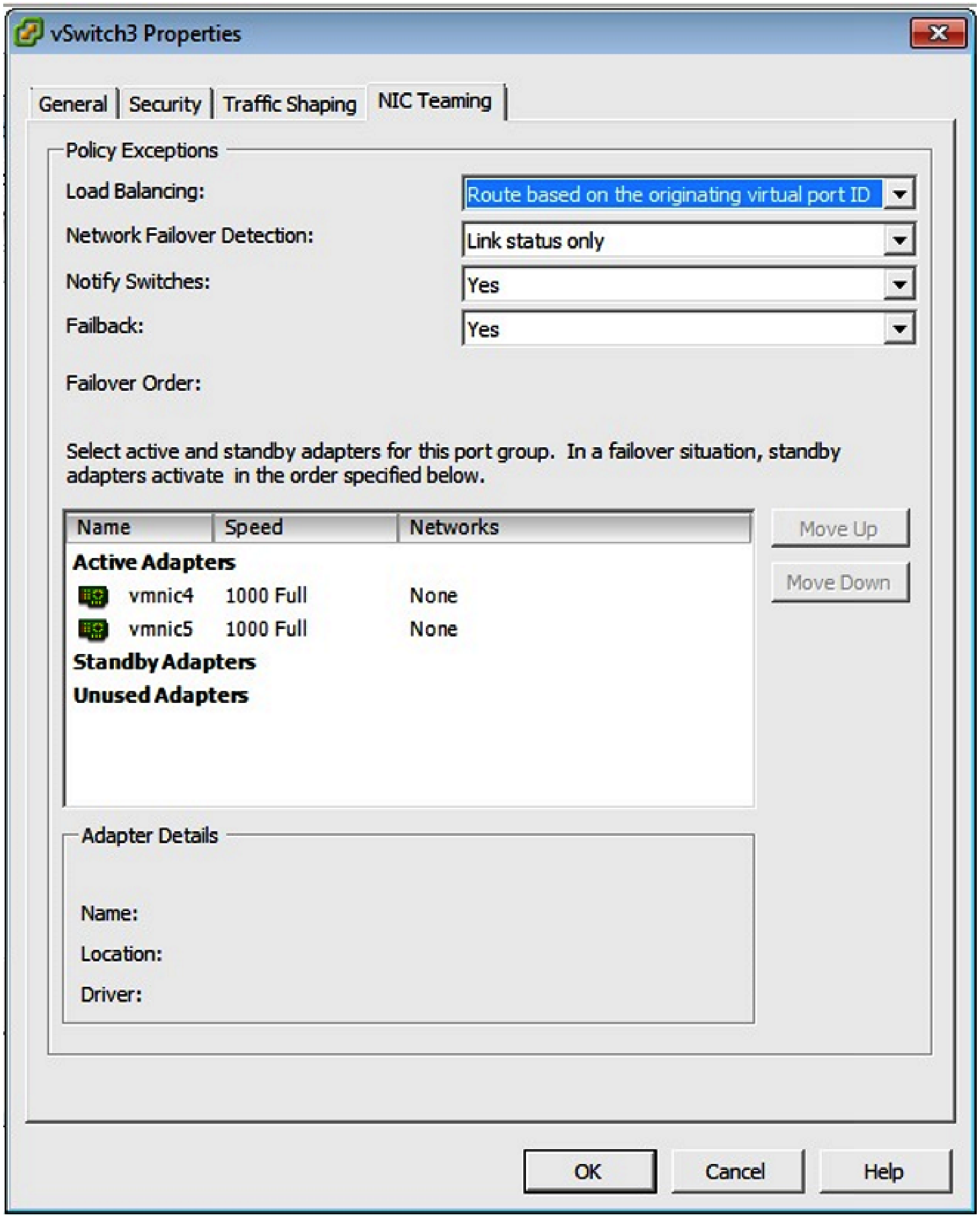
   The system displays ports configuration and summary.

6. On the **Ports** tab, select **vSwitchx** and click **Edit**.

   The system displays vSwitchx Properties window.

7. On the **vSwitchx Properties** window, click **NIC Teaming** tab.

   The system displays configuration options for teaming and failover.



Load Balancing: Route based on the originating virtual port ID

Network Failover Detection: Link status only

Notify Switches: Yes

Failback: Yes

Failover Order:

Select active and standby adapters for this port group. In a failover situation, standby adapters activate in the order specified below.

Name	Speed	Networks
Active Adapters		
vmnic4	1000 Full	None
vmnic5	1000 Full	None
Standby Adapters		
Unused Adapters		

Name:

Location:

Driver:

8. On the **Policy Exceptions** section, select a **Load Balancing** method from the given choices:

Choice Option	Description
Route based on the originating port ID	Choose an uplink based on the virtual port where the traffic entered the virtual switch.
Route based on an IP hash	Choose an uplink based on a hash of the source and destination IP addresses of each packet.
Route based on a source MAC hash	Choose an uplink based on a hash of the source Ethernet.
Use explicit failover order	Choose the highest order uplink from the list of Active adapters which passes failover detection criteria. **Note:** This policy really does not do any sort of load balancing. Instead, the first Active NIC on the list is used. If that one fails, the next Active NIC on the list is used, and so on, until the Standby NICs. Only one of uplink will be actively used at any given time.

Note:

The default load balancing policy is **Route based on the originating virtual port ID**.

9. On the **Policy Exceptions** section, select a **Network Failure Detection** method used by vSwitch to detect network failure from the given choices:

Choice Option	Description
Link status only	When a network link fails, the vSwitch is aware of the failure because the link status reports the link as being down. This can usually be verified by seeing if anyone tripped over the cable or mistakenly unplugged the wrong one.
Beacon probing	A beacon is regularly sent out from the vSwitch through its uplinks to see if the other uplinks can receive it. If vSwitch is expected to determine a failure further up the network, such as a failure beyond upstream connected switch, then beacon probing detection method should be used.

10. On the **Policy Exceptions** section, in the **Notify Switches** field select any one from the given choices:

Choice Option	Description
Yes	Select `Yes` to speed things along by sending Reverse Address Resolution Protocol (RARP) frames to the upstream physical switch on behalf of the VM or VMs so that upstream switch updates its MAC address table.
No	Select `No` to stop sending and receiving notification updates.

11. On the **Policy Exceptions** section, in the **Failback** field select an failback option from the given choices:

Choice Option	Description
Yes	If you set the value to `Yes`, the now-operational NIC will immediately go back to being Active again, and the Standby NIC returns to being Standby. Things are returned back to the way they were before the failure.
No	If you set the value to `No`, the replaced NIC will simply remain inactive until either another NIC fails or you return it to Active status.

12. On the **Policy Exceptions** section, **Failover Order** displays the following three different adapter states:

Option	Description
Active adapters	Adapters that are actively used to pass along traffic.
Standby adapters	Adapters will only become active if the defined active adapters have failed.
Unused adapters	Adapters that will never be used by the vSwitch, even if all the Active and Standby adapters have failed.

13. Click **OK**.

Next steps

Configure MLT on the switch to work with NIC teaming on an ESXi server. For more information, see Sample MLT configuration on a Avaya switch on page 26.

Sample MLT configuration on a Avaya switch

About this task

Use this procedure as a sample to perform an MLT setup on the Avaya switch to work with NIC teaming on an ESXi server.

This example sets up an MLT, MLT 1, named *TEAM1* . It adds port *1/12 and 1/13* as the port members. The **`learning disable`** command turns off spanning tree. Setting load balance option to **`Advanced Mode`** causes the traffic hashing algorithm in the Avaya switch to make load-balancing decisions based on the IP address rather than the MAC address (which is **`Basic Mode`**). It is recommended to set load balancing policy on ESXi to **`Route based on an IP hash`** when MLT load balance policy on physical switch is set to **`Advanced mode`**.

Procedure

1. Connect to Avaya switch console.
2. Configure MLT on the Avaya switch by creating a tagged trunk with 802.1q.

   Sample Input:

```
SWITCH(config)# vlan create 200 name "VLAN200" type port
SWITCH(config)# vlan members add 200 1/12,1/13
SWITCH(config)# vlan ports 1/12,1/13 pvid 200
```

Sample Output:

```
SWITCH(config)# show vlan id 200
Id   Name                 Type     Protocol         PID     Active IVL/SVL Mgmt
---- -------------------- -------- ---------------- ------- ------ ------- ----
200  VLAN200              Port     None             0x0000  Yes    IVL     No
        Port Members: 12-13
Total VLANs: 1
```

3. Create the MLT.

   Sample Input:

```
SWITCH(config)# mlt 1 name “TEAM1"
SWITCH(config)# mlt 1 member 1/12,1/13
SWITCH(config)# mlt 1 learning disable
SWITCH(config)# mlt 1 loadbalance advance
SWITCH(config)# mlt 1 enable
```

   Sample Output:

```
SWITCH(config)# show mlt  1
Id Name             Members                Bpdu   Mode           Status  Type
-- ---------------- ---------------------- ------ -------------- ------- ------
1  TEAM1            12-13                  All    Advance        Enabled Access
```

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 28.

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 33.

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 29.
2. Configuring SSID. For more information, see Configuring SSID using WLAN 9100 Orchestration System on page 29.
3. Configuring GRE tunnel. For more information, see Configuring GRE tunnel on WLAN 9100 Orchestration System on page 30.
4. Associating the GRE tunnel to SSID. For more information, see Associating the GRE tunnel to SSID on page 31.
5. Exporting WLAN Access Point configuration. For more information, see Exporting WLAN Access Points configuration on page 32.

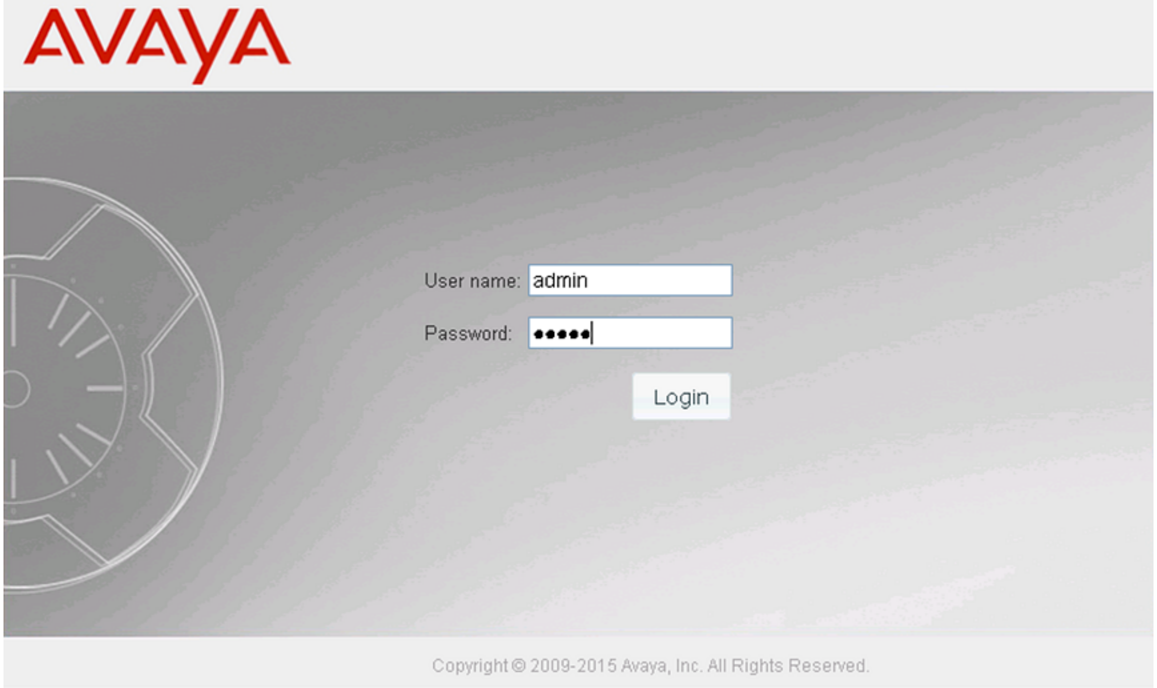
Launching WLAN 9100 Orchestration System

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*>).



User name: admin

Password: •••••

Copyright © 2009-2015 Avaya, Inc. All Rights Reserved.

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

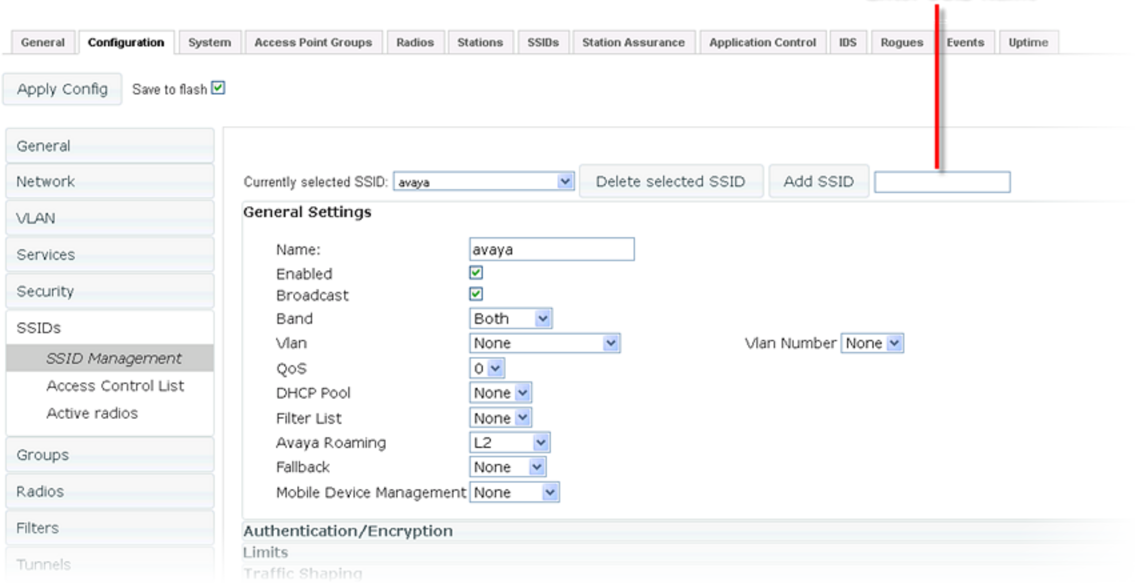
Configure SSID on AP using WLAN 9100 Orchestration System.

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.

Enter SSID Name



Save to flash ☑

Currently selected SSID: avaya

General Settings

Name: avaya
Enabled ☑
Broadcast ☑
Band Both
Vlan None
Vlan Number None
QoS 0
DHCP Pool None
Filter List None
Avaya Roaming L2
Fallback None
Mobile Device Management None

4. Click **Add SSID**.

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

Configuring GRE tunnel on WLAN 9100 Orchestration System

About this task

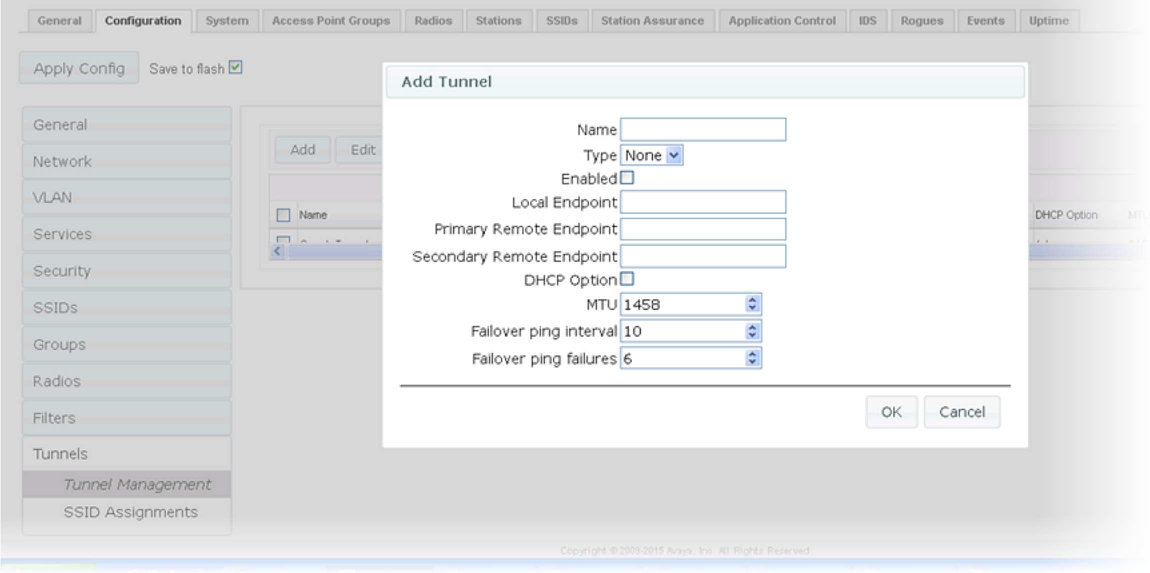
Configure GRE tunnel on AP using WLAN 9100 Orchestration System.

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.



Add Tunnel

Name
Type None
Enabled □
Local Endpoint
Primary Remote Endpoint
Secondary Remote Endpoint
DHCP Option □
MTU 1458
Failover ping interval 10
Failover ping failures 6

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

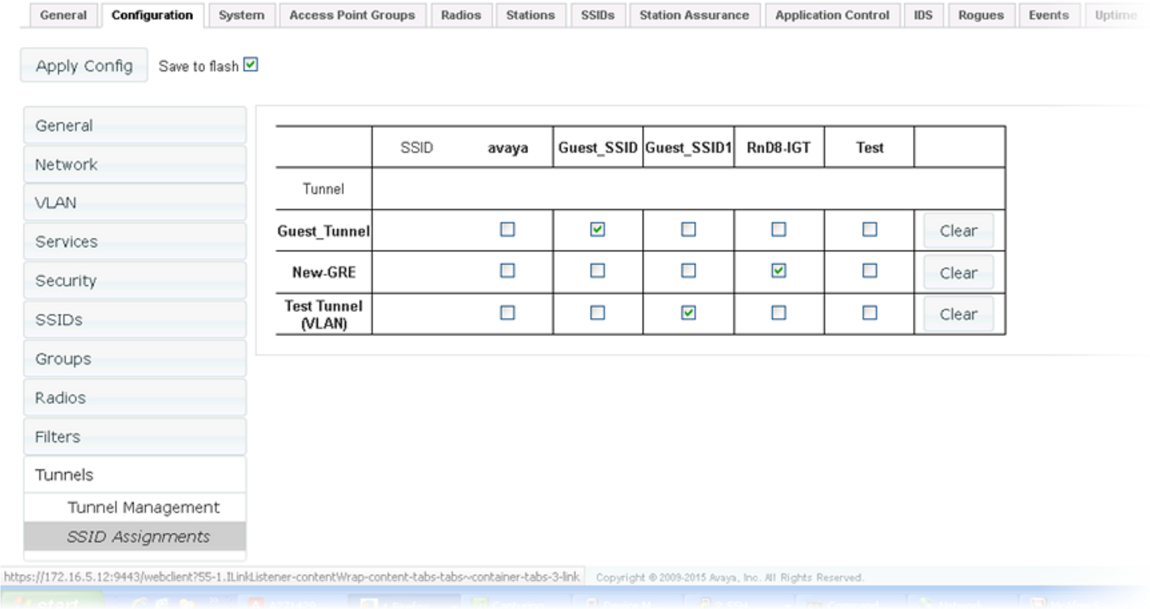
About this task

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.



Save to flash ☑

Tunnel / SSID	avaya	Guest_SSID	Guest_SSID1	RnD8-IGT	Test	
Guest_Tunnel	☐	☑	☐	☐	☐	Clear
New-GRE	☐	☐	☐	☑	☐	Clear
Test Tunnel (VLAN)	☐	☐	☑	☐	☐	Clear

https://172.16.5.12:9443/webclient?55-1.ILinkListener-contentWrap-content-tabs-tabs~container-tabs-3-link Copyright © 2009-2015 Avaya, Inc. All Rights Reserved.

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

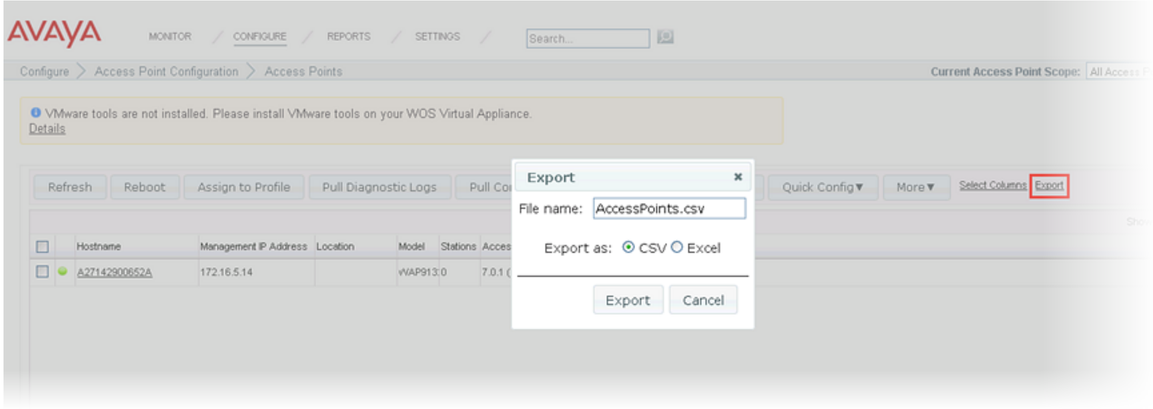
Exporting WLAN Access Points configuration

About this task

Export the Access Points configuration in .csv format.

Procedure

1. Go to **Configure** > **Access Point Configuration** > **Access Points**.
2. Select **Profile Name** column, which is used as tunnel group name.
3. Click **Export link**.



VMware tools are not installed. Please install VMware tools on your WOS Virtual Appliance.
Details

Export

File name: AccessPoints.csv

Export as: ● CSV ○ Excel

☐		Hostname	Management IP Address	Location	Model	Stations	Acces
☐	●	A27142900652A	172.16.5.14		WAP913	0	7.0.1 (

4. Browse and select the .csv file.
5. 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 33.
2. Configuring SSID. For more information, see Configuring SSID on Avaya WLAN 9100 WMI on page 34.
3. Configuring GRE tunnel. For more information, see Configuring GRE tunnel on Avaya WLAN 9100 WMI on page 34.
4. Associating GRE tunnel to SSID. For more information, see Associating the GRE tunnel to SSID on page 35.

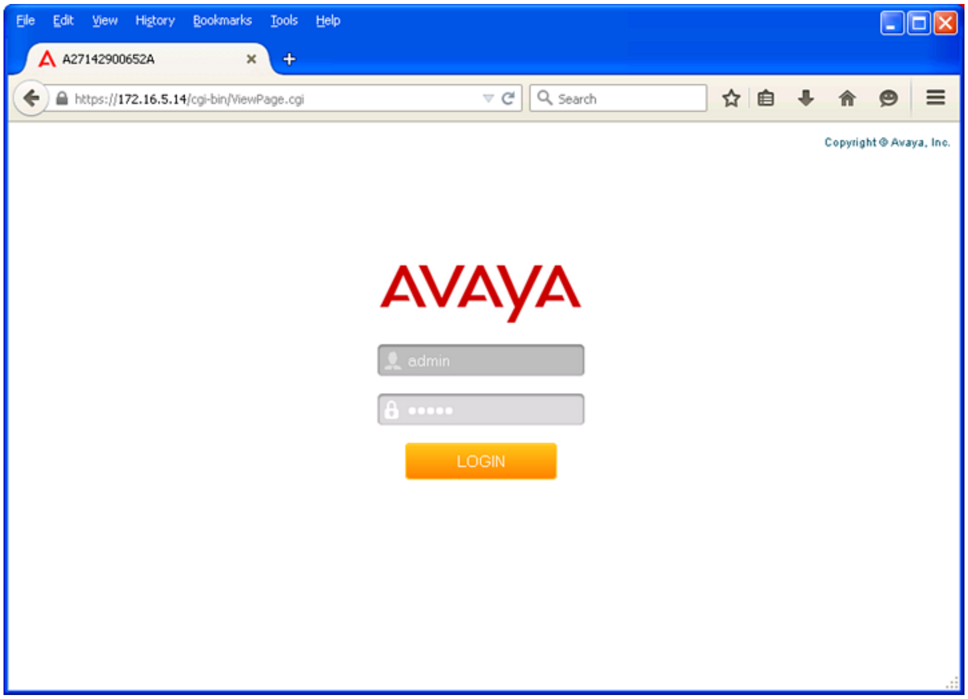
Launching WLAN 9100 Web Management Interface

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

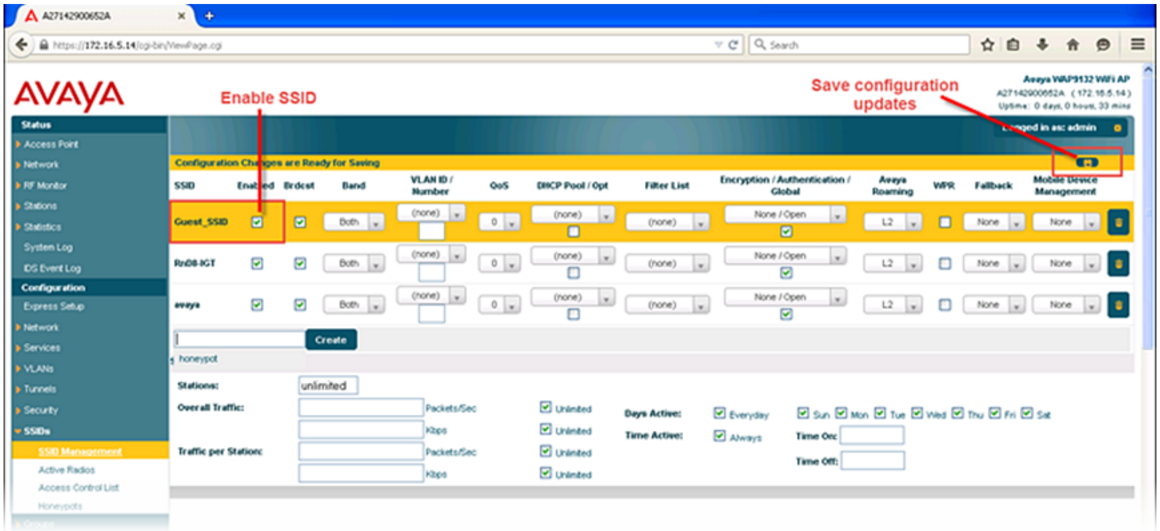
Configure SSID on AP using Avaya WLAN 9100 Web Management Interface.

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**.



Enable SSID

Save configuration updates

Avaya WAP9132 WiFi AP
A27142900652A (172.16.5.14)
Uptime: 0 days, 0 hours, 33 mins

Logged in as: admin

Configuration Changes are Ready for Saving

SSID	Enabled	Brdcst	Band	VLAN ID / Number	QoS	DHCP Pool / Opt	Filter List	Encryption / Authentication / Global	Avaya Roaming	WPR	Fallback	Mobile Device Management
Guest_SSID	☑	☑	Both	(none)	0	(none) ☐	(none)	None / Open ☑	L2	☐	None	None
RnD8-IGT	☑	☑	Both	(none)	0	(none) ☐	(none)	None / Open ☑	L2	☐	None	None
avaya	☑	☑	Both	(none)	0	(none) ☐	(none)	None / Open ☑	L2	☐	None	None

Create

honeypot

Stations: unlimited

Overall Traffic: Packets/Sec ☑ Unlimited; Kbps ☑ Unlimited

Traffic per Station: Packets/Sec ☑ Unlimited; Kbps ☑ Unlimited

Days Active: ☑ Everyday ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time Active: ☑ Always Time On: Time Off:

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.

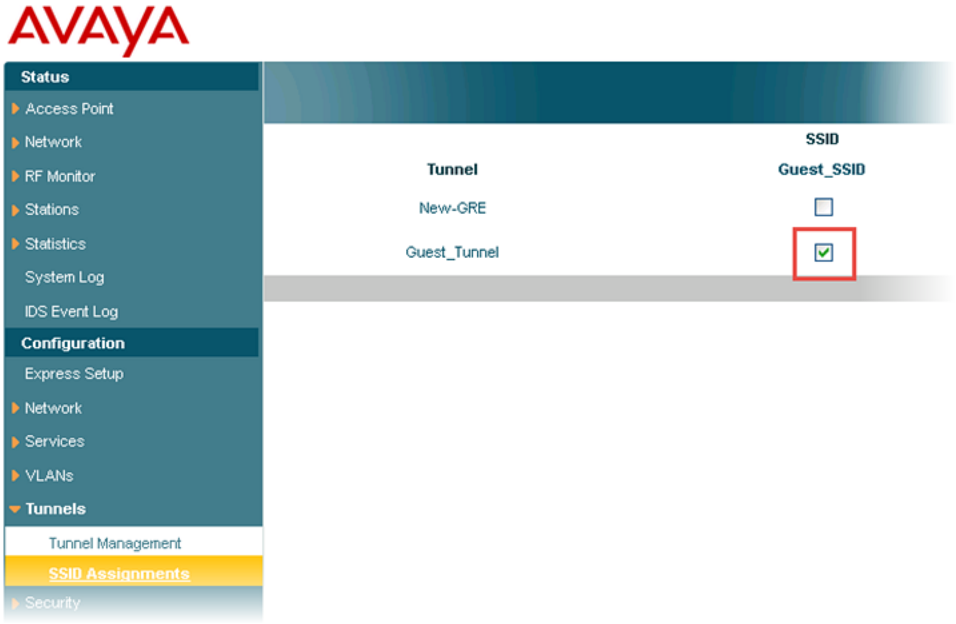
Associating the GRE tunnel to SSID

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.



	SSID
Tunnel	Guest_SSID
New-GRE	□
Guest_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, .zip and .tar file, add, display or delete the GRE Tunnel in the IGT appliance. For more information, see IGT Web User Interface on page 36.
2. Configuring the IGT GRE tunnel VLAN to untag the VLAN traffic. For more information, see IGT Web User Interface on page 36.

IGT Web User Interface

Launch IGT Web User Interface to import, export the GRE Tunnel configuration .csv, .zip 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 36.
- Display GRE Tunnel Status. For more information, see Displaying Guest Tunneling Status on page 37.
- Import GRE Tunnel. For more information, see Importing GRE tunnel on page 39.
- Export GRE Tunnel. For more information, see Exporting GRE Tunnel on page 40.

Adding GRE tunnel

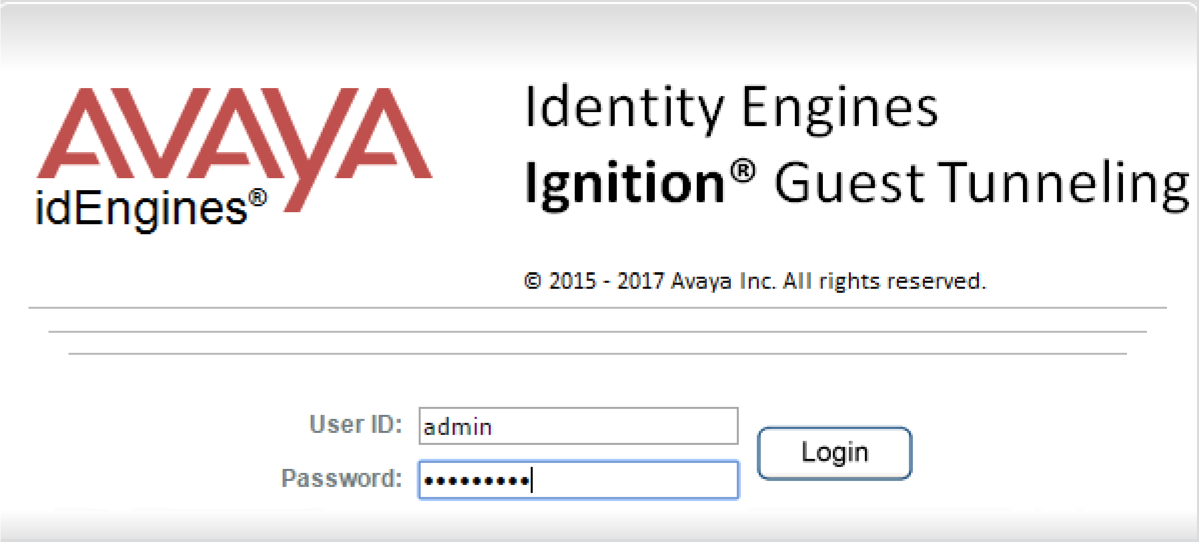
About this task

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`.



AVAYA
idEngines®
Identity Engines
Ignition® Guest Tunneling
© 2015 - 2017 Avaya Inc. All rights reserved.
User ID:
Password:
Login

User ID: admin

Password: ••••••••••

3. On how to change first login/password, refer to Changing the password on page 51. For installing License, refer to Installing Avaya Ignition Guest Tunneling License on page 58
4. In the **Tunnel** menu, click **Add** to add new GRE tunnel.
5. Enter the tunnel remote endpoint.
6. 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

Before you begin

- Login to IGT web interface using the **User ID** and **Password**.

About this task

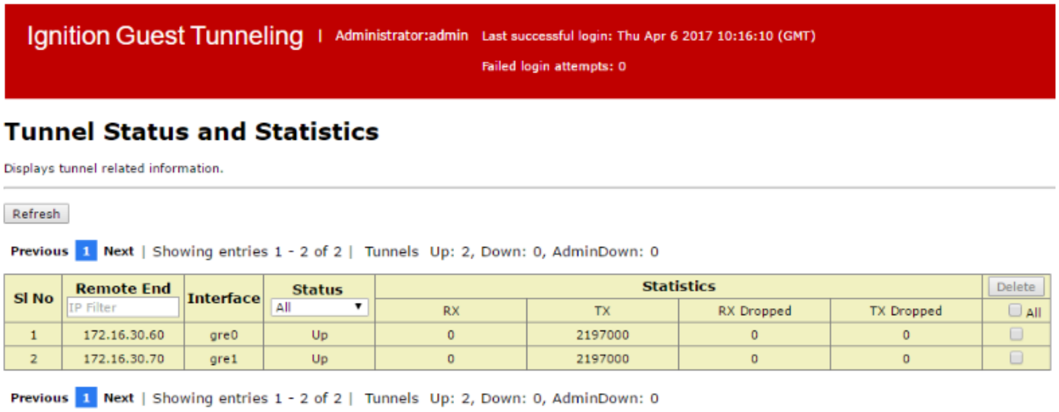
Use this procedure to display the status and statistics of tunnels configured in the IGT system.

Note:

The system displays the **status** as `Up` , `Down` and `AdminDown` for reachable, not reachable and administratively disabled tunnel remote end points.

Procedure

1. From the navigation panel, go to **Tunnel** > **Status** to display the status and statistics of tunnels.



Ignition Guest Tunneling | Administrator:admin Last successful login: Thu Apr 6 2017 10:16:10 (GMT)
Failed login attempts: 0

Tunnel Status and Statistics

Displays tunnel related information.

Previous 1 Next | Showing entries 1 - 2 of 2 | Tunnels Up: 2, Down: 0, AdminDown: 0

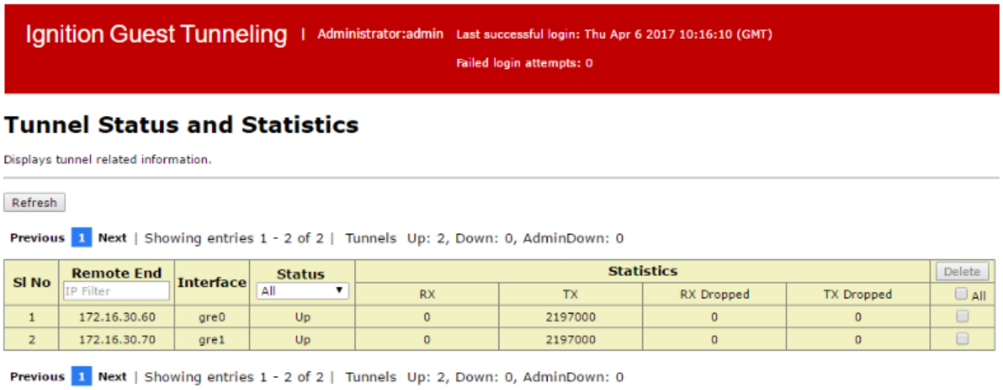
Sl No	Remote End	Interface	Status	Statistics				Delete
	IP Filter		All ▾	RX	TX	RX Dropped	TX Dropped	□ All
1	172.16.30.60	gre0	Up	0	2197000	0	0	□
2	172.16.30.70	gre1	Up	0	2197000	0	0	□

Previous 1 Next | Showing entries 1 - 2 of 2 | Tunnels Up: 2, Down: 0, AdminDown: 0

Field	Description
Remote End	Tunnel Remote endpoint IP address (usually Access point).
Interface	Tunnel interface name.
Status	Tunnel status. Down, Up or AdminDown.
RX	Number of packets received on this tunnel.
TX	Number of packets send from this tunnel.
RX Dropped	Number of packets dropped on receiving.
TX Dropped	Number of packets dropped on sending.

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.
4. **(Optional)** Admin can easily search for a particular IP or set of IPs using expressions. The IP filters supported are listed below, where x is a wild card character.
    - x.50.50.50 ---> 1.50.50.50 to 255.50.50.50
    - 50.x.x.x ---> 50.1.1.1 to 50.255.255.255
    - 50.50.x.x ---> 50.50.1.1 to 50.50.255.255
    - 50.50.50.x ---> 50.50.50.1 to 50.50.50.255
    - 50.x.50.50 ---> 50.1.50.50 to 50.255.50.50
    - 50.x.x.50 ---> 50.1.1.50 to 50.255.255.50
    - 50.50.x.50 ----> 50.50.1.50 to 50.50.255.50
    - x.x.x.50
    - x.x.50.50
    - 50.x
    - x.50
    - 50.x.50

5. **(Optional)** Admin can filter the list of Tunnels based on Tunnel status by selecting required status option (**All**, **Up**, **Down** or **AdminDown**) from the drop down list.



Ignition Guest Tunneling | Administrator:admin Last successful login: Thu Apr 6 2017 10:16:10 (GMT)
Failed login attempts: 0

Tunnel Status and Statistics

Displays tunnel related information.

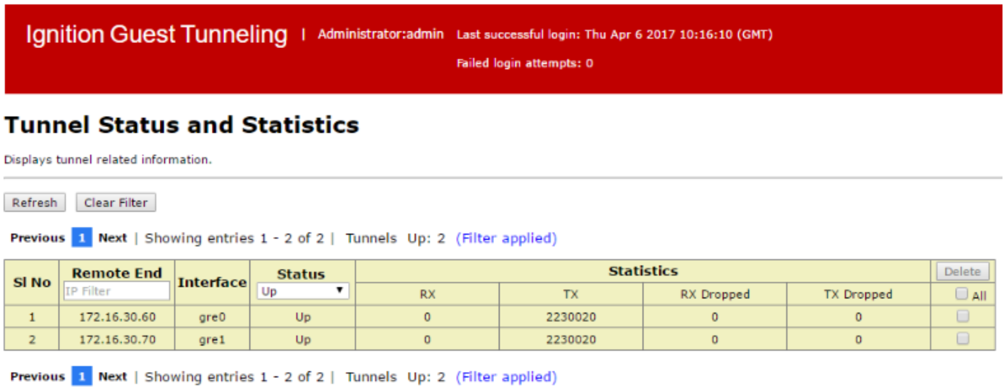
Refresh

Previous 1 Next | Showing entries 1 - 2 of 2 | Tunnels Up: 2, Down: 0, AdminDown: 0

Sl No	Remote End	Interface	Status	Statistics				Delete
	IP Filter		All ▾	RX	TX	RX Dropped	TX Dropped	□ All
1	172.16.30.60	gre0	Up	0	2197000	0	0	□
2	172.16.30.70	gre1	Up	0	2197000	0	0	□

Previous 1 Next | Showing entries 1 - 2 of 2 | Tunnels Up: 2, Down: 0, AdminDown: 0

6. Click **Clear Filter** button to clear all the applied filters.



Ignition Guest Tunneling | Administrator:admin Last successful login: Thu Apr 6 2017 10:16:10 (GMT)
Failed login attempts: 0

Tunnel Status and Statistics

Displays tunnel related information.

Refresh Clear Filter

Previous 1 Next | Showing entries 1 - 2 of 2 | Tunnels Up: 2 (Filter applied)

Sl No	Remote End	Interface	Status	Statistics				Delete
	IP Filter		Up ▾	RX	TX	RX Dropped	TX Dropped	□ All
1	172.16.30.60	gre0	Up	0	2230020	0	0	□
2	172.16.30.70	gre1	Up	0	2230020	0	0	□

Previous 1 Next | Showing entries 1 - 2 of 2 | Tunnels Up: 2 (Filter applied)

Note:

The **Clear Filter** button appears only when a filter is applied.

Importing GRE tunnel

About this task

Use this procedure to import the GRE tunnel configuration from WLAN 9100 or from exported IGT tunnel configuration.

Note:

You can import the GRE tunnel configuration `.csv` file from WLAN 9100 Orchestration server. You can also import `.tar` or `.zip` file from exported IGT tunnel configuration.

Procedure

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

The .csv is exported from the WOS and .tar or .zip from exported IGT tunnel configuration to configure the GRE Tunnels on IGT. For more information see, Exporting WLAN Access Points configuration on page 32

3. Click **Import** to import the configuration file.

   The user interface parses the input file and import tunnel related information into the IGT. The imported information or AP IP address, group list (if present) and its corresponding mapping to tunnels, VLAN list (if present) and its corresponding mapping to tunnels.

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

Exporting GRE Tunnel

About this task

You can export GRE tunnel from IGT and save it in .zip format.

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 .zip file.

Configuring Guest VLAN Untagging

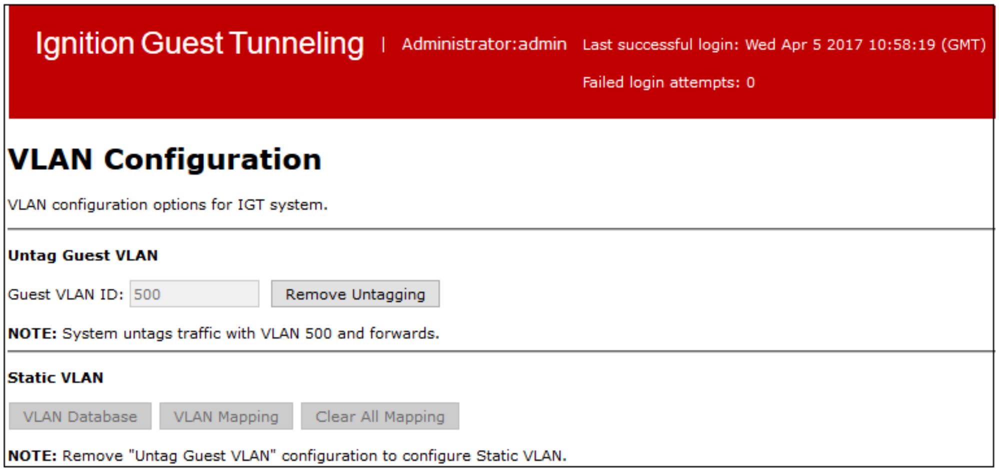
About this task

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

Procedure

1. Navigate to **Tunnel — VLAN** .

   The Guest VLAN Untagging Configuration window is displayed.



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:58:19 (GMT)

Failed login attempts: 0

VLAN Configuration

VLAN configuration options for IGT system.

Untag Guest VLAN

Guest VLAN ID: 500

NOTE: System untags traffic with VLAN 500 and forwards.

Static VLAN

NOTE: Remove "Untag Guest VLAN" configuration to configure Static VLAN.

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**.

Tunnel Grouping

Tunnel grouping allows you to group a set of tunnels and perform operations like enable, disable, and delete. Tunnel grouping involves:

- Managing Groups. For more information, see Managing groups on page 41
- Mapping. For more information, see Map on page 45
- Operation. For more information, see Operation on page 48

Managing groups

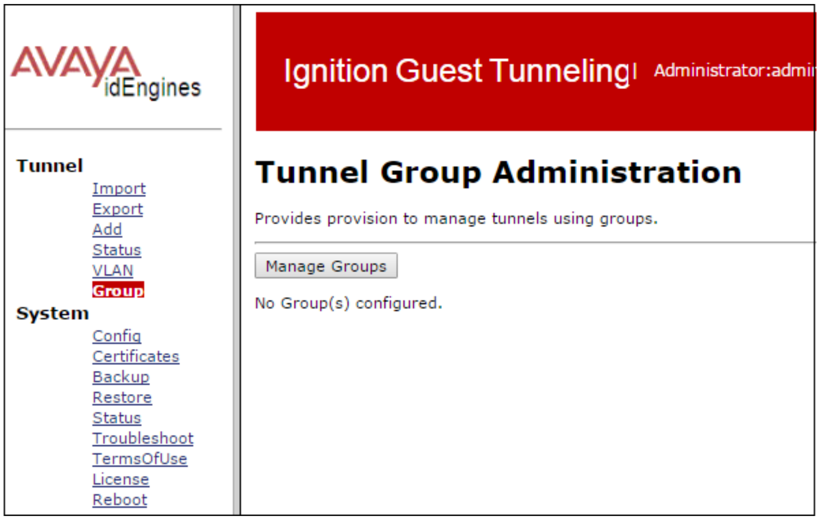
About this task

An Administrator can add, delete or re-name tunnel groups.

Procedure

1. Navigate to **Tunnel** > **Group**.

   The following page appears when no groups are configured.

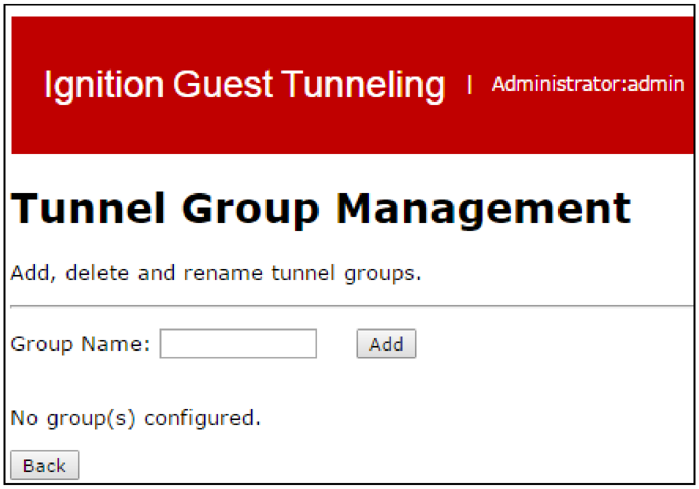


Tunnel Group Administration

Provides provision to manage tunnels using groups.

No Group(s) configured.

2. Click **Manage Groups**.



Tunnel Group Management

Add, delete and rename tunnel groups.

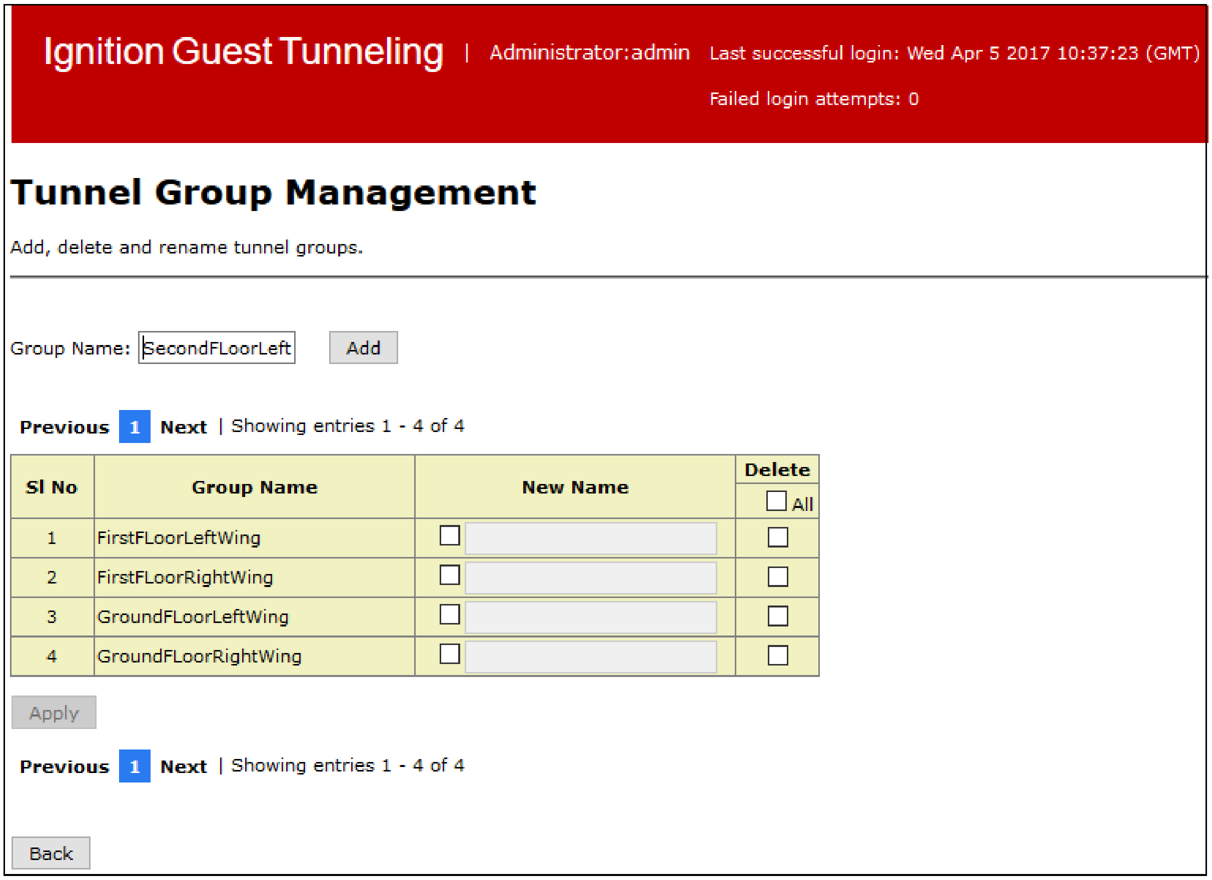
Group Name:

No group(s) configured.

3. **Adding a group:** .

   In the **Group Name** field, enter the group name and click **Add**

   For example, four tunnel groups are added.



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:37:23 (GMT)

Failed login attempts: 0

Tunnel Group Management

Add, delete and rename tunnel groups.

Group Name: SecondFLoorLeft

Previous 1 Next | Showing entries 1 - 4 of 4

Sl No	Group Name	New Name	Delete □ All
1	FirstFLoorLeftWing	□	□
2	FirstFLoorRightWing	□	□
3	GroundFLoorLeftWing	□	□
4	GroundFLoorRightWing	□	□

Apply
Previous 1 Next | Showing entries 1 - 4 of 4
Back

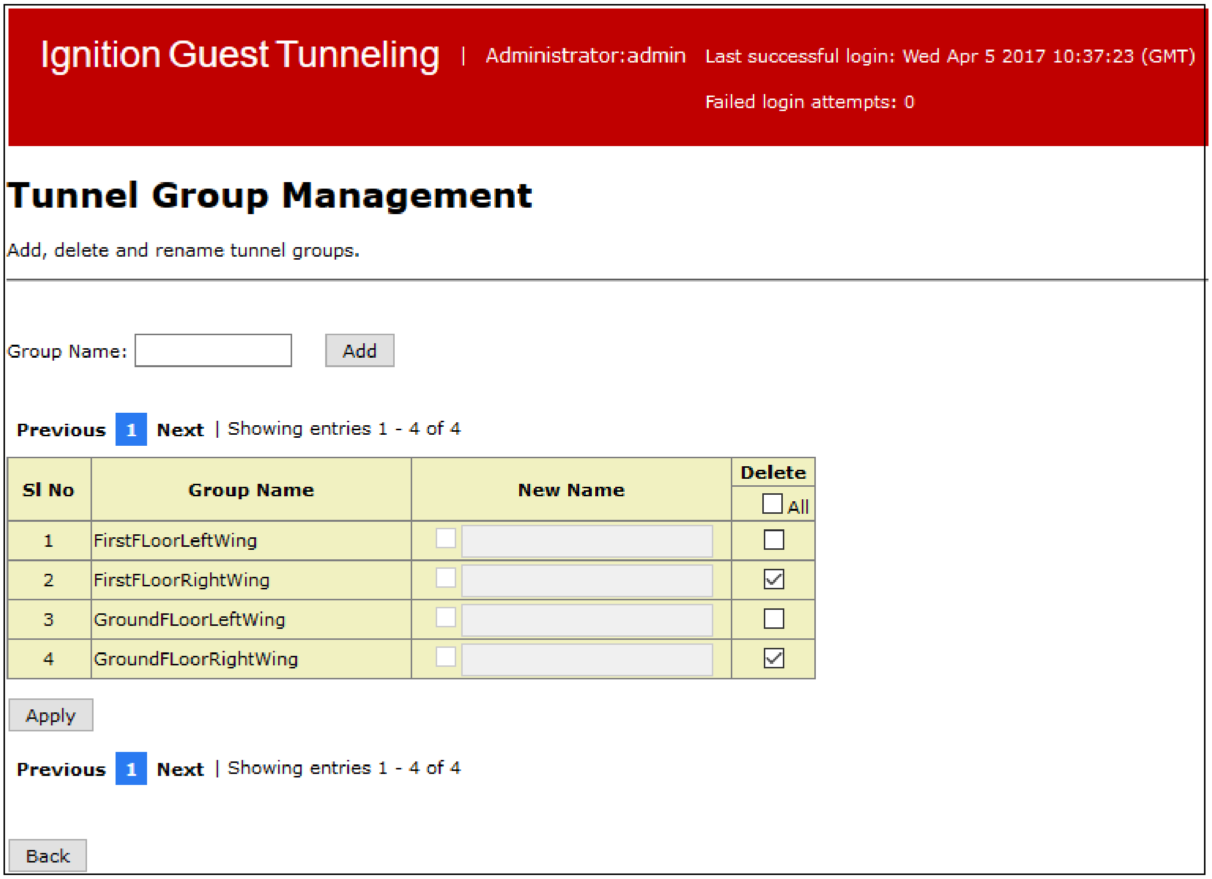
Note:

The maximum tunnel groups that can be configured are 128.

The maximum size of the tunnel group name can be up to 50 characters. Group Name may only contain alphanumeric, hyphen, and underscore characters.

4. **Deleting a group:**

   Administrator can delete single or multiple existing tunnel group(s) by selecting the check-box of the respective **Group Name** and click **Apply**.



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:37:23 (GMT)

Failed login attempts: 0

Tunnel Group Management

Add, delete and rename tunnel groups.

Group Name: Add

Previous 1 Next | Showing entries 1 - 4 of 4

Sl No	Group Name	New Name	Delete
			□ All
1	FirstFLoorLeftWing	□	□
2	FirstFLoorRightWing	□	☑
3	GroundFLoorLeftWing	□	□
4	GroundFLoorRightWing	□	☑

Apply

Previous 1 Next | Showing entries 1 - 4 of 4

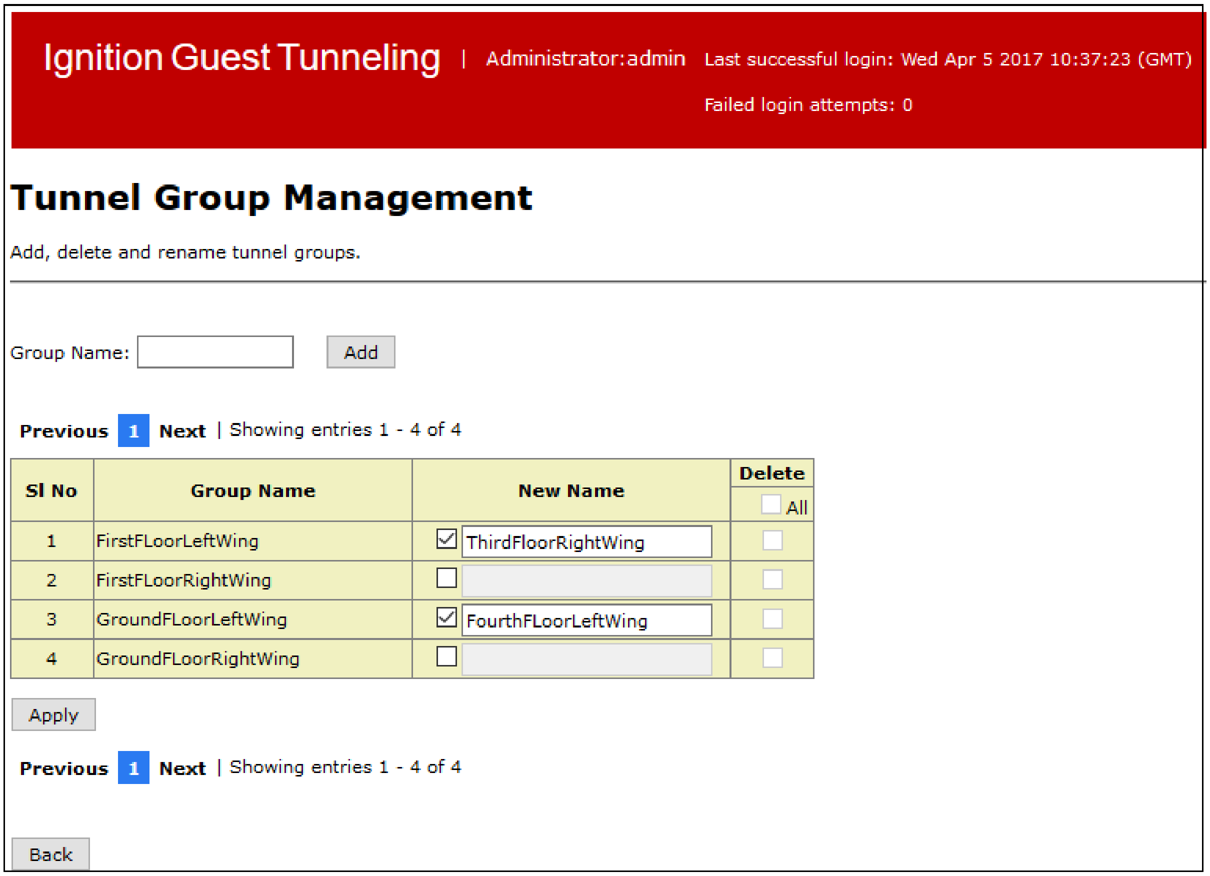
Back

Note:

Only tunnel groups are deleted. The assigned tunnels in the tunnel group still remain in the system.

5. **Renaming a group name:**

   Administrator can rename single or multiple existing tunnel group(s). Renaming a tunnel group moves all the tunnels and their settings under old group-name to new group-name. Select the check-box of the respective **Group Name** and type the new tunnel group name in the field provided, and click **Apply** .



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:37:23 (GMT)

Failed login attempts: 0

Tunnel Group Management

Add, delete and rename tunnel groups.

Group Name: [ ] Add

Previous 1 Next | Showing entries 1 - 4 of 4

Sl No	Group Name	New Name	Delete □ All
1	FirstFLoorLeftWing	☑ ThirdFloorRightWing	□
2	FirstFLoorRightWing	□	□
3	GroundFLoorLeftWing	☑ FourthFLoorLeftWing	□
4	GroundFLoorRightWing	□	□

Apply

Previous 1 Next | Showing entries 1 - 4 of 4

Back

Map

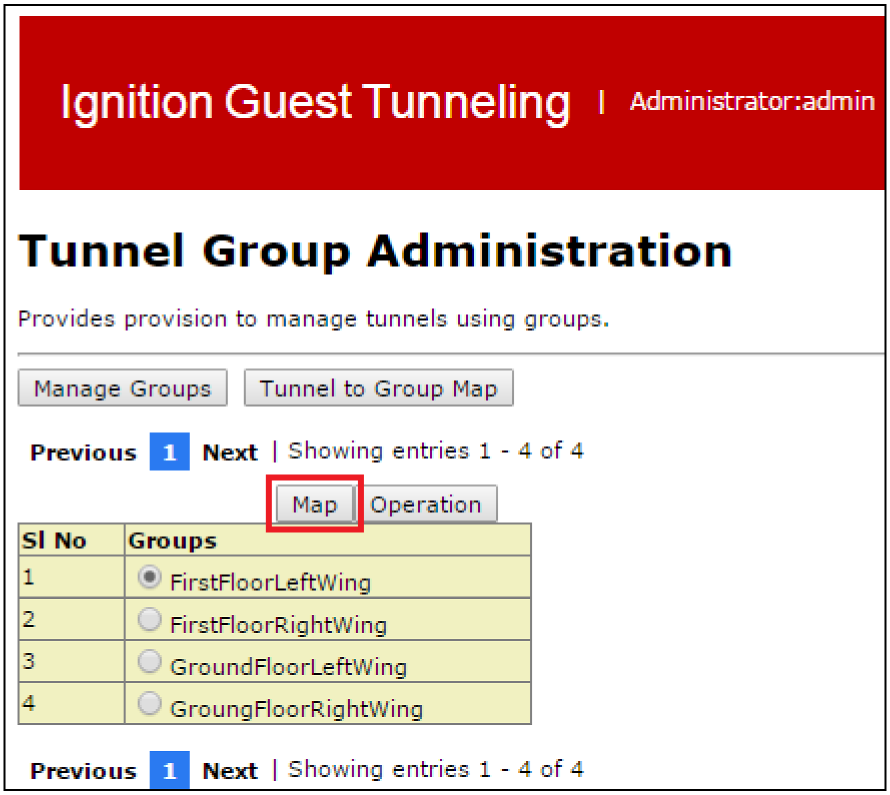
About this task

Administrator can map/unmap tunnels to a group which can be done in two ways: mapping group to tunnel or tunnel to a group.

Procedure

1. **Group — Tunnel mapping:**

   To map Group to Tunnel, select the required tunnel group and click **Map** .



Ignition Guest Tunneling | Administrator:admin

Tunnel Group Administration

Provides provision to manage tunnels using groups.

Manage Groups | Tunnel to Group Map

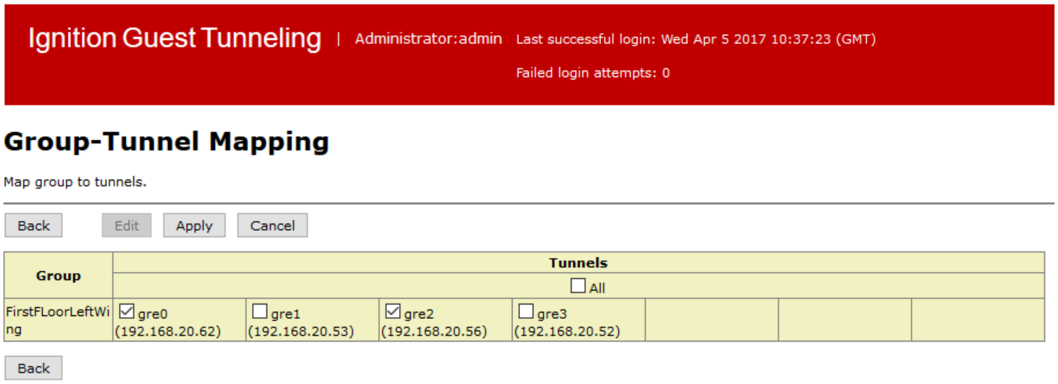
Previous 1 Next | Showing entries 1 - 4 of 4

Map | Operation

Sl No	Groups
1	● FirstFloorLeftWing
2	○ FirstFloorRightWing
3	○ GroundFloorLeftWing
4	○ GroungFloorRightWing

Previous 1 Next | Showing entries 1 - 4 of 4

Click **Edit** and select the required tunnels that need to be mapped and Click **Apply** :



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:37:23 (GMT)

Failed login attempts: 0

Group-Tunnel Mapping

Map group to tunnels.

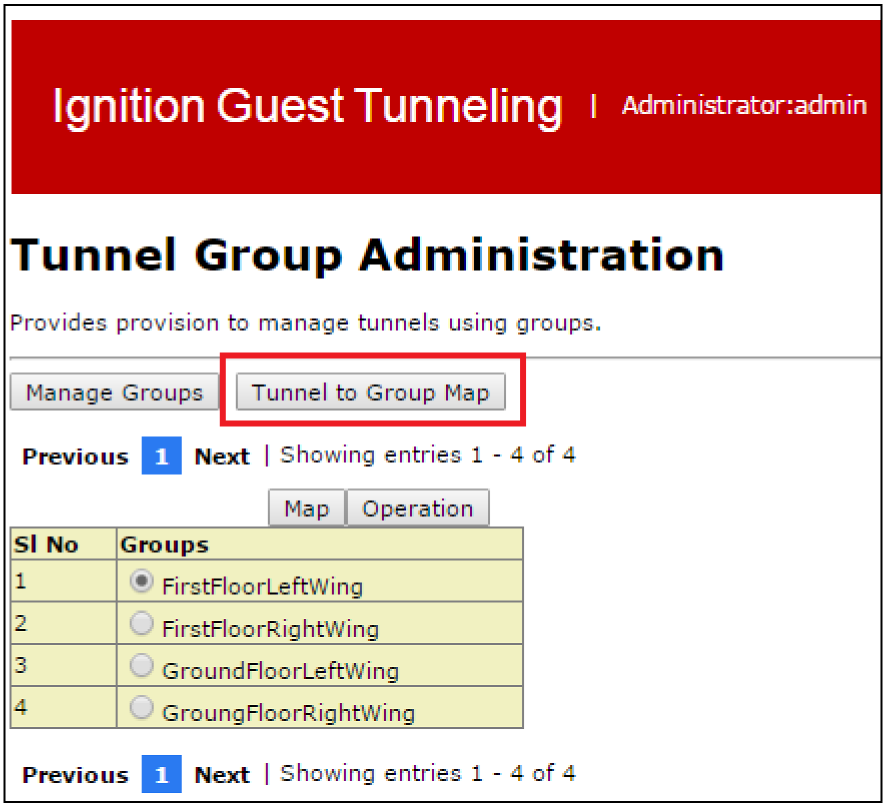
Back Edit Apply Cancel

Group	Tunnels						
	☐ All						
FirstFLoorLeftWing	☑ gre0 (192.168.20.62)	☐ gre1 (192.168.20.53)	☑ gre2 (192.168.20.56)	☐ gre3 (192.168.20.52)			

Back

2. **Tunnel — Group Mapping:**

   Administrator can map Tunnel to Groups. Click **Tunnel to Group Map** :



Ignition Guest Tunneling | Administrator:admin

Tunnel Group Administration

Provides provision to manage tunnels using groups.

Manage Groups
Tunnel to Group Map
Previous 1 Next | Showing entries 1 - 4 of 4
Map
Operation

Sl No	Groups
1	● FirstFloorLeftWing
2	○ FirstFloorRightWing
3	○ GroundFloorLeftWing
4	○ GroungFloorRightWing

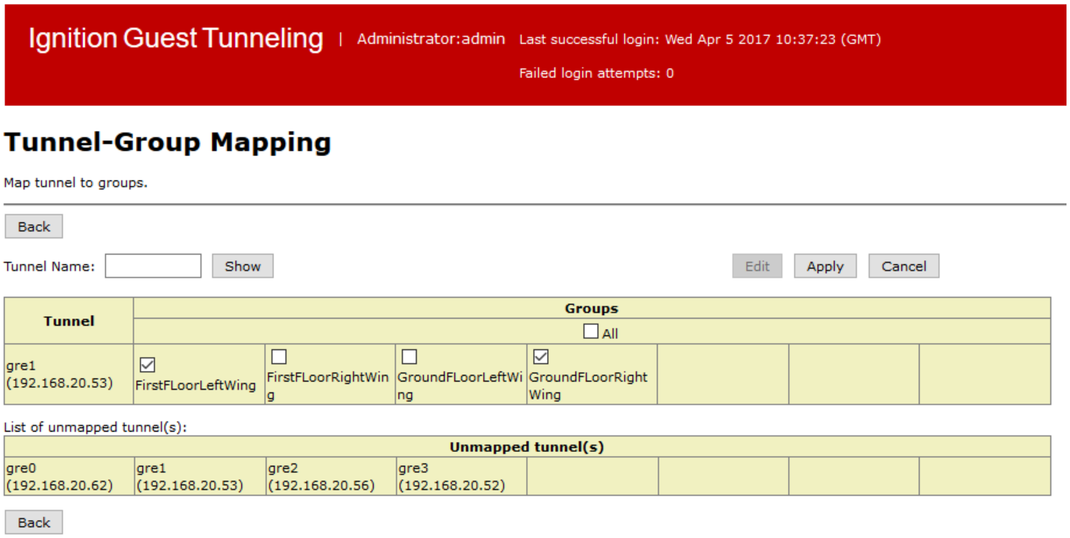
Previous 1 Next | Showing entries 1 - 4 of 4

Enter the **Tunnel Name** in the field provided and Click **Show** .

Note:

The list of unmapped tunnels are displayed on the same page below.

Click **Edit** button, Select the required tunnel groups that need to be mapped to tunnel and Click **Apply** :



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:37:23 (GMT)

Failed login attempts: 0

Tunnel-Group Mapping

Map tunnel to groups.

Tunnel	Groups						
	□ All						
gre1 (192.168.20.53)	☑ FirstFLoorLeftWing	□ FirstFLoorRightWing	□ GroundFLoorLeftWing	☑ GroundFLoorRightWing			

List of unmapped tunnel(s):

Unmapped tunnel(s)							
gre0 (192.168.20.62)	gre1 (192.168.20.53)	gre2 (192.168.20.56)	gre3 (192.168.20.52)				

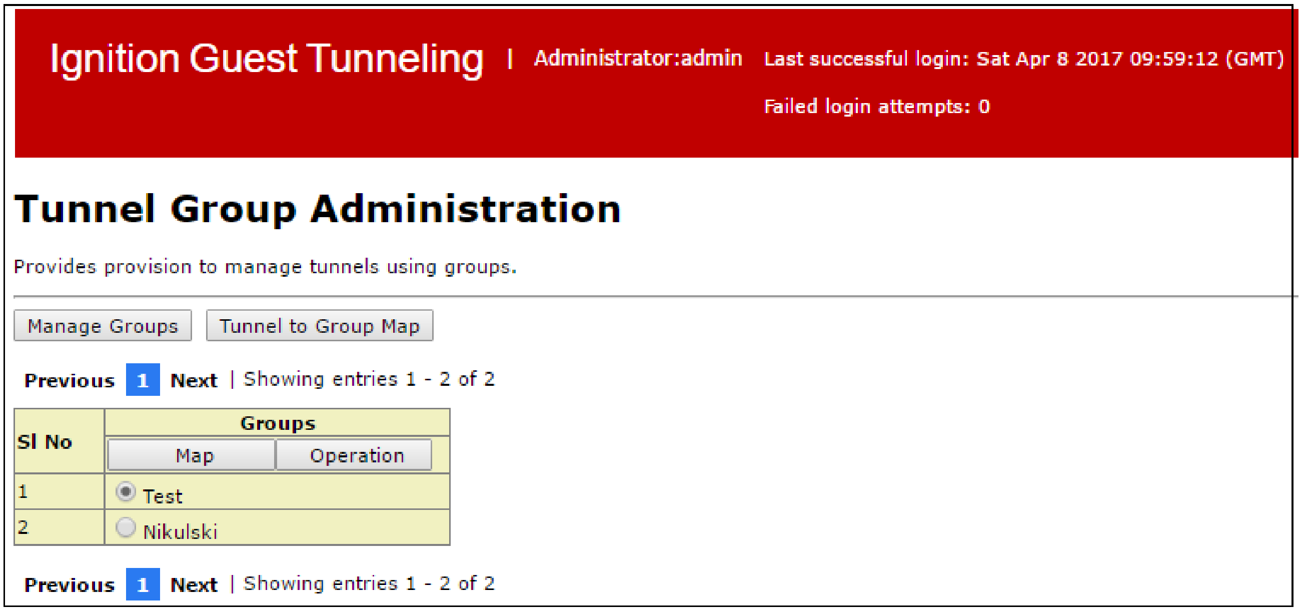
Operation

About this task

Administrator can perform group operations such as Enable/Disable/Delete on a required group.

Procedure

Click **Operation**.



Ignition Guest Tunneling | Administrator:admin Last successful login: Sat Apr 8 2017 09:59:12 (GMT)

Failed login attempts: 0

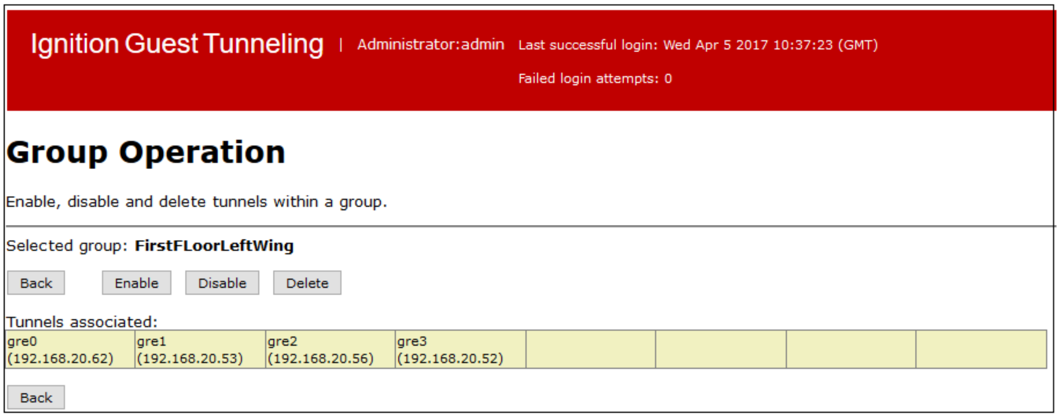
Tunnel Group Administration

Provides provision to manage tunnels using groups.

Manage Groups
Tunnel to Group Map
Previous 1 Next | Showing entries 1 - 2 of 2

Sl No	Groups	
	Map	Operation
1	● Test	
2	○ Nikulski	

Previous 1 Next | Showing entries 1 - 2 of 2



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:37:23 (GMT)

Failed login attempts: 0

Group Operation

Enable, disable and delete tunnels within a group.

Selected group: **FirstFLoorLeftWing**

Tunnels associated:

gre0 (192.168.20.62)	gre1 (192.168.20.53)	gre2 (192.168.20.56)	gre3 (192.168.20.52)				

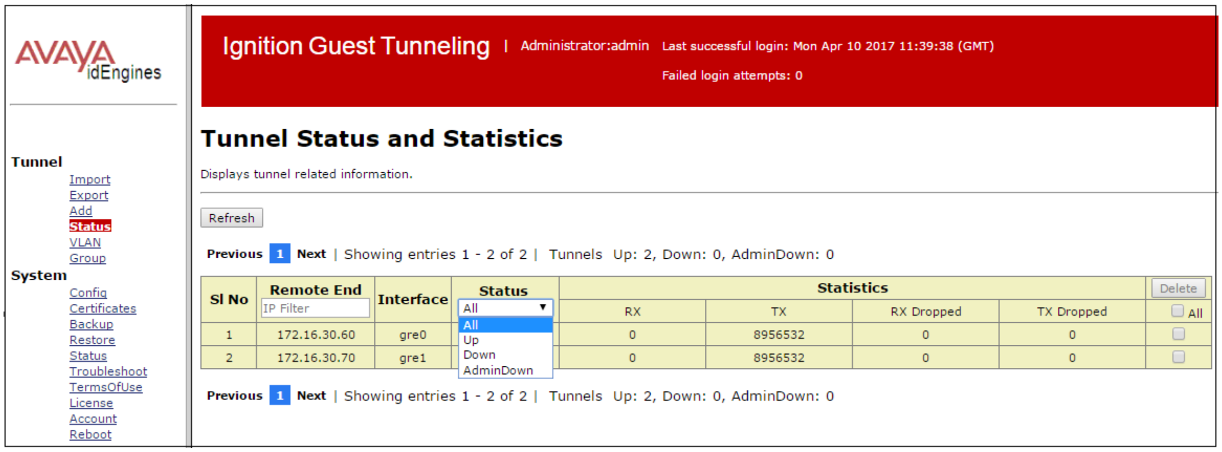
Note:

When performing any group operation on tunnels, those tunnels if they are associated with other groups, they are displayed below on the same page.

- To enable tunnels in the selected group, click **Enable**.
- To disable tunnels in the selected group, click **Disable** .

Note:

On disabling a tunnel group, the tunnel status changes to **AdminDown**.



Ignition Guest Tunneling | Administrator:admin Last successful login: Mon Apr 10 2017 11:39:38 (GMT)
Failed login attempts: 0

Tunnel Status and Statistics

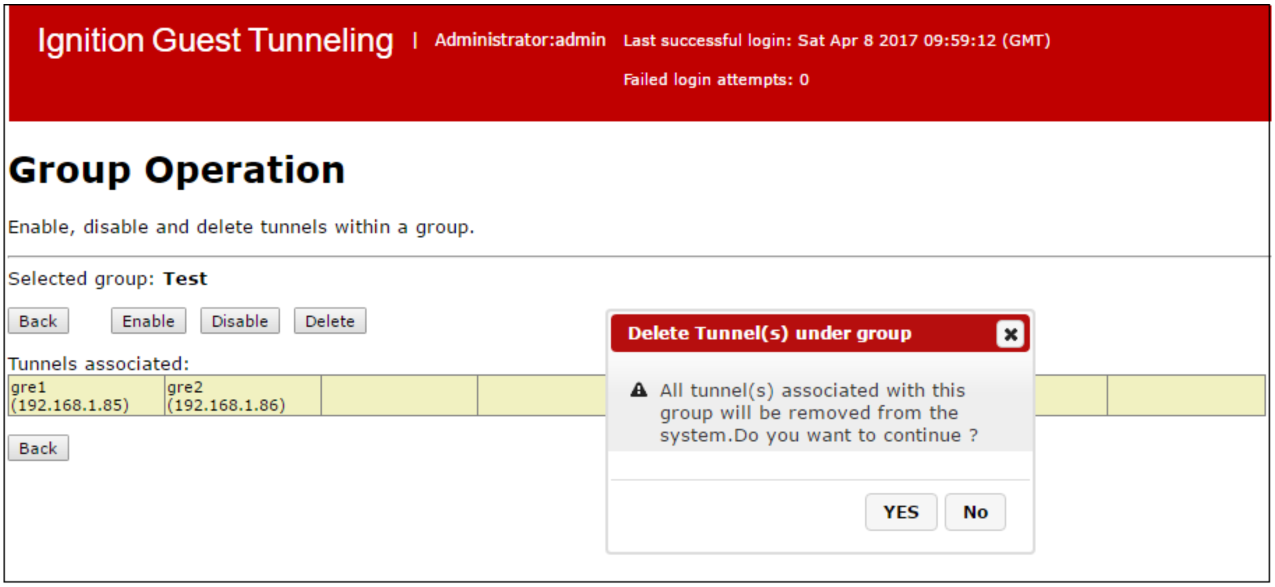
Displays tunnel related information.

Previous 1 Next | Showing entries 1 - 2 of 2 | Tunnels Up: 2, Down: 0, AdminDown: 0

Sl No	Remote End	Interface	Status	Statistics				Delete
	IP Filter		All	RX	TX	RX Dropped	TX Dropped	□ All
1	172.16.30.60	gre0		0	8956532	0	0	□
2	172.16.30.70	gre1		0	8956532	0	0	□

Previous 1 Next | Showing entries 1 - 2 of 2 | Tunnels Up: 2, Down: 0, AdminDown: 0

- To remove tunnels under the group from the system, click **Delete** . A warning message is popped up for confirming the deletion.



Ignition Guest Tunneling | Administrator:admin Last successful login: Sat Apr 8 2017 09:59:12 (GMT)
Failed login attempts: 0

Group Operation

Enable, disable and delete tunnels within a group.

Selected group: **Test**

Tunnels associated:

gre1 (192.168.1.85)	gre2 (192.168.1.86)							

Delete Tunnel(s) under group

All tunnel(s) associated with this group will be removed from the system.Do you want to continue ?

Chapter 6: Managing the IGT GRE Tunnel System

This chapter is intended for an Avaya Identity Engines Ignition Guest Tunneling administrator.

Use the procedures in this chapter to either manage the IGT Tunnel System or to migrate IGT to a newer version.

Managing the IGT GRE Tunnel

Use the following procedures to manage the IGT GRE Tunnel.

For more information on:

- Taking a back up of system configuration, see Taking a backup of the IGT system configuration on page 68.
- Restoring system configuration, see Restoring the IGT system configuration on page 69.
- Configuring TCP Maximum Segment Size (MSS) values, see Configuring Guest Tunneling Appliance on page 67.
- Certificate management, see Certificate Management on page 62.
- Licensing, see Licensing Overview on page 57.
- Logging out, see Logging out of Guest Tunneling Appliance on page 78.

Logging Into Guest Tunneling Appliance

About this task

Use this procedure to login to Avaya Identity Engines Ignition Guest Tunneling Virtual Appliance.

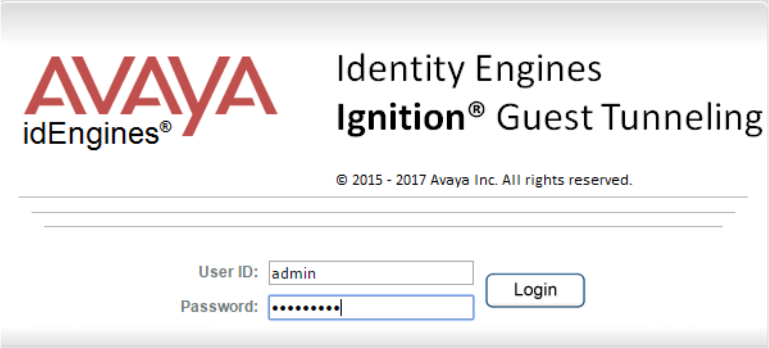
Before you begin

Ensure to do the following:

- Install this application as a virtual appliance on a VMware ESXi 5.1, 5.5 or 6.0 server.
- A computer with a supported Web browser and access to the network.

Procedure

1. On the Web browser, enter the Ignition Guest Tunneling login URL `https://<admin IP>`.
2. On the login screen, enter the User name and Password in the **User ID** and **Password** fields.



Identity Engines
Ignition® Guest Tunneling

© 2015 - 2017 Avaya Inc. All rights reserved.

User ID: admin
Password: •••••••••

3. Click **Login** to login to Avaya Identity Engines Ignition Guest Tunneling Virtual Appliance.

   On successful login, it directs to the **Status** page.

Password Change

About this task

Administrator can change the password and configure password complexity policy.

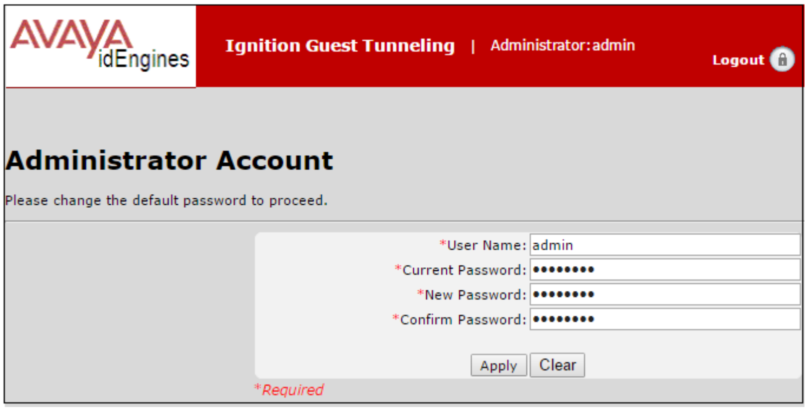
Before you begin

Ensure to log on to Avaya Identity Engines Ignition Guest Tunneling application.

Procedure

1. **First Login Password Change:**

   It is mandatory to change the password on the first login to access the features in the system.



Administrator Account

Please change the default password to proceed.

*User Name: admin
*Current Password: ••••••••
*New Password: ••••••••
*Confirm Password: ••••••••

   Enter all the mandatory fields (Current Password, New Password and Confirm Password) and Click **Apply** button.

Note:

Current password is your initial default login password **admin**.

New password is a combination of alphanumeric and must have the following characteristics:

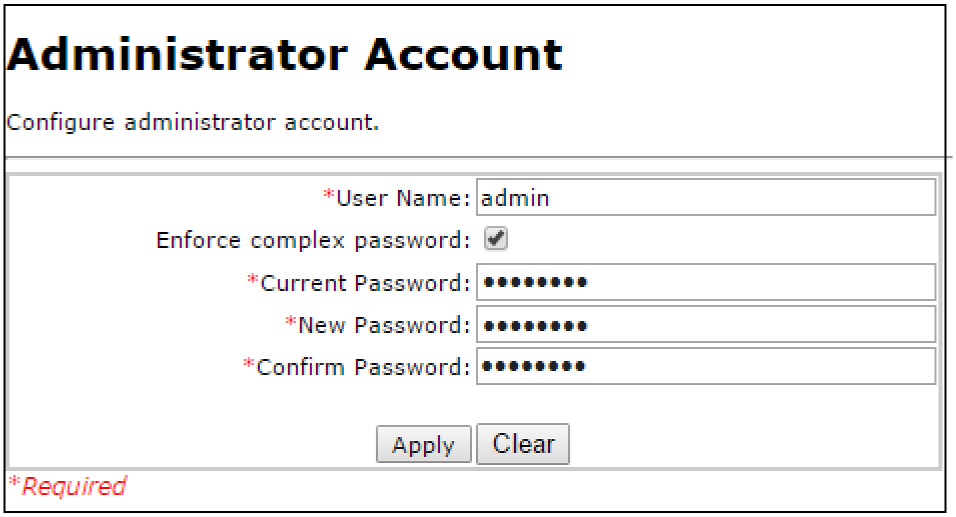
- Use a minimum of 8 characters
- Include at least one uppercase letter
- Include at least one lowercase letter
- Include at least one numeric number
- Include at least one special character from !, @, #, $, %, ^, &, *, (,), -, +

Caution:

Password change using the CLI has been deprecated.

2. **Password complexity:**

Administrator can enable or disable password complexity. Complex passwords are more secure. To enable or disable password complexity, navigate to **System** > **Account**.



Administrator Account

Configure administrator account.

*User Name:	admin
Enforce complex password:	☑
*Current Password:	••••••••
*New Password:	••••••••
*Confirm Password:	••••••••

*Required

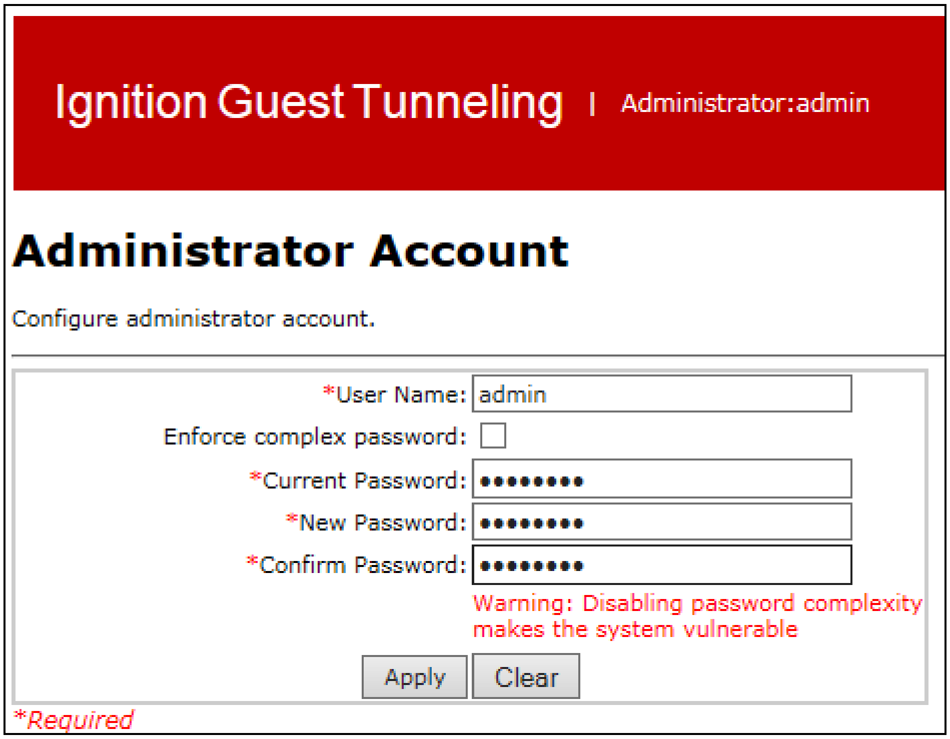
The **Enforce complex password** check box is selected by default.

All fields (Current Password, New Password and Confirm Passwords) are mandatory. The new password must match the password complexity requirements.

Note:

New password cannot be same as last three passwords.

To disable password complexity, deselect the **Enforce complex password** check box and enter the new password of your own choice. If administrator disables password complexity, the new password need not match the password complexity requirement. Disabling password complexity makes the system vulnerable.



Administrator Account

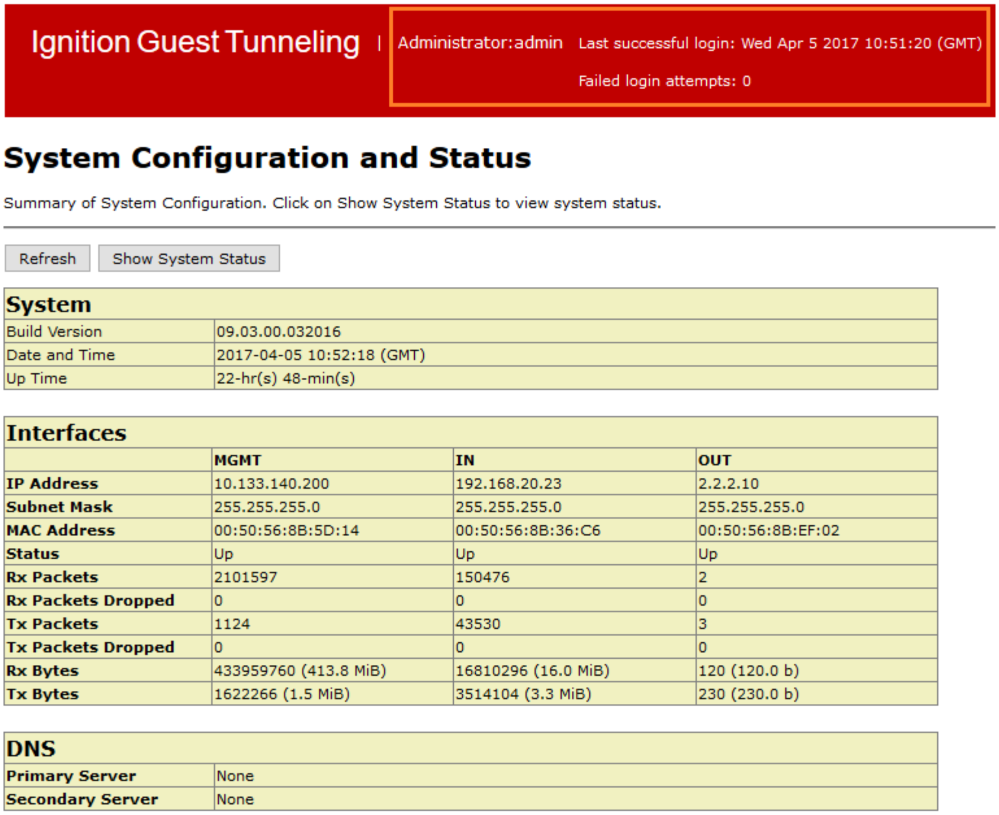
Configure administrator account.

*User Name:	admin
Enforce complex password:	□
*Current Password:	••••••••
*New Password:	••••••••
*Confirm Password:	••••••••
	Warning: Disabling password complexity makes the system vulnerable

*Required

Login History

- When Administrator logs into IGT Web UI, the last successful login time and the number of failed attempts of the Admin account before current login is displayed in the **System Configuration and Status** page.



System Configuration and Status

Summary of System Configuration. Click on Show System Status to view system status.

System	
Build Version	09.03.00.032016
Date and Time	2017-04-05 10:52:18 (GMT)
Up Time	22-hr(s) 48-min(s)

Interfaces	MGMT	IN	OUT
IP Address	10.133.140.200	192.168.20.23	2.2.2.10
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
MAC Address	00:50:56:8B:5D:14	00:50:56:8B:36:C6	00:50:56:8B:EF:02
Status	Up	Up	Up
Rx Packets	2101597	150476	2
Rx Packets Dropped	0	0	0
Tx Packets	1124	43530	3
Tx Packets Dropped	0	0	0
Rx Bytes	433959760 (413.8 MiB)	16810296 (16.0 MiB)	120 (120.0 b)
Tx Bytes	1622266 (1.5 MiB)	3514104 (3.3 MiB)	230 (230.0 b)

DNS	
Primary Server	None
Secondary Server	None

Maximum number of Sessions

- The Administrator can login to IGT Web UI simultaneously for up to **five** concurrent sessions.

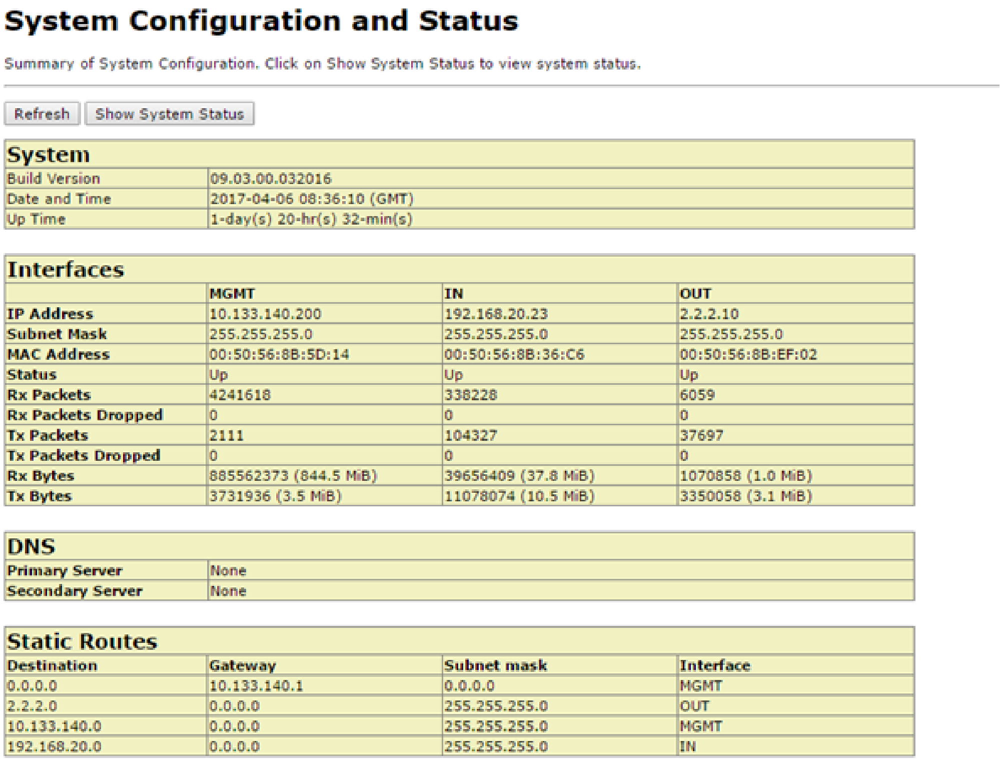
  Note:

  If the Administrator tries to login to IGT from a sixth session, the system displays a message, **“Maximum number of sessions reached”**. Once the session limit is reached, the Admin needs to exit from one of the five active sessions to allow user to login with a new session.

  Note:

  - In the unlikely scenario where the Administrator is not able to gracefully exit from the existing sessions, he/she can login to the IGT console and clear these sessions using the command **`clear sessions`** .
  - This session limit is for Web sessions only. The System status page shows the list of Active Web Sessions.

- Click **Show System Status** to view the list of Active Web sessions.



System Configuration and Status

Summary of System Configuration. Click on Show System Status to view system status.

System	
Build Version	09.03.00.032016
Date and Time	2017-04-06 08:36:10 (GMT)
Up Time	1-day(s) 20-hr(s) 32-min(s)

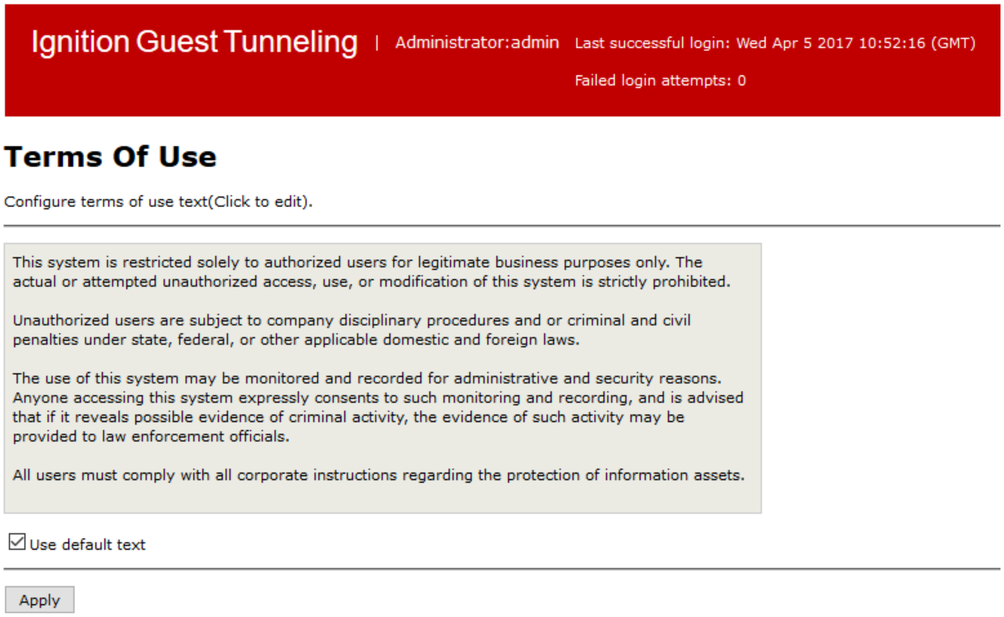
Interfaces			
	MGMT	**IN**	**OUT**
IP Address	10.133.140.200	192.168.20.23	2.2.2.10
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
MAC Address	00:50:56:8B:5D:14	00:50:56:8B:36:C6	00:50:56:8B:EF:02
Status	Up	Up	Up
Rx Packets	4241618	338228	6059
Rx Packets Dropped	0	0	0
Tx Packets	2111	104327	37697
Tx Packets Dropped	0	0	0
Rx Bytes	885562373 (844.5 MiB)	39656409 (37.8 MiB)	1070858 (1.0 MiB)
Tx Bytes	3731936 (3.5 MiB)	11078074 (10.5 MiB)	3350058 (3.1 MiB)

DNS	
Primary Server	None
Secondary Server	None

Static Routes			
Destination	**Gateway**	**Subnet mask**	**Interface**
0.0.0.0	10.133.140.1	0.0.0.0	MGMT
2.2.2.0	0.0.0.0	255.255.255.0	OUT
10.133.140.0	0.0.0.0	255.255.255.0	MGMT
192.168.20.0	0.0.0.0	255.255.255.0	IN

Terms of Use

- IGT **Terms of Use** banner provides the ability to display a customer configured security warning banner on the system login screen.
- Click **System** > **Terms of Use** to view the **Terms of Use** banner.



Last successful login: Wed Apr 5 2017 10:52:16 (GMT)

Failed login attempts: 0

Terms Of Use

Configure terms of use text(Click to edit).

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

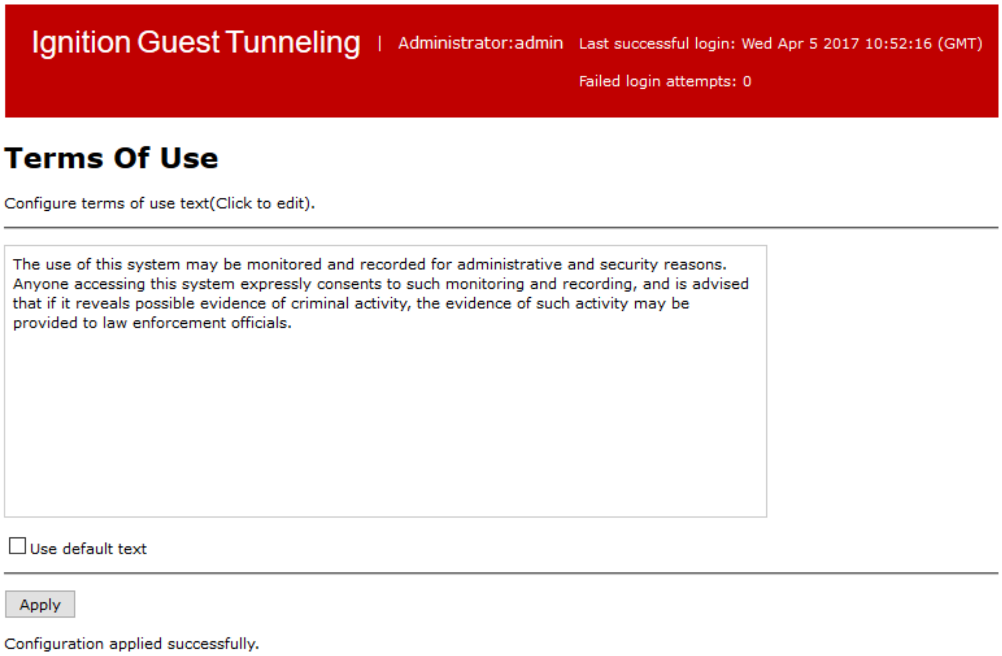
All users must comply with all corporate instructions regarding the protection of information assets.

☑ Use default text

Note:

The default banner is displayed when the **Use default text** check box is selected.

- To edit the Terms of Use banner, do the following:
  - Uncheck the **Use default text** check box.
  - Enter the new **Terms of Use** text.
  - Click **Apply** button. System displays a message **Configuration applied successfully**.



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:52:16 (GMT)
Failed login attempts: 0

Terms Of Use

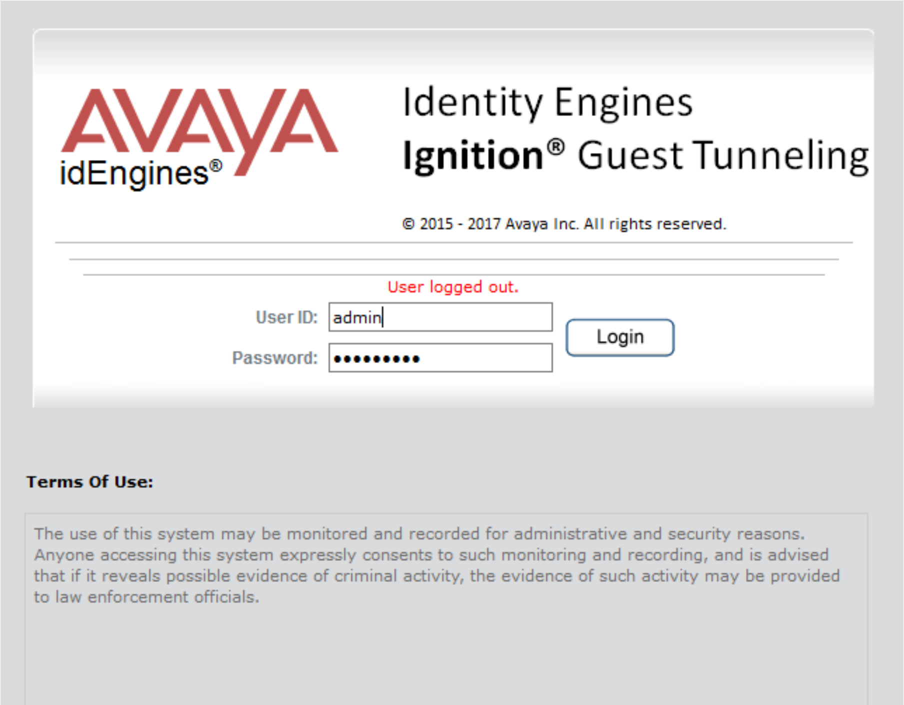
Configure terms of use text(Click to edit).

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

□ Use default text

Configuration applied successfully.

Logout from the current session. The Login Page reflecting new Terms of Use gets displayed as shown below :



AVAYA idEngines®
Identity Engines
Ignition® Guest Tunneling
© 2015 - 2017 Avaya Inc. All rights reserved.

User logged out.

User ID: admin

Password: •••••••••

Terms Of Use:

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

Note:

If the Admin wants to revert to the default banner, select the **Use default text** check box and click **Apply** button.

Licensing Overview

This section is meant for introducing Licensing mechanism for Avaya Identity Engines Ignition Guest Tunneling application. It supports the Keycode Retrieval System (KRS) based licensing model providing time based license along with support for two levels of licensing (Lite and Large). It provides a temporary 30 days license that can be obtained from http://www.avaya.com/identitytrial.

Note:

It is required to have a valid license to navigate and perform any task after you log in to the IGT application. For more information on logging on to the application, see Logging into Guest Tunneling Appliance on page 50.

IGT supports two types of licenses:

- LITE, supports 10 GRE tunnels for small scale deployments.
- LARGE, supports 500 GRE tunnels for large scale deployments.

Obtaining KRS Licenses

About this task

If you have received paper LACs with your purchase, follow the instructions on them on how to obtain your licenses. These are KRS licenses.

Before you begin

Send an e-mail to `datalicensing@avaya.com` to request your KRS licenses and include the following information:

Procedure

1. End user company name and full mailing address (no mailboxes).
2. End user company URL.
3. End user contact name.
4. End user corporate email address.
5. End user phone number.
6. License Authorization Code (LAC) that shows in the box at the bottom right of the LAC certificate.
7. System Serial Number.

   ❗ **Important:**

   After the information is verified, licenses are sent to you by email.

Installing Avaya Identity Engines Ignition Guest Tunneling License

Before you begin

Customer must obtain a valid IGT license from Avaya before proceeding for installation.

About this task

Perform this procedure to install the IGT license.

Before you begin

- Ensure to log on to Avaya Identity Engines Ignition Guest Tunneling application.

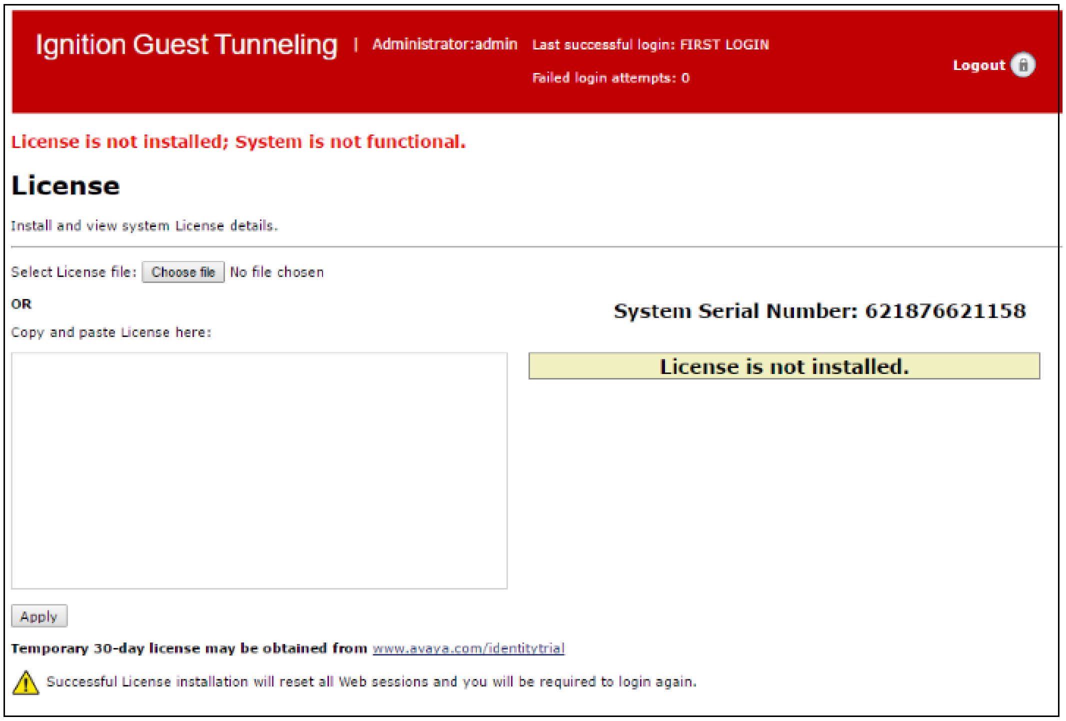
Procedure

1. On the menu bar, click **System** > **License**.

   The system displays the License page.

   ✳ **Note:**

   If the license is not installed, on login user is redirected to the License page.



License is not installed; System is not functional.

License

Install and view system License details.

Select License file: No file chosen

OR

Copy and paste License here:

System Serial Number: 621876621158

License is not installed.

Temporary 30-day license may be obtained from www.avaya.com/identitytrial

⚠ Successful License installation will reset all Web sessions and you will be required to login again.

2. Install the license file using any one of the following given option:

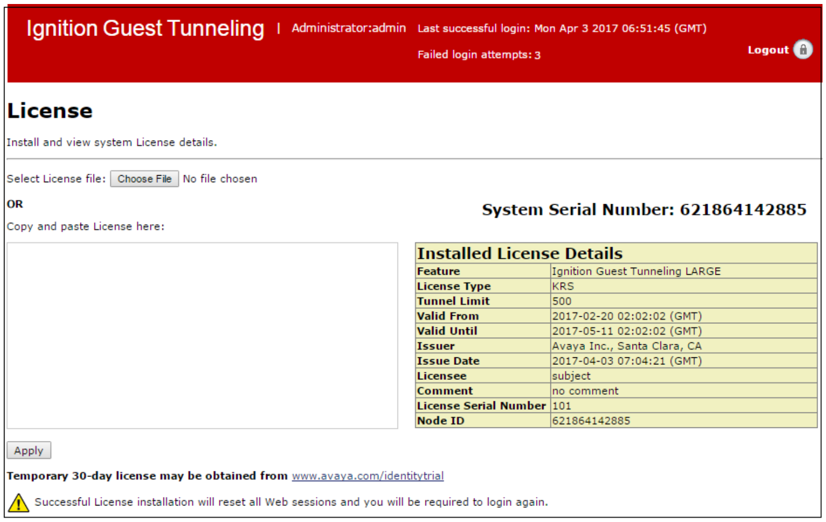
Choice Option	Choice Description
Choose a file	Click **Browse** to upload a file. Browse to the license file location, select the appropriate file.
Copy paste	Find the license you received from Avaya Support and open it in your e-mail tool or text editor. Return to the License Installation window on the application and paste the license text in the **Copy paste** section.

3. Click **Apply**.

   After the license is successfully applied, the system displays the **License Details** on the right side of the License page.

   Note:

   After successful import, session is automatically logged out and redirected to login page.



Ignition Guest Tunneling | Administrator:admin Last successful login: Mon Apr 3 2017 06:51:45 (GMT)
Failed login attempts: 3

License

Install and view system License details.

Select License file: Choose File No file chosen

OR

Copy and paste License here:

System Serial Number: 621864142885

Installed License Details	
Feature	Ignition Guest Tunneling LARGE
License Type	KRS
Tunnel Limit	500
Valid From	2017-02-20 02:02:02 (GMT)
Valid Until	2017-05-11 02:02:02 (GMT)
Issuer	Avaya Inc., Santa Clara, CA
Issue Date	2017-04-03 07:04:21 (GMT)
Licensee	subject
Comment	no comment
License Serial Number	101
Node ID	621864142885

Temporary 30-day license may be obtained from www.avaya.com/identitytrial

⚠ Successful License installation will reset all Web sessions and you will be required to login again.

Installed License detail	Description
Feature	Specifies the license type of the Guest Tunneling.
License Type	IGT currently supports Keycode Retrieval System (KRS) based licensing model.
Tunnel Limit	Specifies the tunnel capacity.
Valid From	Specifies the start date and time of the installed license.
Valid Until	Specifies the End date and time of the installed license.
Issuer	Specifies issuer name .
Issue date	Specifies the date on which the license is generated and issued.
Licensee	Specifies the Licensee name.
License serial number	Specifies the serial number of the generated license.
Node ID	Specifies the serial number.

4. Verify the license details and make sure you have uploaded a valid license file.

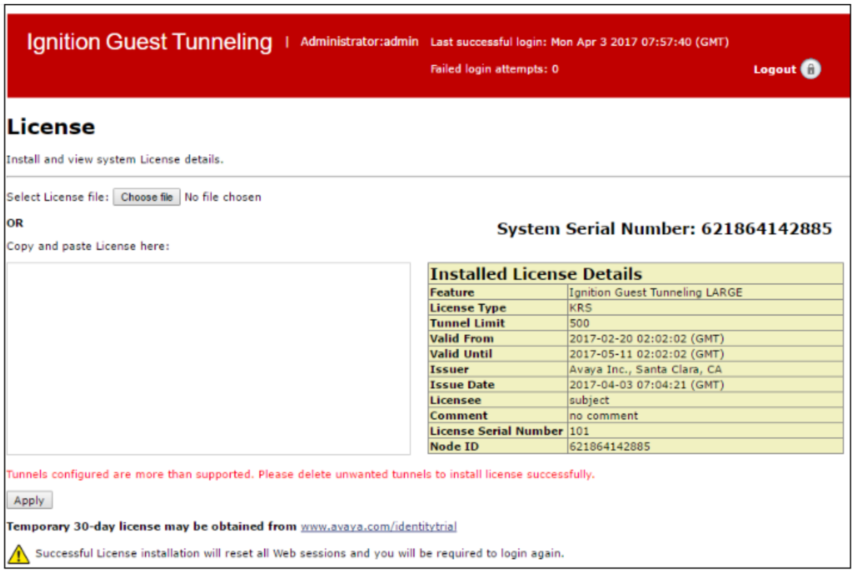
   If the license did not get applied successfully, system will return an error message.

Option	Description
If the license is valid	System redirects you to the License page.
If the license is not valid or is expired	System displays a message to prompt you to enter a valid license. You can still login to web UI, but you will not be able to configure anything on the system. In addition to losing access to configuration pages, IGT also stops forwarding the traffic. Once license is expired, the status of all the tunnels will change to AdminDown. Administrator can still have access to Export and Status under **Tunnel** heading, all the pages under **System** heading and the Logout option.

Option	Description
	Note: To upgrade or downgrade a license or renewal of expired license, user needs to obtain a valid license and follow the same steps he did to apply the initial license. Please refer Obtaining KRS License on page 58
If the license is about to expire in next 30 days	System displays a highlighted message showing the number of days remaining.

Note:

- Administrator can downgrade system from LARGE license to LITE, only if the number of tunnels configured are less than or equal to number of tunnels supported . The user can delete the excess tunnels by navigating to the Tunnel Status page.
- Administrator can upgrade system from LITE to LARGE license. Also, Administrator can also upgrade from trial license to any of the supported licenses.
- If tunnels configured are more than the licenses being upgraded, installation will fail and an error message appears:
- The user can delete the excess tunnels by navigating to the Tunnel Status page.



Last successful login: Mon Apr 3 2017 07:57:40 (GMT)

Failed login attempts: 0

License

Install and view system License details.

Select License file: Choose file No file chosen

OR

Copy and paste License here:

System Serial Number: 621864142885

Installed License Details

Feature	Ignition Guest Tunneling LARGE
License Type	KRS
Tunnel Limit	500
Valid From	2017-02-20 02:02:02 (GMT)
Valid Until	2017-05-11 02:02:02 (GMT)
Issuer	Avaya Inc., Santa Clara, CA
Issue Date	2017-04-03 07:04:21 (GMT)
Licensee	subject
Comment	no comment
License Serial Number	101
Node ID	621864142885

Tunnels configured are more than supported. Please delete unwanted tunnels to install license successfully.

Apply

Temporary 30-day license may be obtained from www.avaya.com/identitytrial

⚠ Successful License installation will reset all Web sessions and you will be required to login again.

Note:

- If license is not installed or license expires, Administrator can still have access to Export and Status under **Tunnel** heading and all the pages under **System** heading.
- Administrator is informed about license expiry 30 days before installed license expiry date on Status page one time after every successful login; this information is available on license page. If license is not installed, Administrator is redirected to License page as landing page.

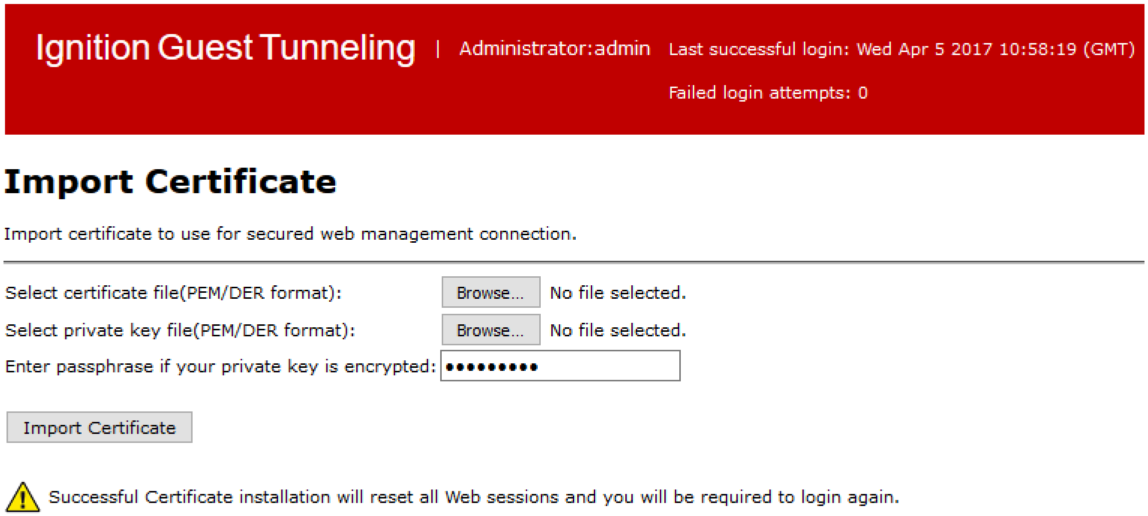
- Administrator is notified on all pages if license is not installed or expired or invalid due to serial number mismatch.
- Backed up system configuration can be restored with or without license information using **Exclude license** option on **Restore** page.
- License is tied to system management IP address. Therefore, Changing IP address will make the installed license invalid.

⚠ **Caution:**

After log in, until a valid license is installed, the system denies access to all configurations.

Certificate Management

This feature allows a user to import and use custom certificate for secure (https) web management connection to Ignition Guest Tunneling application. Navigate to **System** > **Certificates**.



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:58:19 (GMT)

Failed login attempts: 0

Import Certificate

Import certificate to use for secured web management connection.

Select certificate file(PEM/DER format): Browse... No file selected.

Select private key file(PEM/DER format): Browse... No file selected.

Enter passphrase if your private key is encrypted: ●●●●●●●●●

⚠ Successful Certificate installation will reset all Web sessions and you will be required to login again.

To import a certificate,

- Click **Browse** and select the valid certificate file which is in PEM/DER format. It can also be a chain certificate in PEM format.
- Click **Browse** and select the valid private key file which is in PEM/DER format

  Note:

  Obtain your server certificate and private key from a trusted certificate authority.
- Enter passphrase in the field provided (if your private key is encrypted)
- Click on the **Import Certificate** button

Note:

After successful import, session is automatically logged out and redirected to login page.

The existing default certificate is replaced with the new certificate.

If the user want to revert back to the default certificate, it can be done from the console using **`certificate rebuild`** command.

Syslog

About this task

Administrator can configure IGT to log system messages to external syslog servers. Maximum of three syslog servers can be configured on IGT to receive system messages. IGT supports 3 types of logs:

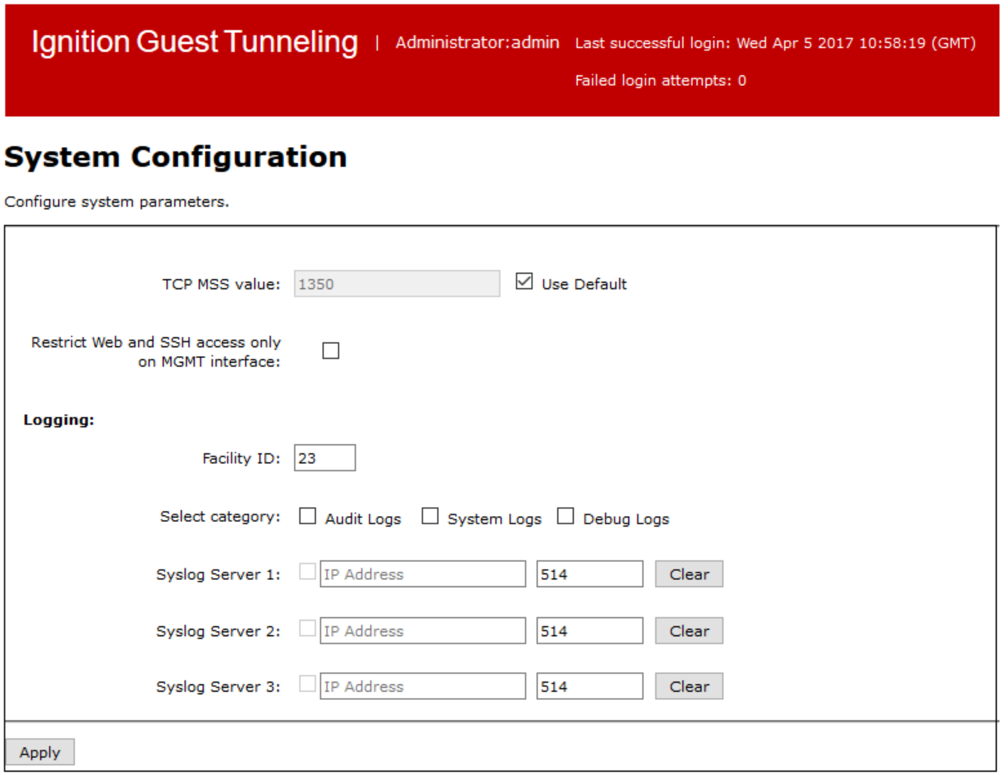
- Audit logs
- System logs
- Debug logs

Before you begin

Ensure that you are logged on to Avaya Identity Engines Ignition Guest Tunneling application.

Procedure

1. Navigate to **System** > **Config**.



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:58:19 (GMT)
Failed login attempts: 0

System Configuration

Configure system parameters.

TCP MSS value: 1350 ☑ Use Default

Restrict Web and SSH access only on MGMT interface: □

Logging:

Facility ID: 23

Select category: □ Audit Logs □ System Logs □ Debug Logs

Syslog Server 1: □ IP Address 514 Clear

Syslog Server 2: □ IP Address 514 Clear

Syslog Server 3: □ IP Address 514 Clear

For information on TCP MSS value, see Configuring Guest Tunneling Appliance on page 67

To log server configuration, user has to configure IP address and Port number of the syslog server. Syslog uses the User Datagram Protocol (UDP), default port 514, for communication.

Note:

By default, none of the logs are enabled. Syslog servers can be individually enabled or disabled.

2. **Configuring Audit Logs:**

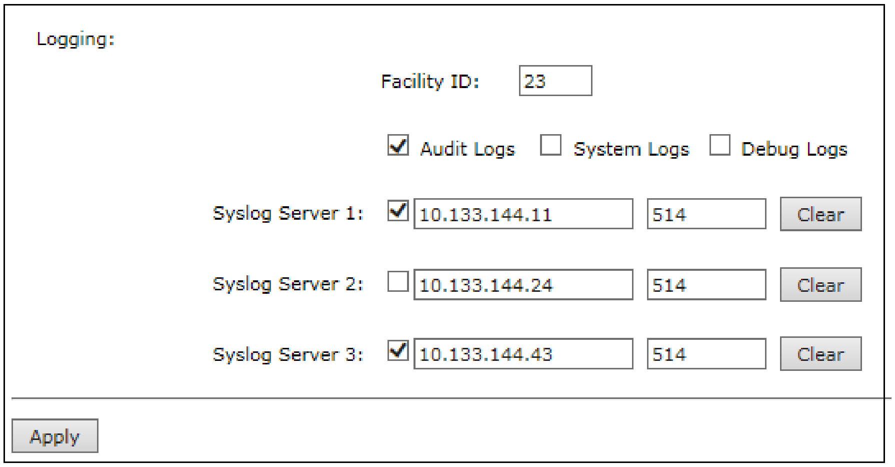
Audit logs are created whenever the administrator modifies any configuration in IGT.

To configure Audit logs,

- Enter the **Facility ID**. By default, the Facility ID is 23 (Local7). The valid range is from 1 to 11 and 16 to 23.

  Valid facilities are: user(1), mail(2), daemon(3), auth(4), syslog(5), lpr(6), news(7), uucp(music), cron(9), authpriv(10), ftp(11), local0 to local7(16-23)
- Select the **Audit Logs** check box
- Enter the **IP Address**
- Enter the **Port number**
- Select the **Syslog Server** check box that need to be configured

- Click **Apply** button



Logging:

Facility ID: 23

☑ Audit Logs □ System Logs □ Debug Logs

Syslog Server 1: ☑ 10.133.144.11 514

Syslog Server 2: □ 10.133.144.24 514

Syslog Server 3: ☑ 10.133.144.43 514

Note:

Administrator can configure one or multiple syslog servers by selecting the check box of the required server that need to be configured.

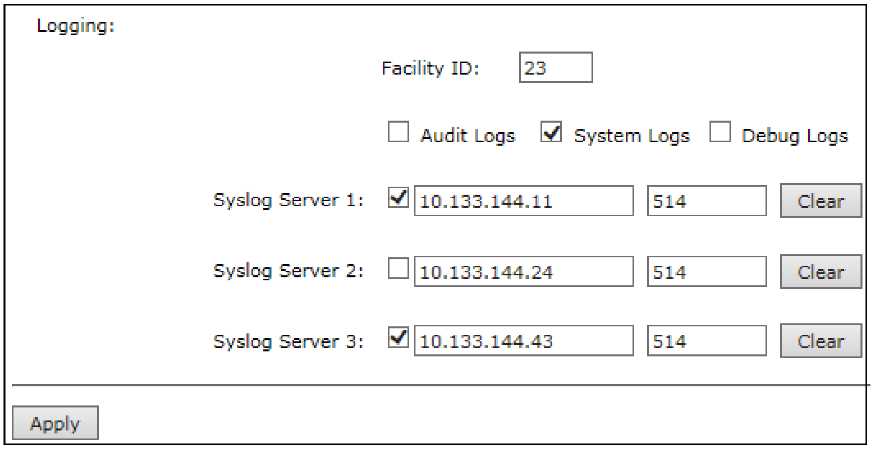
3. **Configuring System Logs:**

   This category of messages logs the system events like Tunnel status Up, Down or AdminDown, Interface status Up/Down.

   To configure System logs,

   - Enter the **Facility ID**. By default, the Facility ID is 23 (Local7). The valid range is from 1 to 11 and 16 to 23.

     Valid facilities are: user(1), mail(2), daemon(3), auth(4), syslog(5), lpr(6), news(7), uucp(music), cron(9), authpriv(10), ftp(11), local0 to local7(16-23)
   - Select the **System Logs** check box
   - Enter the **IP Address**
   - Enter the **Port number**
   - Select the **Syslog Server** check box that need to be configured
   - Click **Apply** button



Logging:

Facility ID: 23

□ Audit Logs ☑ System Logs □ Debug Logs

Syslog Server 1: ☑ 10.133.144.11 514

Syslog Server 2: □ 10.133.144.24 514

Syslog Server 3: ☑ 10.133.144.43 514

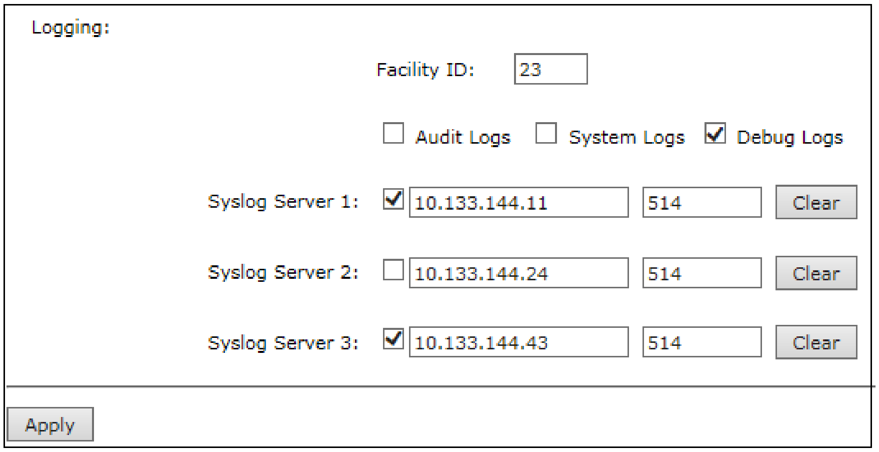
4. **Configuring Debug Logs:**

   This type of logs helps an administrator to get detailed logs for trouble shooting the system. Currently verbose system level logs are sent as part of Debug logs.

   To configure Debug logs,

   - Enter the **Facility ID**. By default, the Facility ID is 23 (Local7). The valid range is from 1 to 11 and 16 to 23.

     Valid facilities are: user(1), mail(2), daemon(3), auth(4), syslog(5), lpr(6), news(7), uucp(music), cron(9), authpriv(10), ftp(11), local0 to local7(16-23)
   - Select the **Debug Logs** check box
   - Enter the **IP Address**
   - Enter the **Port number**
   - Select the **Syslog Server** check box that need to be configured
   - Click **Apply** button



Logging:

Facility ID: 23

□ Audit Logs □ System Logs ☑ Debug Logs

Syslog Server 1: ☑ 10.133.144.11 514

Syslog Server 2: □ 10.133.144.24 514

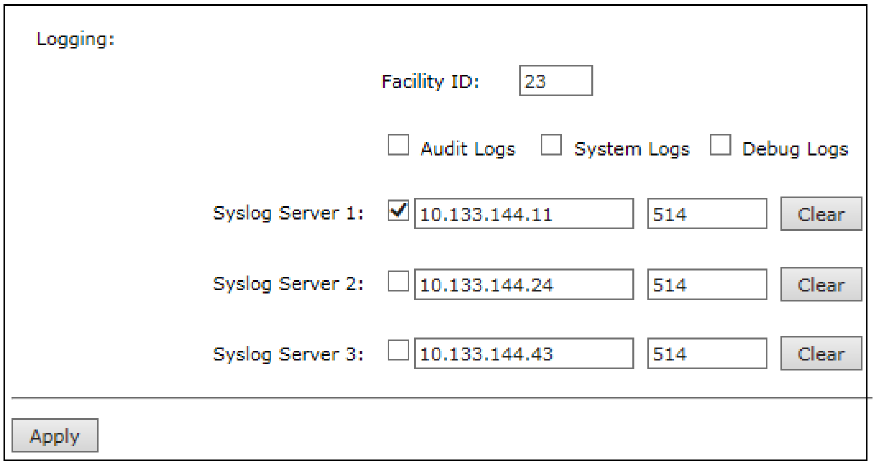
Syslog Server 3: ☑ 10.133.144.43 514

5. **Reset Syslog Configuration:**

   Administrator can clear configuration of individual servers.

To clear configured individual servers,

- Select the **Syslog Server** check box
- Click **Clear** button
- Click **Apply** button



Logging:

Facility ID: 23

□ Audit Logs □ System Logs □ Debug Logs

Syslog Server 1: ☑ 10.133.144.11 514

Syslog Server 2: □ 10.133.144.24 514

Syslog Server 3: □ 10.133.144.43 514

Configuring Guest Tunneling Appliance

Before you begin

- Login to IGT web interface using the default **User ID** and **Password**.

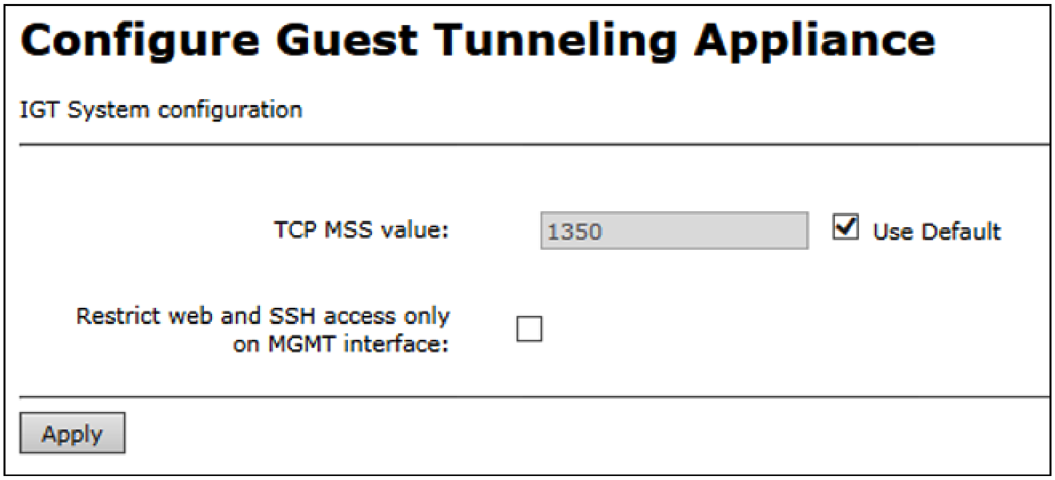
About this task

Use this procedure to perform IGT system configuration. You can configure the TCP Maximum Segment Size (MSS) value and restrict the Web and Secure Shell (SSH) access.

Procedure

1. From the navigation panel, go to **System** > **Config**.

   The system displays the Configure Guest Tunneling Appliance window.



Configure Guest Tunneling Appliance

IGT System configuration

TCP MSS value: 1350 ☑ Use Default

Restrict web and SSH access only on MGMT interface: ☐

2. On the **Configure Guest Tunneling Appliance** window, clear **Use Default** checkbox to enter the **TCP MSS value** in the range between `577 and 1422 bytes`.

   Note:

   By default the **Use Default** checkbox is selected with `1350` as the default TCP MSS value.

3. On the **Configure Guest Tunneling Appliance** window, select **Restrict web and SSH access only on MGMT interface** to block SSH and Web access over IN and OUT Interfaces.
4. Click **Apply** to apply and save.

Taking a backup of the IGT system configuration

About this task

You must take a backup of the IGT system configuration before you make any configuration changes, because when the IGT VM is updated, it is replaced with a new VM.

Caution:

The IGT system backup does not include tunnel and VLAN configuration. For more information on exporting tunnel configuration, see Exporting GRE Tunnel on page 40

Procedure

1. Navigate to **System** > **Backup**.
2. Optionally, Password can be set for back up file. To set the password, select Encrypt back up option and provide the password as required.
3. Click **Export**.

   The Save as dialog appears.
4. Select a location on your local hard disk to save the .zip file.

5. Click **Save**.

Restoring the IGT system configuration

About this task

Restore the IGT system configuration.

Procedure

1. Navigate to **System** > **Restore**.
2. Click **Browse** to select the backed up .zip file from your local hard disk.
3. If back up file is password protected, provide the back up password.
4. Enable **Exclude license** check box if you do not want the license to be imported.
5. Click **Import** to restore the system configuration.

   Note:

   The system automatically reboots after the import.

Viewing the Guest Tunneling System summary and status

Before you begin

- Login to IGT web interface using the default **User ID** and **Password**.

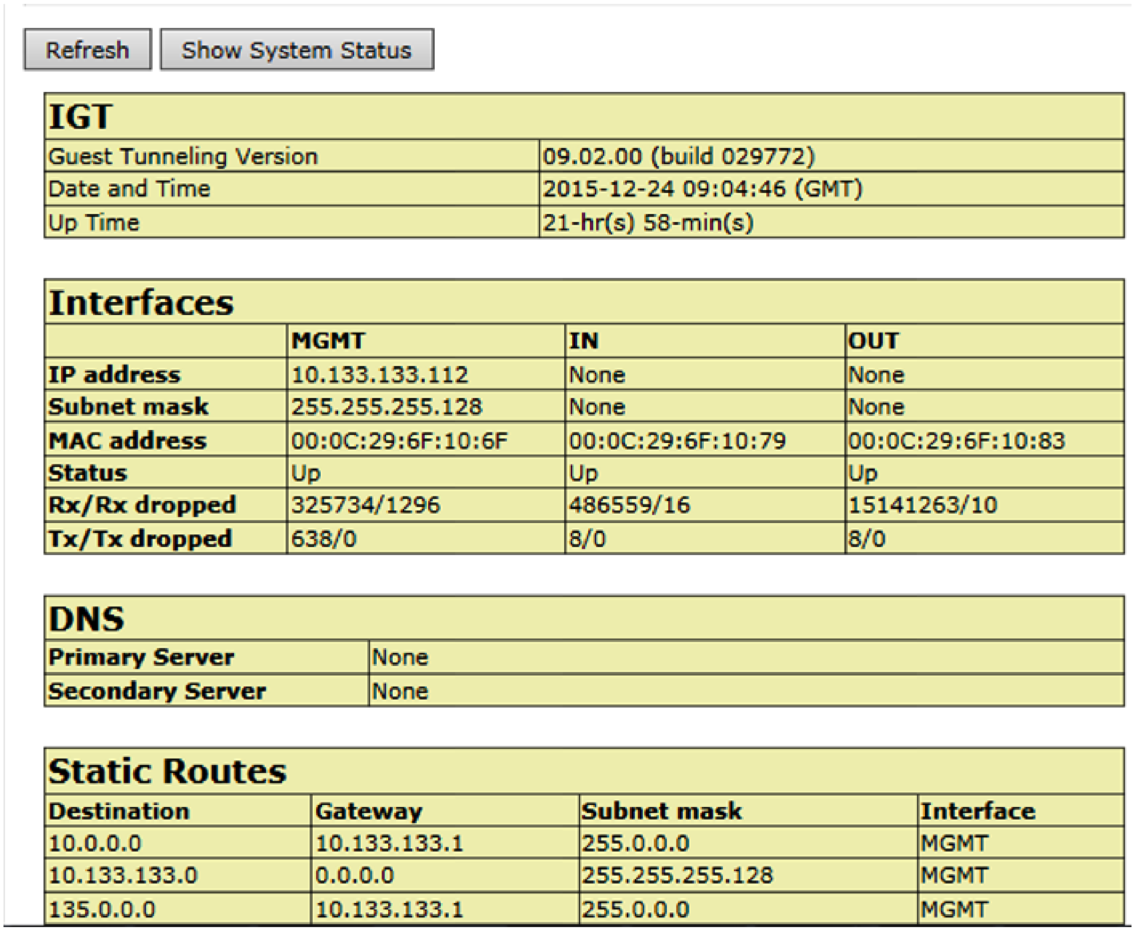
About this task

Use this procedure to view the summary of the IGT configuration and status of the system from the IGT web interface.

Procedure

1. Navigate to **System** > **Status**.

   The system displays the Guest Tunneling System Status page with the summary of IGT configuration.



IGT	
Guest Tunneling Version	09.02.00 (build 029772)
Date and Time	2015-12-24 09:04:46 (GMT)
Up Time	21-hr(s) 58-min(s)

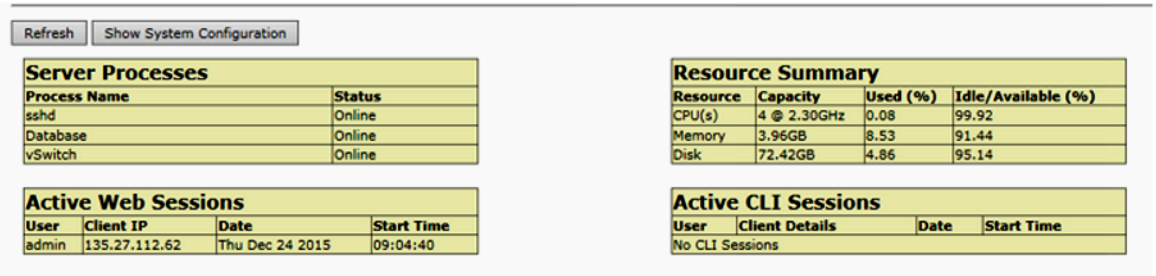
Interfaces			
	MGMT	**IN**	**OUT**
IP address	10.133.133.112	None	None
Subnet mask	255.255.255.128	None	None
MAC address	00:0C:29:6F:10:6F	00:0C:29:6F:10:79	00:0C:29:6F:10:83
Status	Up	Up	Up
Rx/Rx dropped	325734/1296	486559/16	15141263/10
Tx/Tx dropped	638/0	8/0	8/0

DNS	
Primary Server	None
Secondary Server	None

Static Routes			
Destination	**Gateway**	**Subnet mask**	**Interface**
10.0.0.0	10.133.133.1	255.0.0.0	MGMT
10.133.133.0	0.0.0.0	255.255.255.128	MGMT
135.0.0.0	10.133.133.1	255.0.0.0	MGMT

2. On the **Guest Tunneling System Status** page, click the **Show System Status** button.

   The system displays the Guest Tunneling System Status with the summary of IGT system status.



Server Processes	
Process Name	**Status**
sshd	Online
Database	Online
vSwitch	Online

Resource Summary			
Resource	**Capacity**	**Used (%)**	**Idle/Available (%)**
CPU(s)	4 @ 2.30GHz	0.08	99.92
Memory	3.96GB	8.53	91.44
Disk	72.42GB	4.86	95.14

Active Web Sessions			
User	**Client IP**	**Date**	**Start Time**
admin	135.27.112.62	Thu Dec 24 2015	09:04:40

Active CLI Sessions			
User	**Client Details**	**Date**	**Start Time**
No CLI Sessions			

3. **(Optional)** Click the **Show System Configuration** button to view the summary of IGT configuration.

4. **(Optional)** Click **Refresh** to refresh the system status and IGT configuration.

Troubleshooting the Guest Tunneling Appliance

Before you begin

- Login to IGT web interface using the default **User ID** and **Password**.

About this task

Use this procedure to diagnose and troubleshoot problems in the IGT system. Perform this procedure to collect logs, to configure data, and to capture packets.

Note:

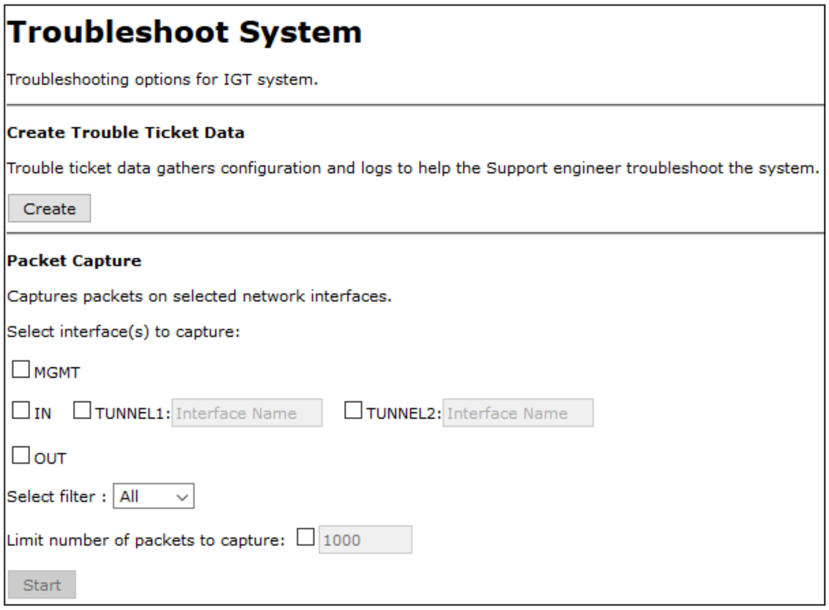
In the event of a fault in IGT system, generate a trouble ticket file that Avaya support staff can use to diagnose the problem.

For more troubleshooting information on the Avaya Identity Engines Ignition Guest Tunneling, see Troubleshooting on page 97.

Procedure

1. Navigate to **System** > **Troubleshoot**.

   The system displays the Troubleshoot Guest Tunneling Appliance page.

   Troubleshoot System

   Troubleshooting options for IGT system.

   Create Trouble Ticket Data

   Trouble ticket data gathers configuration and logs to help the Support engineer troubleshoot the system.

   Packet Capture

   Captures packets on selected network interfaces.

   Select interface(s) to capture:

   □ MGMT

   □ IN □ TUNNEL1: Interface Name □ TUNNEL2: Interface Name

   □ OUT

   Select filter : All

   Limit number of packets to capture: □ 1000

2. On the **Troubleshoot Guest Tunneling Appliance** page, click **Create** to archive logs, configuration, and version information.

   The system displays message to open or save `<IGT_TroubleTicket_IGT IP adress_YYYYMMDD_HHMMSS.zip>` file.

   Note:

   Trouble Ticket data archives the system logs.

Troubleshooting IGT using Packet Capture

About this task

Administrator can troubleshoot IGT system by capturing and analyzing network packets.

For more troubleshooting information and answers to what to do if you encounter error while using Avaya Identity Engines Ignition Guest Tunneling, see Troubleshooting on page 97.

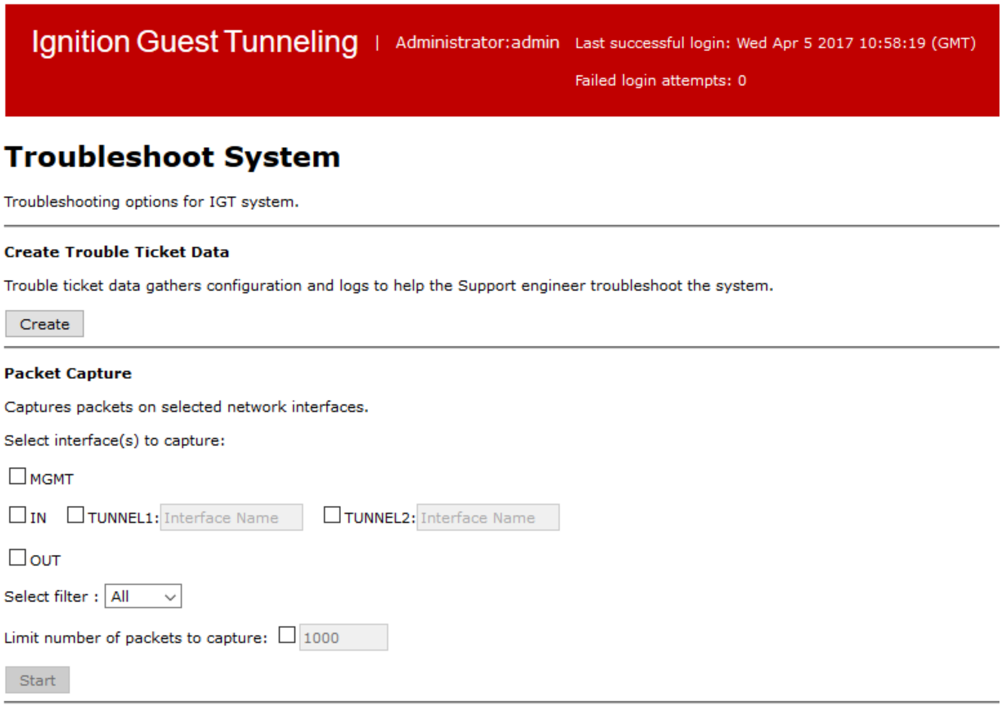
Before you begin

- Login to IGT Web interface using the Admin credentials.

Procedure

1. From the navigation panel, go to **System** > **Troubleshoot**.

   System displays the Troubleshoot Guest Tunneling Appliance page.



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:58:19 (GMT)

Failed login attempts: 0

Troubleshoot System

Troubleshooting options for IGT system.

Create Trouble Ticket Data

Trouble ticket data gathers configuration and logs to help the Support engineer troubleshoot the system.

Create

Packet Capture

Captures packets on selected network interfaces.

Select interface(s) to capture:

□ MGMT

□ IN □ TUNNEL1: Interface Name □ TUNNEL2: Interface Name

□ OUT

Select filter : All

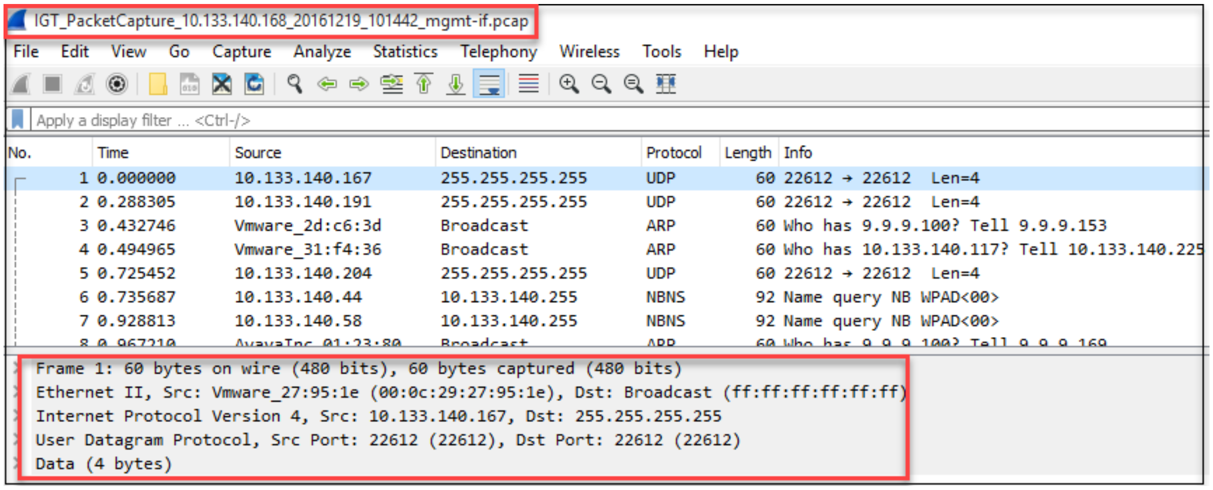
Limit number of packets to capture: □ 1000

Start

2. On the **Troubleshoot Guest Tunneling Appliance** page, select one or more interface to capture packets from the given choices:
   - MGMT
   - IN
   - TUNNEL1
   - TUNNEL2
   - OUT

Find below some sample captures files opened with Wireshark application:

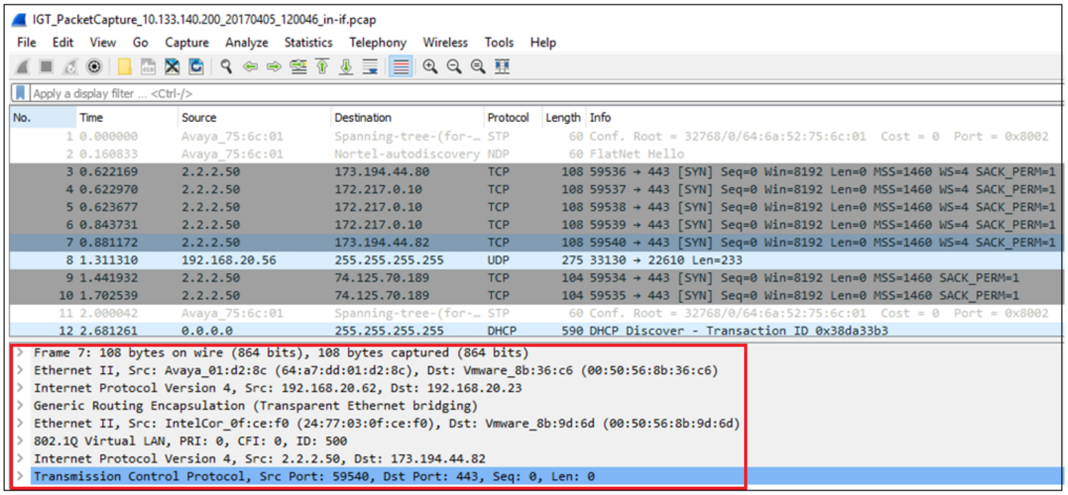
Packet Captured in MGMT Interface:


IGT_PacketCapture_10.133.140.168_20161219_101442_mgmt-if.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source             Destination       Protocol  Length Info
    1 0.000000  10.133.140.167     255.255.255.255   UDP           60 22612 → 22612  Len=4
    2 0.288305  10.133.140.191     255.255.255.255   UDP           60 22612 → 22612  Len=4
    3 0.432746  Vmware_2d:c6:3d    Broadcast         ARP           60 Who has 9.9.9.100? Tell 9.9.9.153
    4 0.494965  Vmware_31:f4:36    Broadcast         ARP           60 Who has 10.133.140.117? Tell 10.133.140.225
    5 0.725452  10.133.140.204     255.255.255.255   UDP           60 22612 → 22612  Len=4
    6 0.735687  10.133.140.44      10.133.140.255    NBNS          92 Name query NB WPAD<00>
    7 0.928813  10.133.140.58      10.133.140.255    NBNS          92 Name query NB WPAD<00>
    8 0.967210  AvayaInc_01:23:80  Broadcast         ARP           60 Who has 9.9.9.100? Tell 9.9.9.169
```

```
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Vmware_27:95:1e (00:0c:29:27:95:1e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.133.140.167, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 22612 (22612), Dst Port: 22612 (22612)
Data (4 bytes)
```

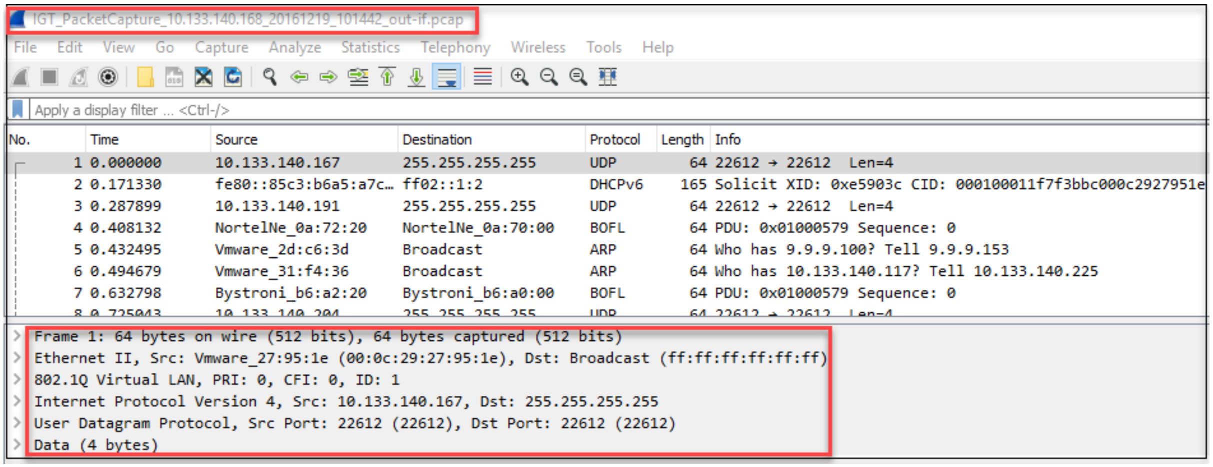
Packet Captured in IN Interface:


IGT_PacketCapture_10.133.140.200_20170405_120046_in-if.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source          Destination          Protocol Length Info
    1 0.000000  Avaya_75:6c:01  Spanning-tree-(for-… STP          60 Conf. Root = 32768/0/64:6a:52:75:6c:01  Cost = 0  Port = 0x8002
    2 0.160833  Avaya_75:6c:01  Nortel-autodiscovery NDP          60 FlatNet Hello
    3 0.622169  2.2.2.50        173.194.44.80        TCP         108 59536 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    4 0.622970  2.2.2.50        172.217.0.10         TCP         108 59537 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    5 0.623677  2.2.2.50        172.217.0.10         TCP         108 59538 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    6 0.843731  2.2.2.50        172.217.0.10         TCP         108 59539 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    7 0.881172  2.2.2.50        173.194.44.82        TCP         108 59540 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    8 1.311310  192.168.20.56   255.255.255.255      UDP         275 33130 → 22610 Len=233
    9 1.441932  2.2.2.50        74.125.70.189        TCP         104 59534 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
   10 1.702539  2.2.2.50        74.125.70.189        TCP         104 59535 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
   11 2.000042  Avaya_75:6c:01  Spanning-tree-(for-… STP          60 Conf. Root = 32768/0/64:6a:52:75:6c:01  Cost = 0  Port = 0x8002
   12 2.681261  0.0.0.0         255.255.255.255      DHCP        590 DHCP Discover - Transaction ID 0x38da33b3
```

```
> Frame 7: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
> Ethernet II, Src: Avaya_01:d2:8c (64:a7:dd:01:d2:8c), Dst: Vmware_8b:36:c6 (00:50:56:8b:36:c6)
> Internet Protocol Version 4, Src: 192.168.20.62, Dst: 192.168.20.23
> Generic Routing Encapsulation (Transparent Ethernet bridging)
> Ethernet II, Src: IntelCor_0f:ce:f0 (24:77:03:0f:ce:f0), Dst: Vmware_8b:9d:6d (00:50:56:8b:9d:6d)
> 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 500
> Internet Protocol Version 4, Src: 2.2.2.50, Dst: 173.194.44.82
> Transmission Control Protocol, Src Port: 59540, Dst Port: 443, Seq: 0, Len: 0
```

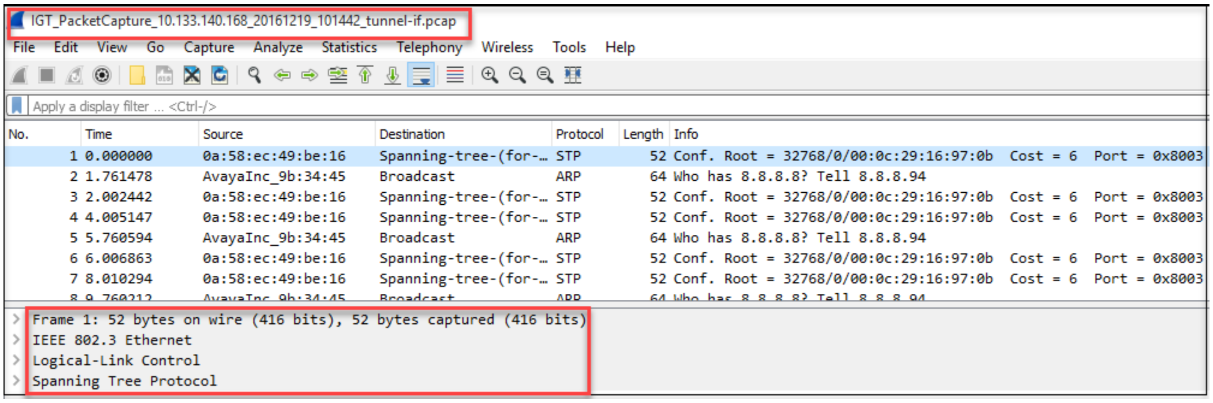
Packet Captured in OUT Interface:


IGT_PacketCapture_10.133.140.168_20161219_101442_out-if.pcap
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

```
No.     Time       Source                Destination       Protocol  Length Info
      1 0.000000   10.133.140.167        255.255.255.255   UDP          64 22612 → 22612  Len=4
      2 0.171330   fe80::85c3:b6a5:a7c…  ff02::1:2         DHCPv6      165 Solicit XID: 0xe5903c CID: 000100011f7f3bbc000c2927951e
      3 0.287899   10.133.140.191        255.255.255.255   UDP          64 22612 → 22612  Len=4
      4 0.408132   NortelNe_0a:72:20     NortelNe_0a:70:00 BOFL         64 PDU: 0x01000579 Sequence: 0
      5 0.432495   Vmware_2d:c6:3d       Broadcast         ARP          64 Who has 9.9.9.100? Tell 9.9.9.153
      6 0.494679   Vmware_31:f4:36       Broadcast         ARP          64 Who has 10.133.140.117? Tell 10.133.140.225
      7 0.632798   Bystroni_b6:a2:20     Bystroni_b6:a0:00 BOFL         64 PDU: 0x01000579 Sequence: 0
      8 0.725043   10.133.140.204        255.255.255.255   UDP          64 22612 → 22612  Len=4
```

```
> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
> Ethernet II, Src: Vmware_27:95:1e (00:0c:29:27:95:1e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1
> Internet Protocol Version 4, Src: 10.133.140.167, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 22612 (22612), Dst Port: 22612 (22612)
> Data (4 bytes)
```

Packet Captured in Tunnel Interface:

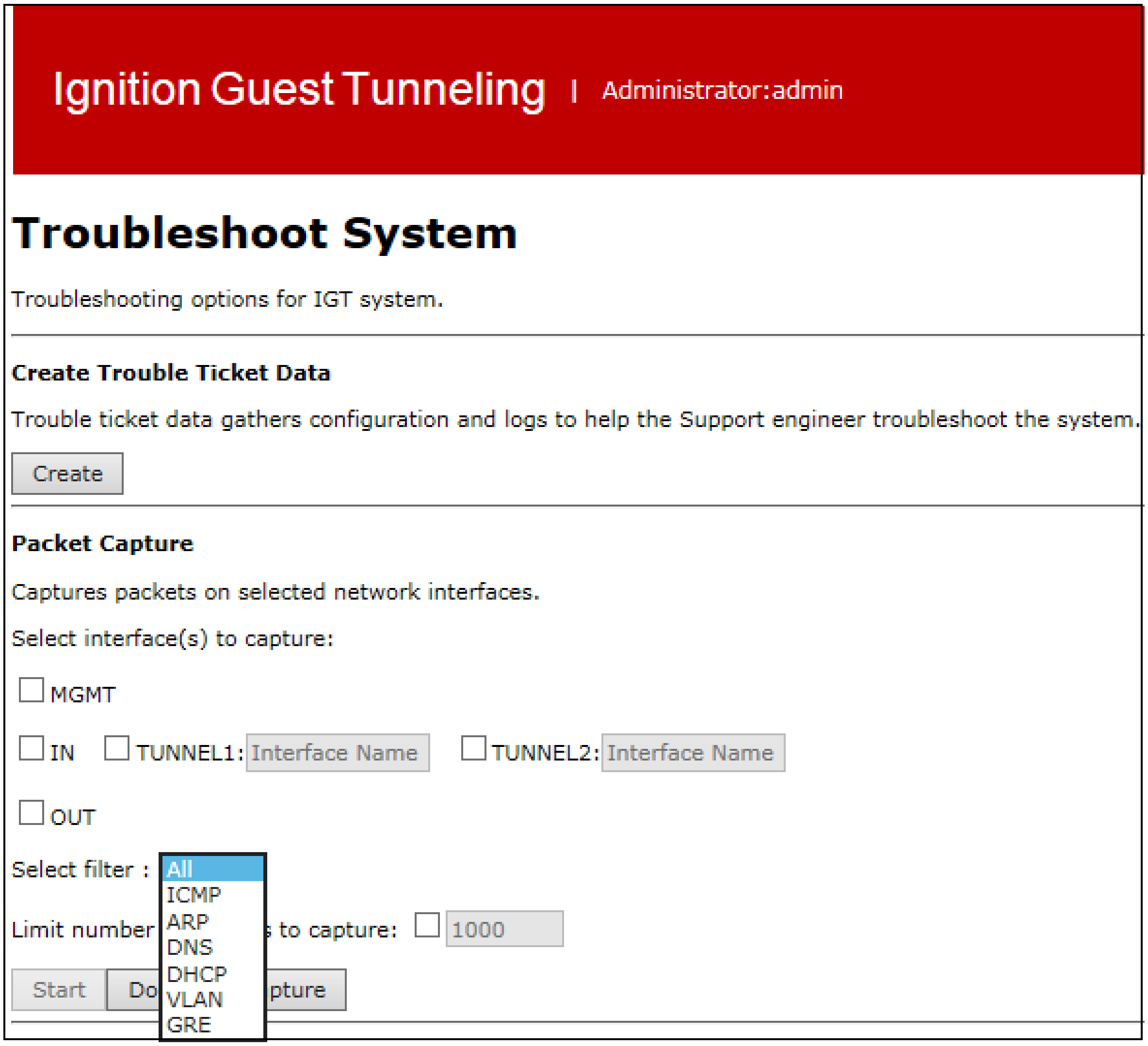

IGT_PacketCapture_10.133.140.168_20161219_101442_tunnel-if.pcap
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

```
No.     Time       Source              Destination            Protocol  Length Info
      1 0.000000   0a:58:ec:49:be:16   Spanning-tree-(for-…   STP          52 Conf. Root = 32768/0/00:0c:29:16:97:0b  Cost = 6  Port = 0x8003
      2 1.761478   AvayaInc_9b:34:45   Broadcast              ARP          64 Who has 8.8.8.8? Tell 8.8.8.94
      3 2.002442   0a:58:ec:49:be:16   Spanning-tree-(for-…   STP          52 Conf. Root = 32768/0/00:0c:29:16:97:0b  Cost = 6  Port = 0x8003
      4 4.005147   0a:58:ec:49:be:16   Spanning-tree-(for-…   STP          52 Conf. Root = 32768/0/00:0c:29:16:97:0b  Cost = 6  Port = 0x8003
      5 5.760594   AvayaInc_9b:34:45   Broadcast              ARP          64 Who has 8.8.8.8? Tell 8.8.8.94
      6 6.006863   0a:58:ec:49:be:16   Spanning-tree-(for-…   STP          52 Conf. Root = 32768/0/00:0c:29:16:97:0b  Cost = 6  Port = 0x8003
      7 8.010294   0a:58:ec:49:be:16   Spanning-tree-(for-…   STP          52 Conf. Root = 32768/0/00:0c:29:16:97:0b  Cost = 6  Port = 0x8003
      8 9.760212   AvayaInc_9b:34:45   Broadcast              ARP          64 Who has 8.8.8.8? Tell 8.8.8.94
```

```
> Frame 1: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
> IEEE 802.3 Ethernet
> Logical-Link Control
> Spanning Tree Protocol
```

- Administrator can capture packets on interfaces MGMT, IN, OUT and on any two tunnel interfaces (For Example, gre0, gre1, gre2......gre(n). where n is the maximum supported tunnels). Tunnel name has to be specified if tunnel interface is selected and the name to be specified here is the "Interface" name specified in the "Tunnel ---> Status" page for each remote endpoint.
- All interfaces can capture packets independently. i.e. for e.g. it is not required to enable IN or OUT interface, if packets are to be captured only on the tunnel interfaces.
- At any point of time, only one capture can be triggered.
- Administrator should not alter the network interfaces of IGT and in the ESXi vSwitch when packet capture is being done.
- While Packet capturing, if multiple interfaces are selected, the download capture will be in a zip format (containing in-if.pcap, out-if.pcap, tunnel-if.pcap files) having all selected interfaces captures.

3. The protocol filter provided can be used to further narrow down the type of packets to be captured. The Supported filters are ALL, ICMP, ARP, DNS, DHCP, VLAN and GRE.



Ignition Guest Tunneling | Administrator:admin

Troubleshoot System

Troubleshooting options for IGT system.

Create Trouble Ticket Data

Trouble ticket data gathers configuration and logs to help the Support engineer troubleshoot the system.

Packet Capture

Captures packets on selected network interfaces.

Select interface(s) to capture:

□ MGMT

□ IN □ TUNNEL1: Interface Name □ TUNNEL2: Interface Name

□ OUT

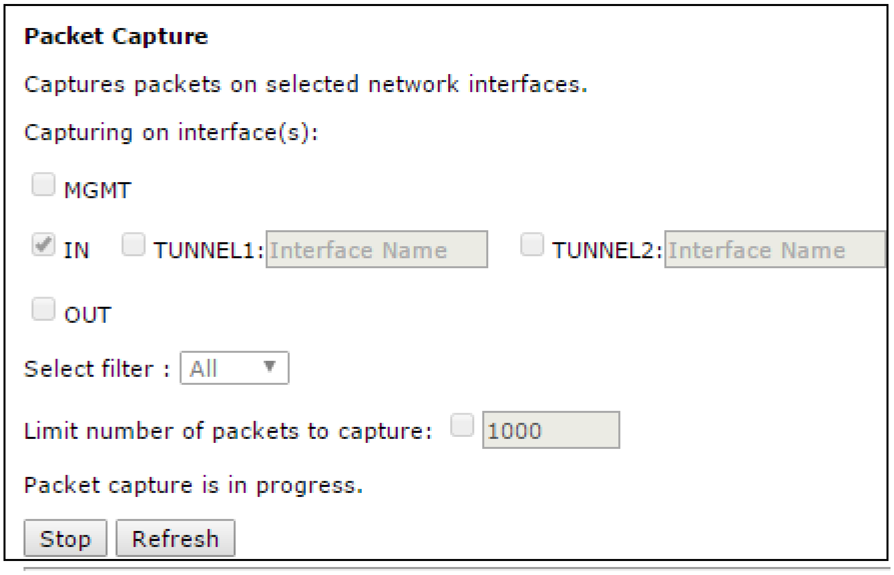
Select filter : All

Limit number s to capture: □ 1000

4. Administrator can set the limit on the number of packets to be captured. By default, the capture runs till it is stopped or it reaches the system limit. Select the Check box and set the limit.

   The limit that can be entered for the Packet Capture count ranges from 1 to 1000000. If enabled the count, it will stop capturing at that specified limit.

5. Click **Stop** to stop the packet capture.



Packet Capture

Captures packets on selected network interfaces.

Capturing on interface(s):

□ MGMT

☑ IN □ TUNNEL1: Interface Name □ TUNNEL2: Interface Name

□ OUT

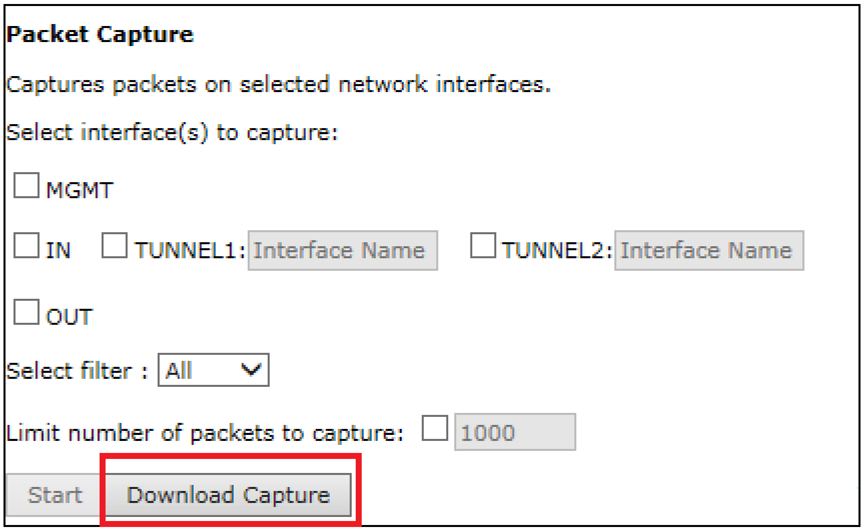
Select filter : All

Limit number of packets to capture: □ 1000

Packet capture is in progress.

6. Click **Download Capture** to download the captured packet in `IGT_PacketCapture_IPAddress_Date_Timestamp.zip` file format.

   The downloaded capture file will be copied to the default browser location which is the c:\\ downloads.



Packet Capture

Captures packets on selected network interfaces.

Select interface(s) to capture:

□ MGMT

□ IN □ TUNNEL1: Interface Name □ TUNNEL2: Interface Name

□ OUT

Select filter : All

Limit number of packets to capture: □ 1000

Only if packets are captured on one interface, the downloaded file will be in pcap format. In case multiple interfaces are selected, each interface packets are captured in the .pcap format and zipped together as a .zip file for download.

Note:

- The `IGT_PacketCapture_IPAddress_Date_Timestamp.zip` file contains the Packet Capture files of the selected interface in `<interface>-if.pcap` format.

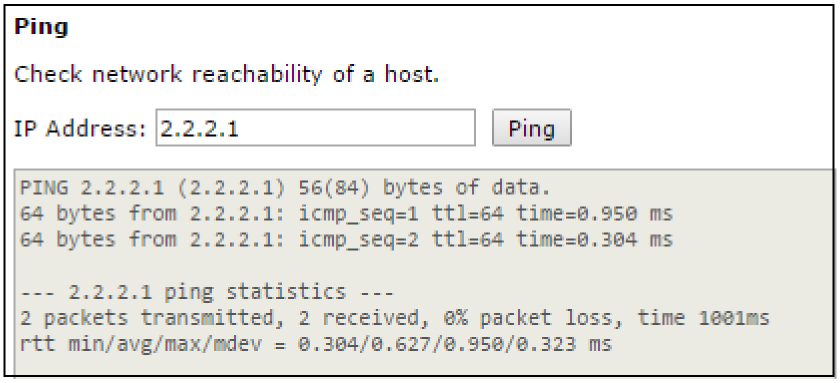
- The system starts capturing packets on the selected interface. Capture continues to run in back ground even if the user moved away from troubleshoot page or logged out of current session.
- The limit of packets is on a per interface basis.
- IGT will wait for capture to reach the specified limit to reach on each interface before stopping the capture.
- Packet captured on TUNNEL1 and TUNNEL2 are part of single capture file tunnel-if.pcap.
- The tunnel interfaces will only contain GRE de-capsulated packets. If the Administrator wants to view the GRE headers, then the packet capture needs to be enabled on the IN interface.
- If GRE filter is selected, then in a normal guest traffic, these packets will only be seen on the IN interface and not on Tunnel interfaces.

Please find below some real world debugging scenarios where Packet Capture feature can be used:

- **If Client is not getting IP address**, Start the capture in IN and OUT interfaces and check for the filter on DHCP exchange packets.
- **Monitor specific Guest user traffic**: Start the capture on IN and OUT interfaces. On the IN capture, filter for specific guest user packets (based on Guest IP address) and verify whether the packets are GRE encapsulated. On the OUT capture, filter for the same guest user packets (based on Guest IP address) and verify whether the packets are plain packets i.e. without GRE encapsulation.
- **Monitor specific Guest VLAN traffic**: Start the capture on IN and OUT interfaces. On the IN capture, filter for specific guest user packets (based on Guest IP address) and verify whether the packets are GRE encapsulated and that the inner client packets are VLAN tagged. Also, on the OUT capture, trace the same client packets and verify the packets are without GRE encapsulation. The client packets on the OUT interface will be tagged or not based on whether IGT is configured to remove the tag and send or not.

Ping

To check the network reachability of a host, enter the **IP address** and click **Ping** button.



Ping

Check network reachability of a host.

IP Address: 2.2.2.1

```
PING 2.2.2.1 (2.2.2.1) 56(84) bytes of data.
64 bytes from 2.2.2.1: icmp_seq=1 ttl=64 time=0.950 ms
64 bytes from 2.2.2.1: icmp_seq=2 ttl=64 time=0.304 ms

--- 2.2.2.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.304/0.627/0.950/0.323 ms
```

Note:

Ping support from console can be used if the WebUI is not reachable. For more information, see Verifying the IGT connectivity - Troubleshooting on page 97

Rebooting Guest Tunneling Appliance

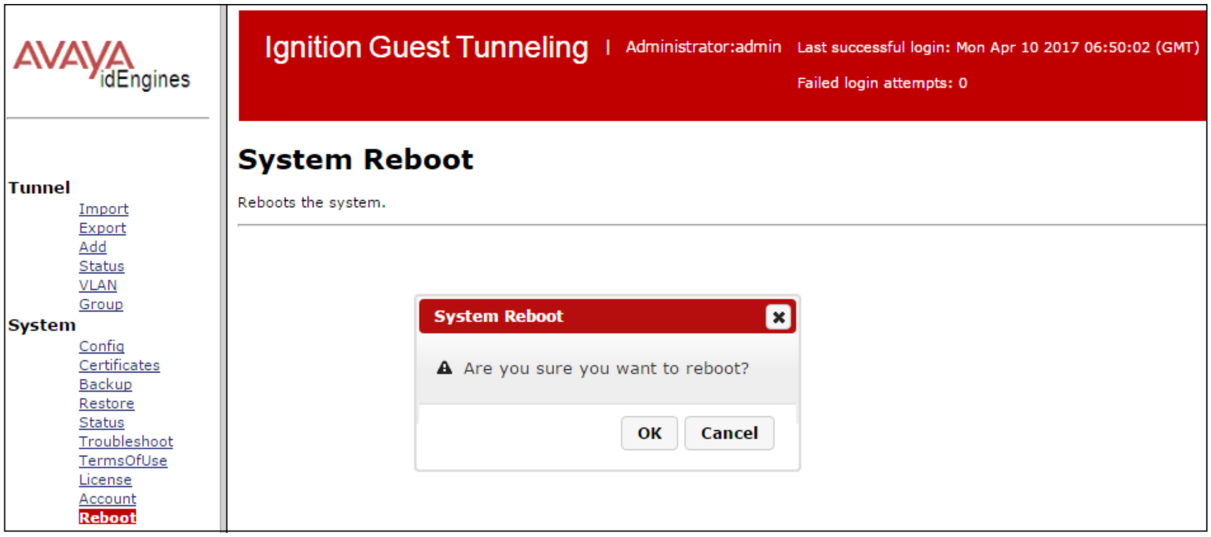
About this task

Use this procedure to reboot Guest Tunneling Appliance.

Procedure

1. On the IGT web interface, navigate to **System** > **Reboot**.

   The system displays System Reboot pop-up window.



Ignition Guest Tunneling | Administrator:admin Last successful login: Mon Apr 10 2017 06:50:02 (GMT)

Failed login attempts: 0

System Reboot

Reboots the system.

System Reboot

Are you sure you want to reboot?

2. On the **Reboot** pop-up window, click **Ok** to reboot the Guest Tunneling Appliance.
3. **(Optional)** Click **Cancel** to cancel the system reboot.

Logging out of Guest Tunneling Appliance

About this task

Logout from Guest Tunneling appliance.

Procedure

Navigate to **System** > **Logout**.

The system logs you out and displays the **Guest Tunneling Appliance** login page.

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 a backup of the IGT system configuration on page 68.
- Take a backup of the Tunnel Configuration of your current version. For more information, see Exporting GRE Tunnel on page 40.

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 the IGT system configuration on page 69.

   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 39.

   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.

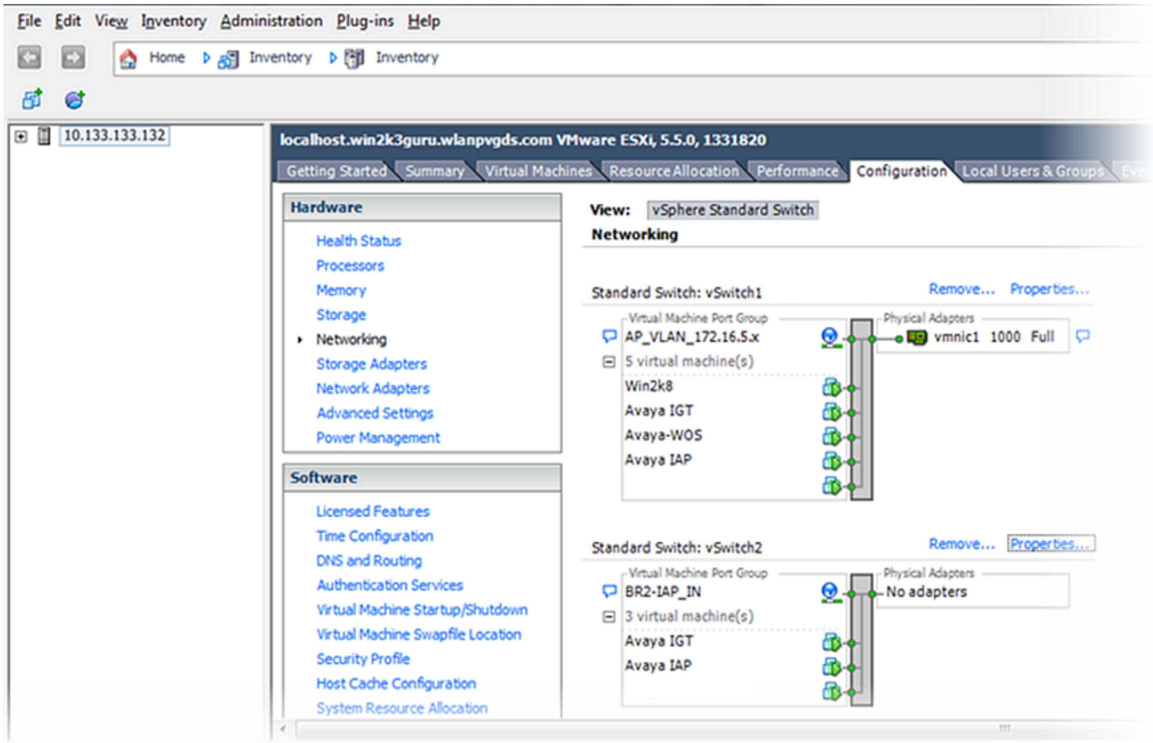
Before you begin

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

Procedure

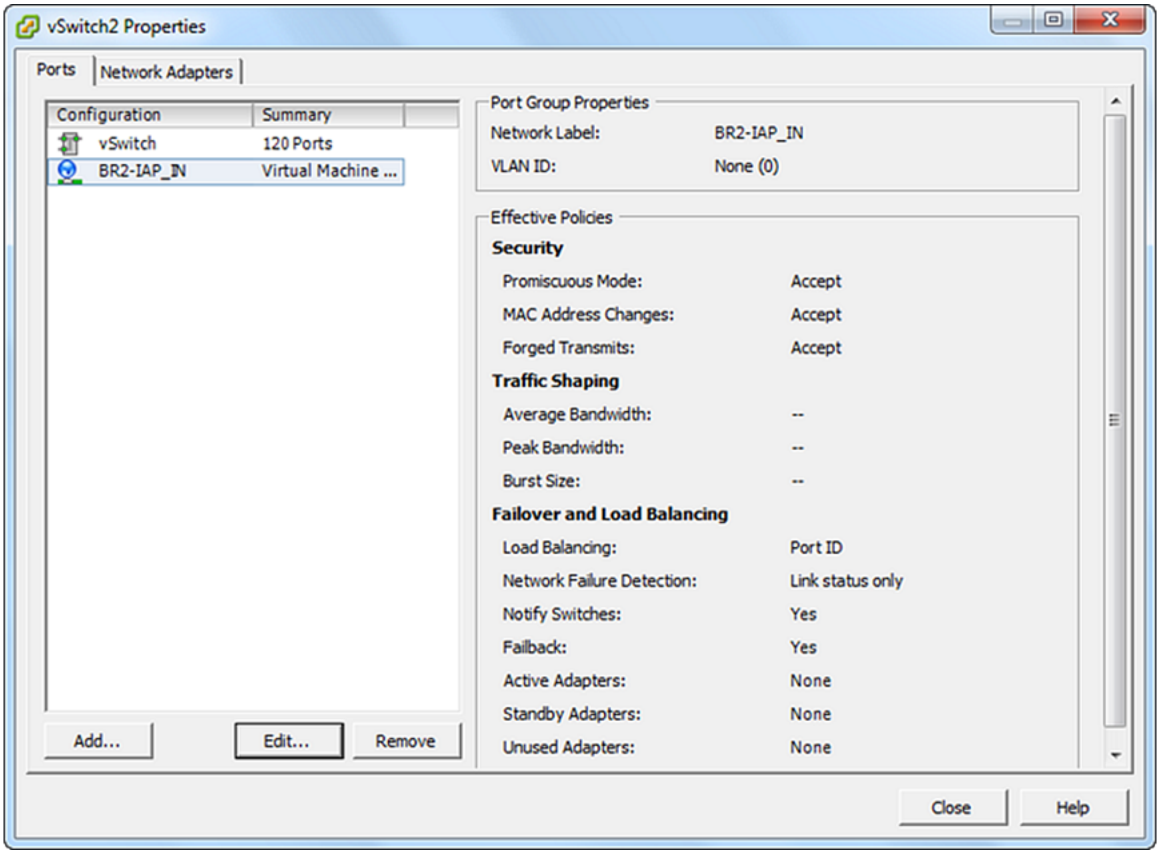
1. Navigate to **Configuration** tab in **vSphere Client**.
2. Click **Networking** in the **Hardware** section.

   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**.



Configuration	Summary
vSwitch	120 Ports
BR2-IAP_IN	Virtual Machine ...

Port Group Properties

Network Label: BR2-IAP_IN

VLAN ID: None (0)

Effective Policies

Security

Promiscuous Mode:	Accept
MAC Address Changes:	Accept
Forged Transmits:	Accept

Traffic Shaping

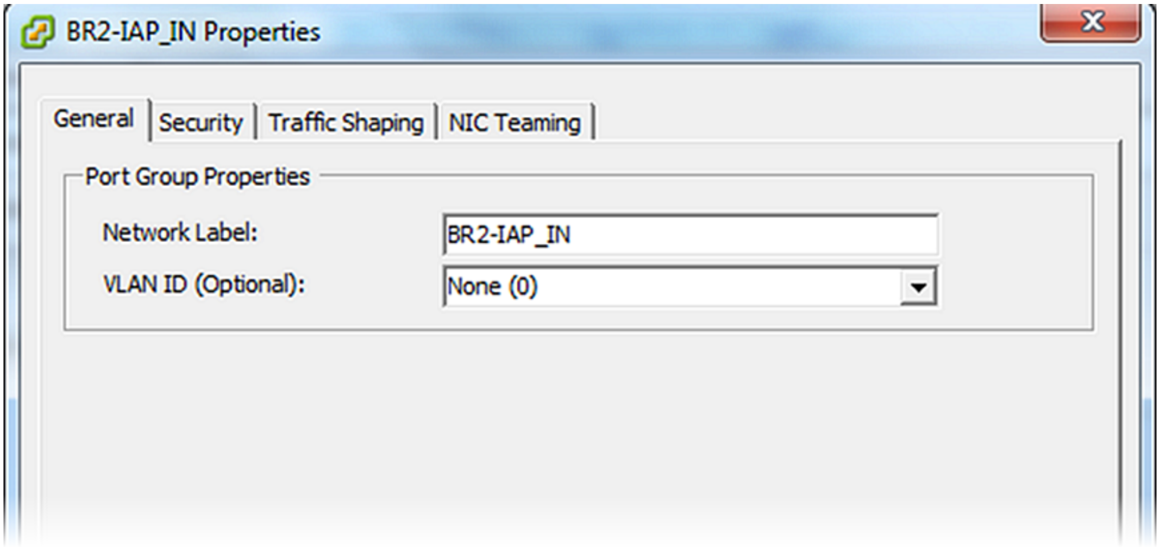
Average Bandwidth:	--
Peak Bandwidth:	--
Burst Size:	--

Failover and Load Balancing

Load Balancing:	Port ID
Network Failure Detection:	Link status only
Notify Switches:	Yes
Failback:	Yes
Active Adapters:	None
Standby Adapters:	None
Unused Adapters:	None

The interface properties window displays.

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



Port Group Properties

Network Label: BR2-IAP_IN

VLAN ID (Optional): None (0)

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**.
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 34.

   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 34.

    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 34.
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**.
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 36.

Configuring Static VLANs

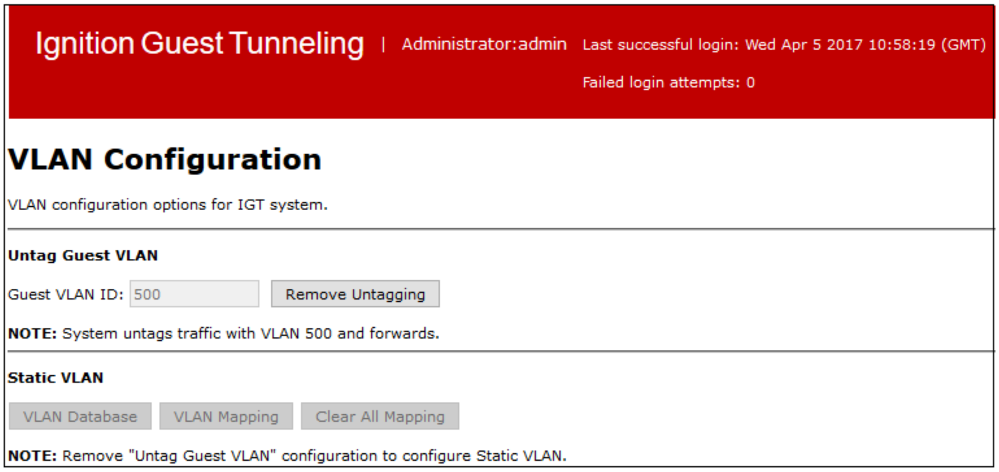
About this task

Administrator can statically configure VLAN(s) on a tunnel on the system to allow the traffic related to the configured VLAN(s) to pass through the tunnel.

Procedure

1. After logging into IGT, navigate to **Tunnel** > **VLAN** .

   The **Static VLAN configuration** page looks like below:



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:58:19 (GMT)
Failed login attempts: 0

VLAN Configuration

VLAN configuration options for IGT system.

Untag Guest VLAN

Guest VLAN ID: 500 Remove Untagging

NOTE: System untags traffic with VLAN 500 and forwards.

Static VLAN

VLAN Database VLAN Mapping Clear All Mapping

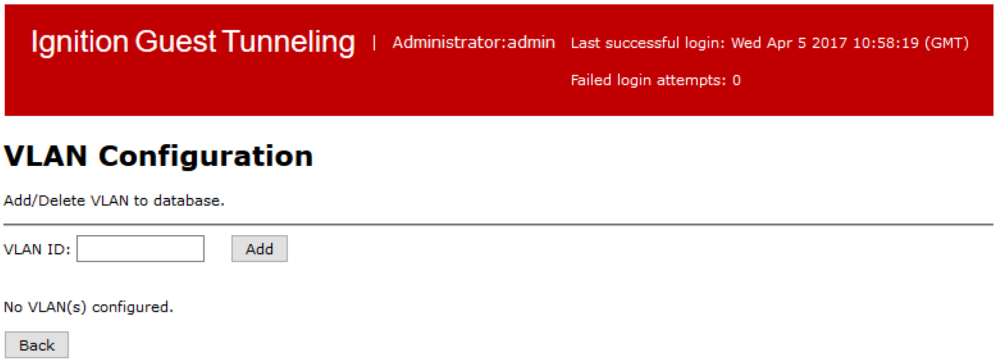
NOTE: Remove "Untag Guest VLAN" configuration to configure Static VLAN.

Note:

The Administrator can either use the **Untag VLAN** feature or the **Static VLAN** feature at any given point of time but not both of them together.

Click on **Clear All Mapping** button to clear all VLAN mappings.

2. Administrator can add or delete VLANs to the IGT VLAN database. Click **VLAN Database** to perform these operations. The below window gets displayed:



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:58:19 (GMT)
Failed login attempts: 0

VLAN Configuration

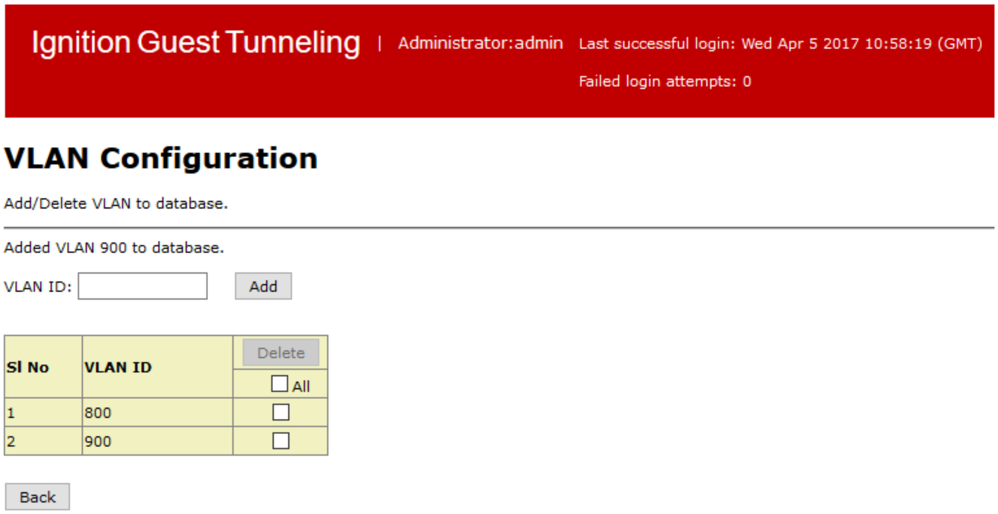
Add/Delete VLAN to database.

VLAN ID: Add

No VLAN(s) configured.

Back

   To add a VLAN, enter the VLAN number in the **VLAN ID** field and click **Add** button. If successfully added, "Added VLAN <vlan id> to database." is seen on the screen. If the addition fails, appropriate error message is shown on the screen. For example, enter the VLAN ID 800 and Click **Add** . Similarly enter the VLAN ID 900 and Click **Add** and the window with the added two VLANs is dispalyed as below:



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:58:19 (GMT)

Failed login attempts: 0

VLAN Configuration

Add/Delete VLAN to database.

Added VLAN 900 to database.

VLAN ID: Add

Sl No	VLAN ID	Delete ☐ All
1	800	☐
2	900	☐

Note:

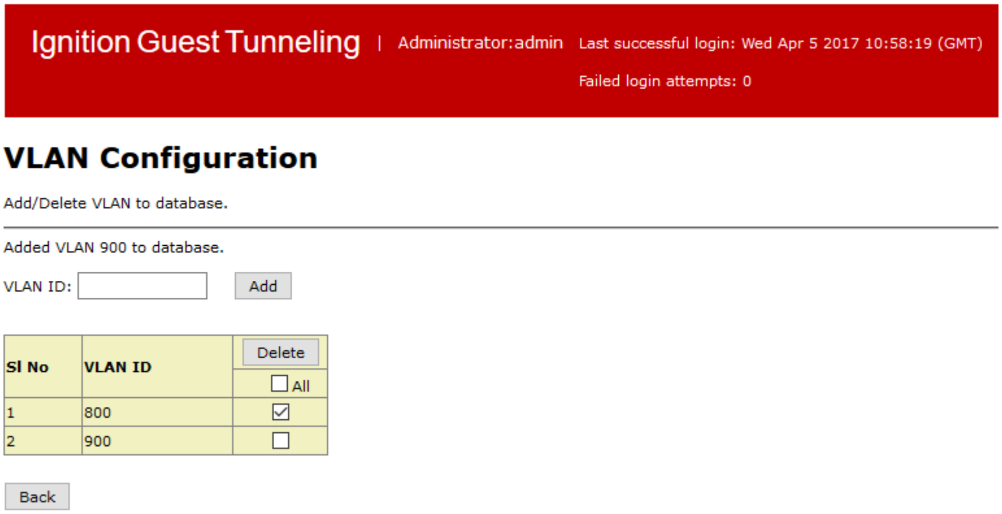
The maximum number of VLAN IDs that can be added is limited to 15.

Click the **Back** button to return back to the VLAN landing page.

3. To delete the VLAN ID from the list, select the required VLAN check box and click **Delete** button. If a VLAN is deleted from the VLAN-Database, the tunnel(s) will reflect the change by removing the deleted VLAN from the tunnel(s) if exist.

   This operation removes VLAN from database and flush mapped tunnels.

   The **All** button can be used to remove all the VLANs from the system and their mappings to tunnels.



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:58:19 (GMT)

Failed login attempts: 0

VLAN Configuration

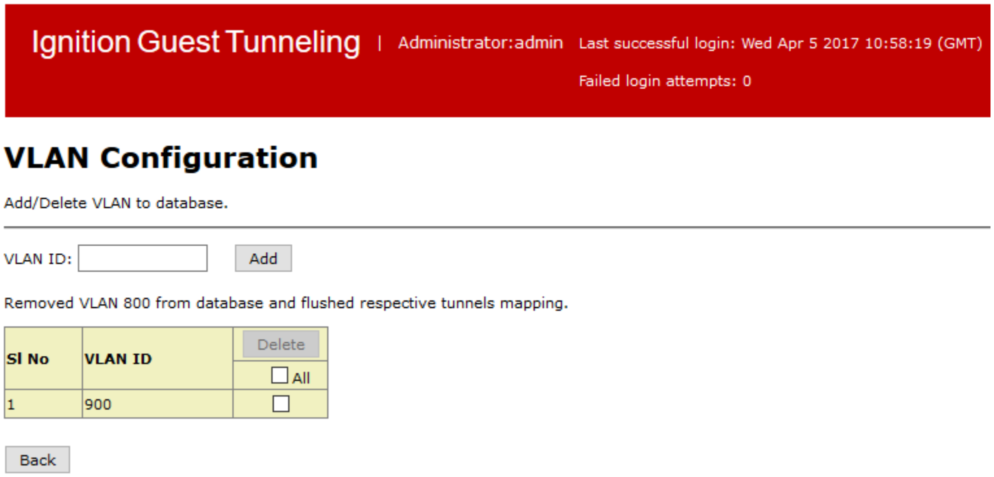
Add/Delete VLAN to database.

Added VLAN 900 to database.

VLAN ID: Add

Sl No	VLAN ID	Delete ☐ All
1	800	☑
2	900	☐

System will prompt for confirming the deletion. Click **Yes** button to delete. Once a VLAN ID is deleted, a confirmation message is displayed as shown below (For example, deleting VLAN ID 800):



Last successful login: Wed Apr 5 2017 10:58:19 (GMT)
Failed login attempts: 0

VLAN Configuration

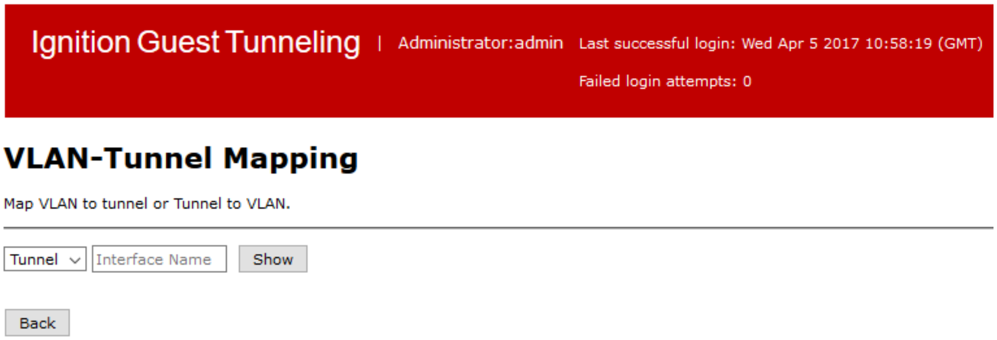
Add/Delete VLAN to database.

VLAN ID:

Removed VLAN 800 from database and flushed respective tunnels mapping.

Sl No	VLAN ID	Delete □ All
1	900	□

4. Administrator can perform VLAN mapping on the configured tunnels. For doing so, go to the VLAN page and Click **VLAN Mapping** to map the added VLANs to the configured tunnels and vice-versa. The below window gets displayed:



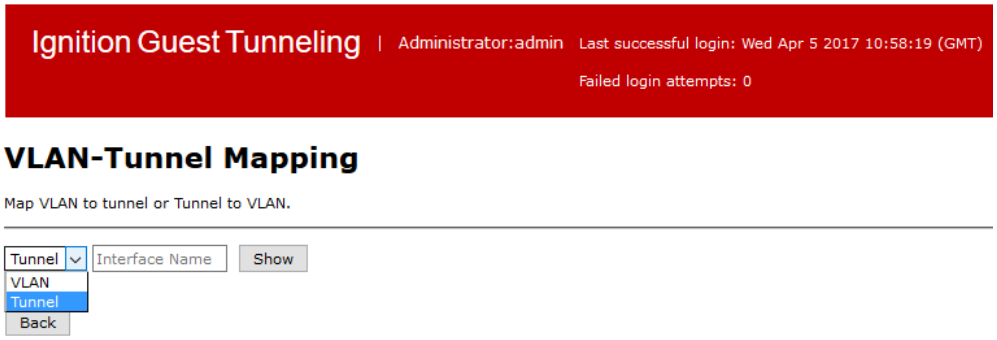
Last successful login: Wed Apr 5 2017 10:58:19 (GMT)
Failed login attempts: 0

VLAN-Tunnel Mapping

Map VLAN to tunnel or Tunnel to VLAN.

Tunnel

Mapping can be done in two ways. Either map Tunnel to VLANs or VLAN to Tunnels. Choose the option from the drop-down list as shown below:

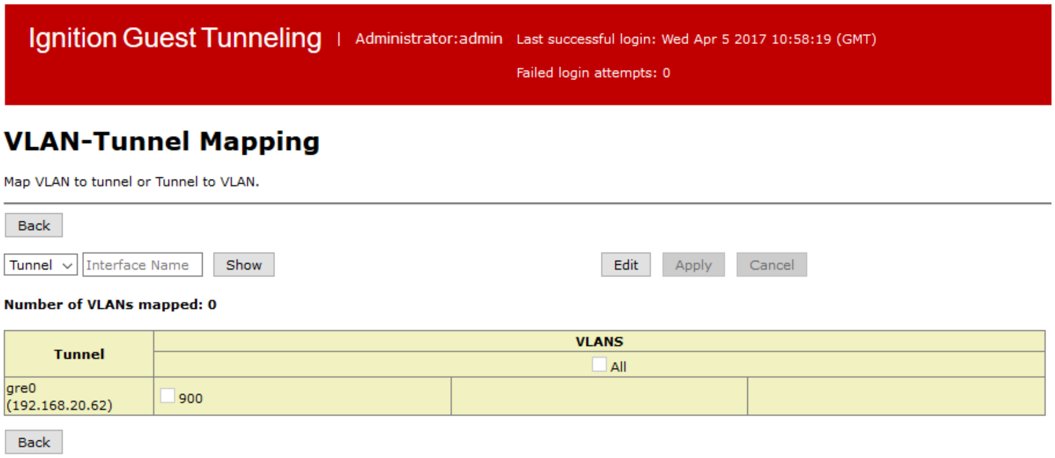


Last successful login: Wed Apr 5 2017 10:58:19 (GMT)
Failed login attempts: 0

VLAN-Tunnel Mapping

Map VLAN to tunnel or Tunnel to VLAN.

5. To map a **Tunnel to VLANs**, select Tunnel Name form the drop down list. Enter the **Tunnel Name** in the field and click **Show**. For example, if Tunnel name gre0 is entered, the window having all the VLANs that can be mapped to Tunnel is displayed as shown below:



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:58:19 (GMT)
Failed login attempts: 0

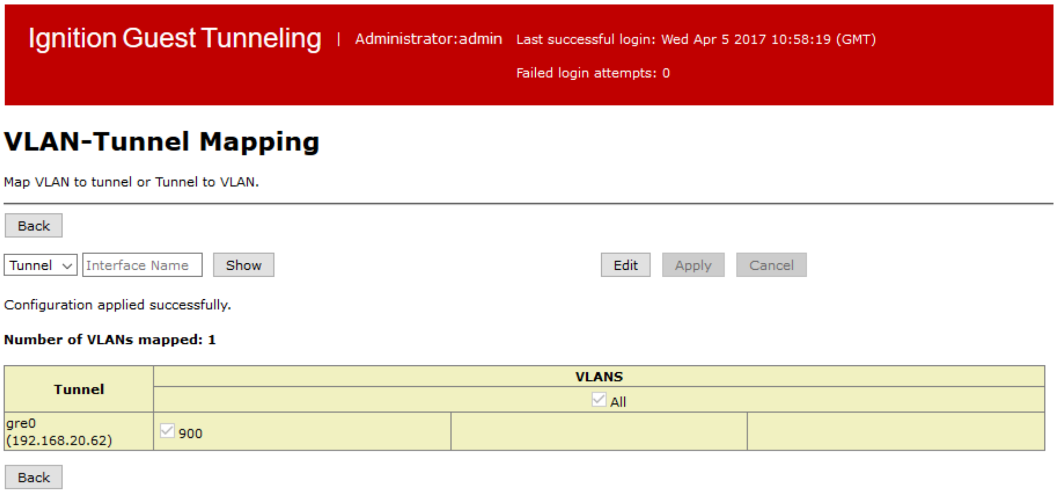
VLAN-Tunnel Mapping

Map VLAN to tunnel or Tunnel to VLAN.

Number of VLANs mapped: 0

Tunnel	VLANS		
	□ All		
gre0 (192.168.20.62)	□ 900		

Click **Edit**, Select the **VLANs** that required to be mapped to the specified Tunnel and Click **Apply**.



Ignition Guest Tunneling | Administrator:admin Last successful login: Wed Apr 5 2017 10:58:19 (GMT)
Failed login attempts: 0

VLAN-Tunnel Mapping

Map VLAN to tunnel or Tunnel to VLAN.

Configuration applied successfully.

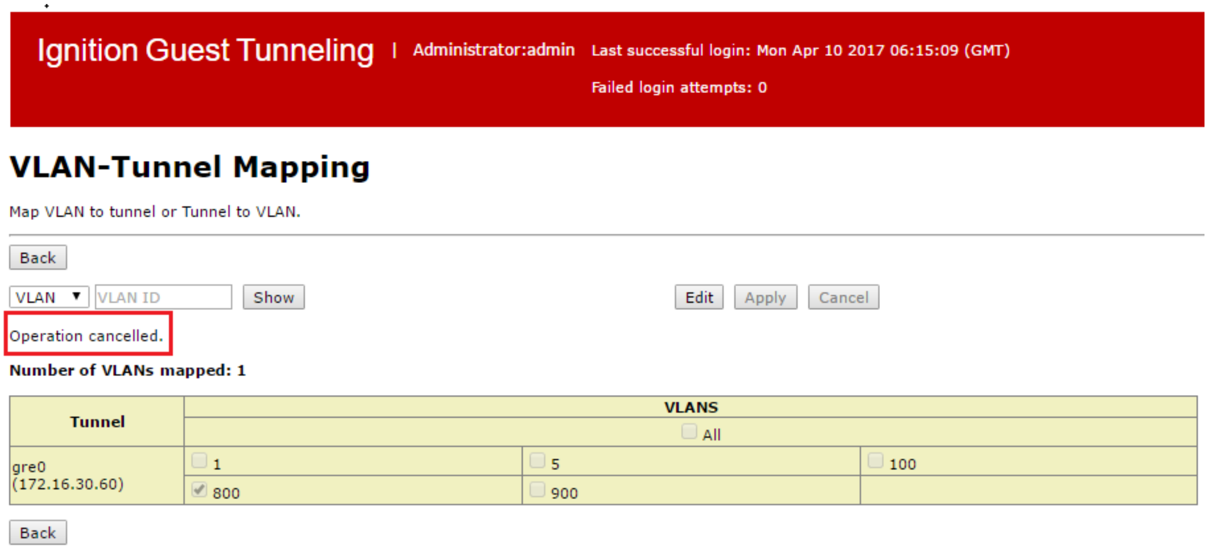
Number of VLANs mapped: 1

Tunnel	VLANS		
	☑ All		
gre0 (192.168.20.62)	☑ 900		

Note:

A message showing that the configuration has been applied successfully and the number of VLANs mapped to Tunnel is displayed.

Administrator can Click the **Cancel** button to restore the previous mapping. A message showing that the operation is cancelled successfully is displayed as shown below:



Ignition Guest Tunneling | Administrator:admin Last successful login: Mon Apr 10 2017 06:15:09 (GMT)

Failed login attempts: 0

VLAN-Tunnel Mapping

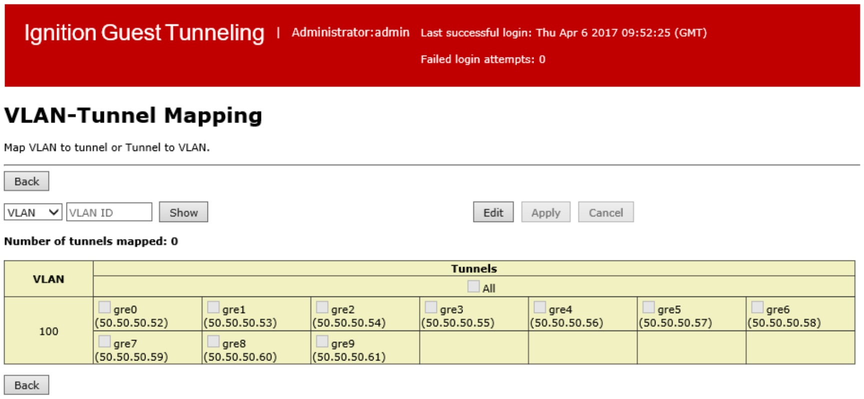
Map VLAN to tunnel or Tunnel to VLAN.

Operation cancelled.

Number of VLANs mapped: 1

Tunnel	VLANS		
	□ All		
gre0 (172.16.30.60)	□ 1	□ 5	□ 100
	☑ 800	□ 900	

6. To map a **VLAN to Tunnel**, Select **VLAN** from the drop-down list, Enter the **VLAN** and click **Show**. For example, if VLAN ID 800 is entered, the window having all the existing Tunnels is displayed as shown below:



Ignition Guest Tunneling | Administrator:admin Last successful login: Thu Apr 6 2017 09:52:25 (GMT)

Failed login attempts: 0

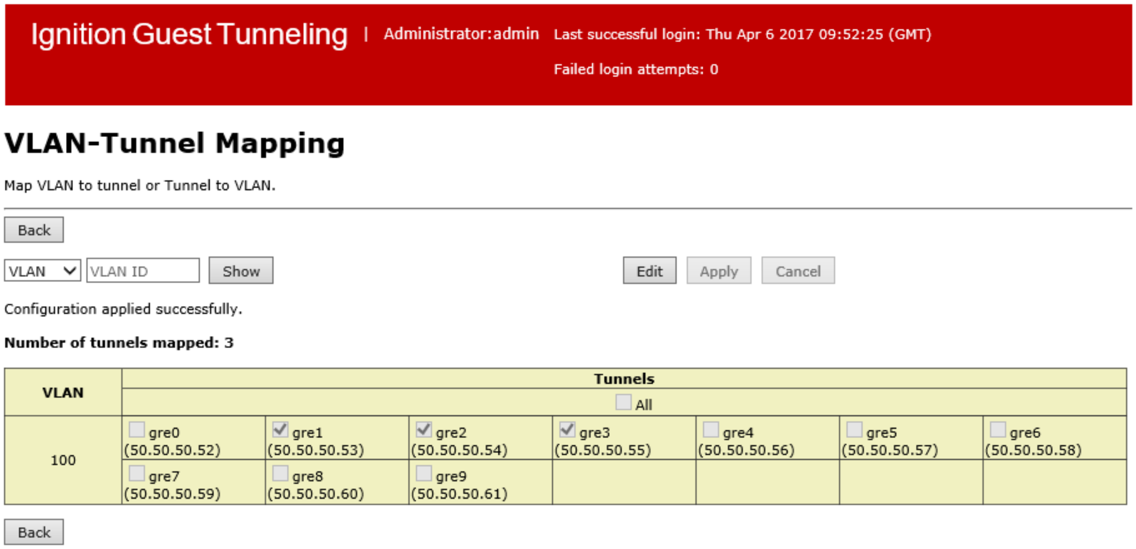
VLAN-Tunnel Mapping

Map VLAN to tunnel or Tunnel to VLAN.

Number of tunnels mapped: 0

VLAN	Tunnels						
	□ All						
100	□ gre0 (50.50.50.52)	□ gre1 (50.50.50.53)	□ gre2 (50.50.50.54)	□ gre3 (50.50.50.55)	□ gre4 (50.50.50.56)	□ gre5 (50.50.50.57)	□ gre6 (50.50.50.58)
	□ gre7 (50.50.50.59)	□ gre8 (50.50.50.60)	□ gre9 (50.50.50.61)				

Click **Edit**, Select the **Tunnel Names** that required to be mapped to the specified VLAN and Click **Apply**.



Ignition Guest Tunneling | Administrator:admin Last successful login: Thu Apr 6 2017 09:52:25 (GMT)
Failed login attempts: 0

VLAN-Tunnel Mapping

Map VLAN to tunnel or Tunnel to VLAN.

Configuration applied successfully.

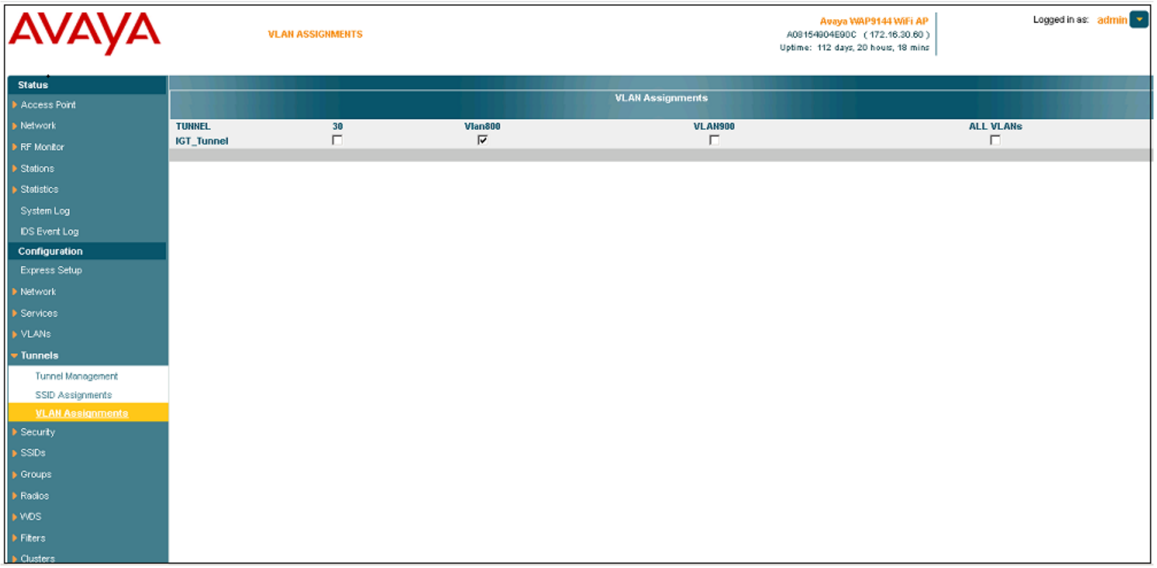
Number of tunnels mapped: 3

VLAN	Tunnels						
	□ All						
100	□ gre0 (50.50.50.52)	☑ gre1 (50.50.50.53)	☑ gre2 (50.50.50.54)	☑ gre3 (50.50.50.55)	□ gre4 (50.50.50.56)	□ gre5 (50.50.50.57)	□ gre6 (50.50.50.58)
	□ gre7 (50.50.50.59)	□ gre8 (50.50.50.60)	□ gre9 (50.50.50.61)				

Administrator can Click the **Cancel** button to restore the previous mapping.

Note:

To support specific VLAN tunneling functionality in IGT, we need to have the corresponding AP configuration as shown in the below screen shot.



VLAN Assignments

TUNNEL	30	Vlan800	VLAN900	ALL VLANs
IGT_Tunnel	□	☑	□	□

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.

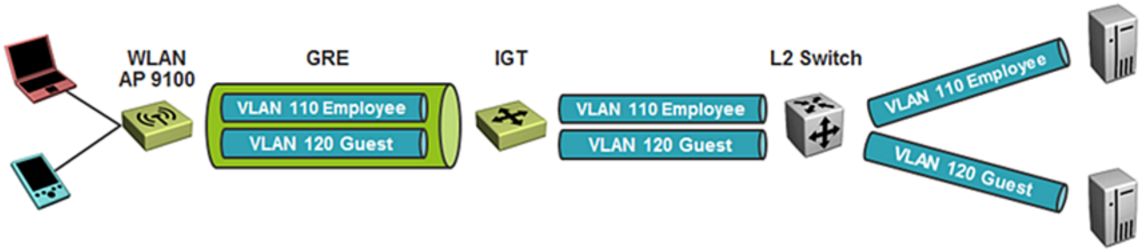


Figure 4: Topology diagram of multiple VLAN support in IGT

Configuring VLAN on ESXi Server for IGT OUT interface

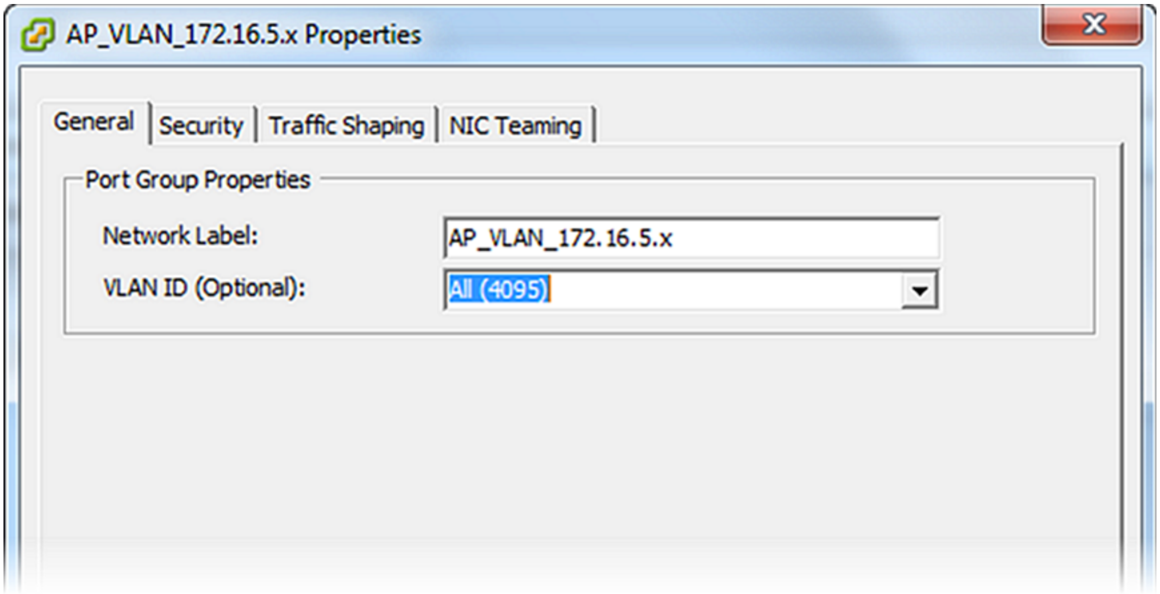
About this task

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.



Network Label: AP_VLAN_172.16.5.x

VLAN ID (Optional): All (4095)

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 83.
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 34.
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

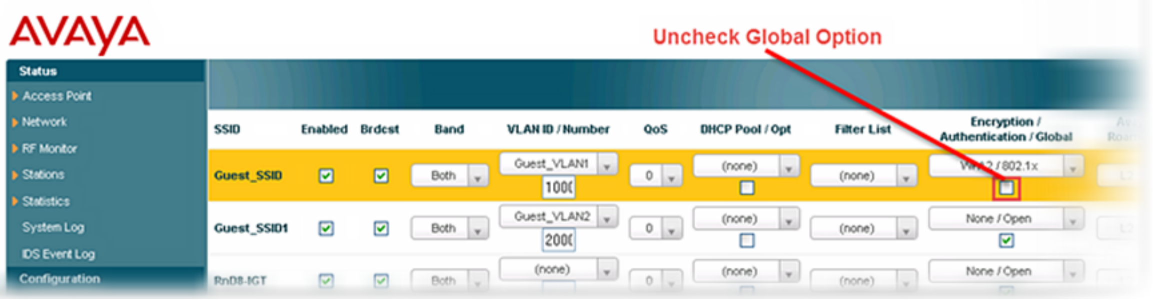
This section describes the procedure to configure Dynamic Client VLAN assignment through IDE Server.

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 34.
2. Select **Encryption / Authentication / Global** type as `WPA2/802.1X`.

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



SSID	Enabled	Brdcst	Band	VLAN ID / Number	QoS	DHCP Pool / Opt	Filter List	Encryption / Authentication / Global
Guest_SSID	☑	☑	Both	Guest_VLAN1 100(	0	(none) □	(none)	WPA2 / 802.1x □
Guest_SSID1	☑	☑	Both	Guest_VLAN2 200(	0	(none) □	(none)	None / Open ☑
RnD8-IGT	☑	☑	Both	(none)	0	(none)	(none)	None / Open

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

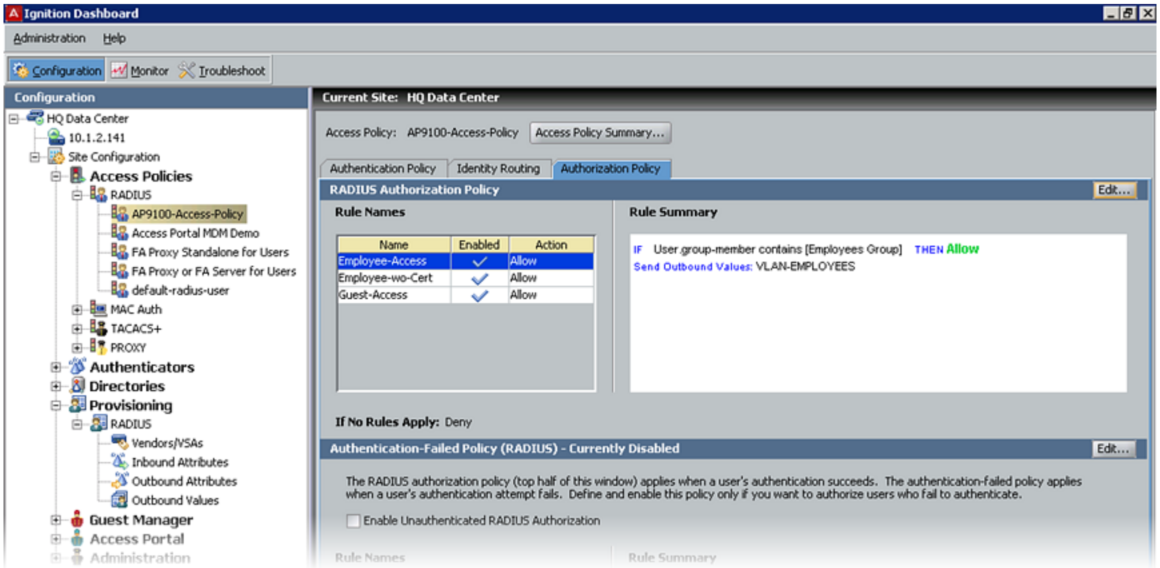
4. Configure the Ignition Server as the external radius server by entering the **Primary Host / IP Address** and **Shared Secret** for the ports 1812 and 1813.

5. Configure VLAN. For more information, see Configuring VLANs on WLAN 9100 on page 83.

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.



Current Site: HQ Data Center

Access Policy: AP9100-Access-Policy

RADIUS Authorization Policy

Rule Names

Name	Enabled	Action
Employee-Access	✓	Allow
Employee-wo-Cert	✓	Allow
Guest-Access	✓	Allow

Rule Summary

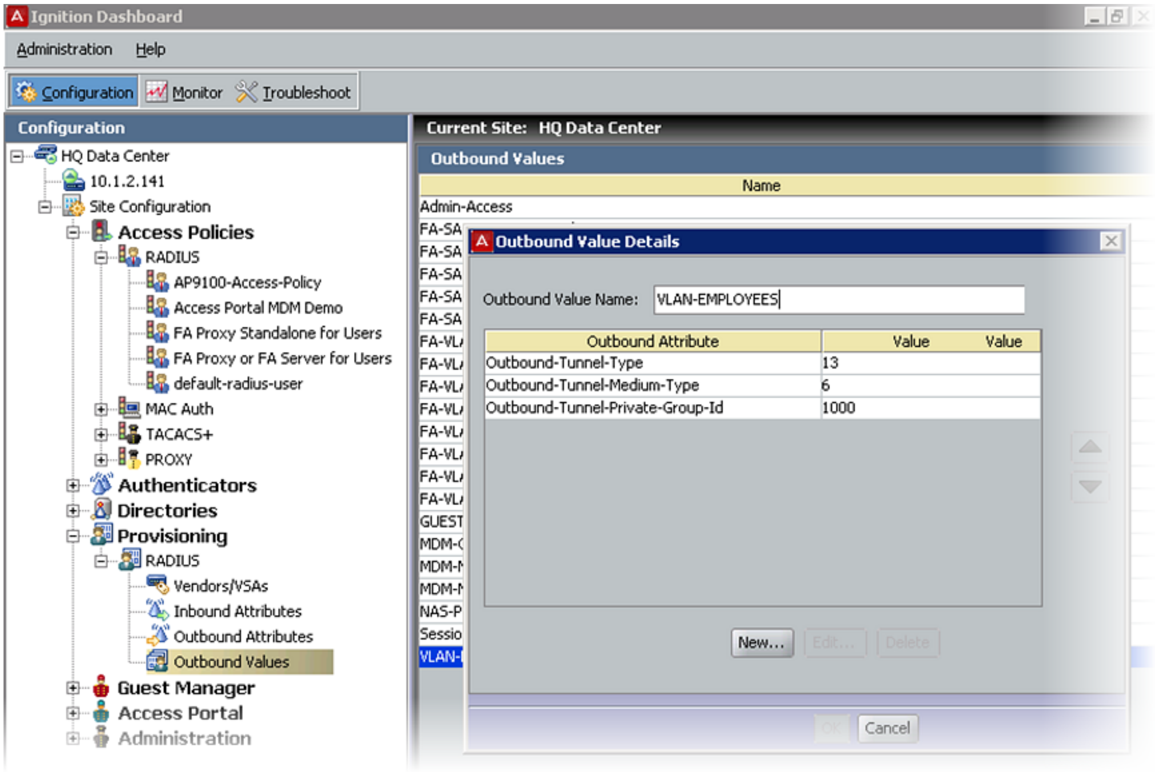
IF User.group-member contains [Employees Group] THEN Allow
Send Outbound Values: VLAN-EMPLOYEES

If No Rules Apply: Deny

Authentication-Failed Policy (RADIUS) - Currently Disabled

The RADIUS authorization policy (top half of this window) applies when a user's authentication succeeds. The authentication-failed policy applies when a user's authentication attempt fails. Define and enable this policy only if you want to authorize users who fail to authenticate.

□ Enable Unauthenticated RADIUS Authorization



Outbound Value Name: VLAN-EMPLOYEES

Outbound Attribute	Value	Value
Outbound-Tunnel-Type	13	
Outbound-Tunnel-Medium-Type	6	
Outbound-Tunnel-Private-Group-Id	1000	

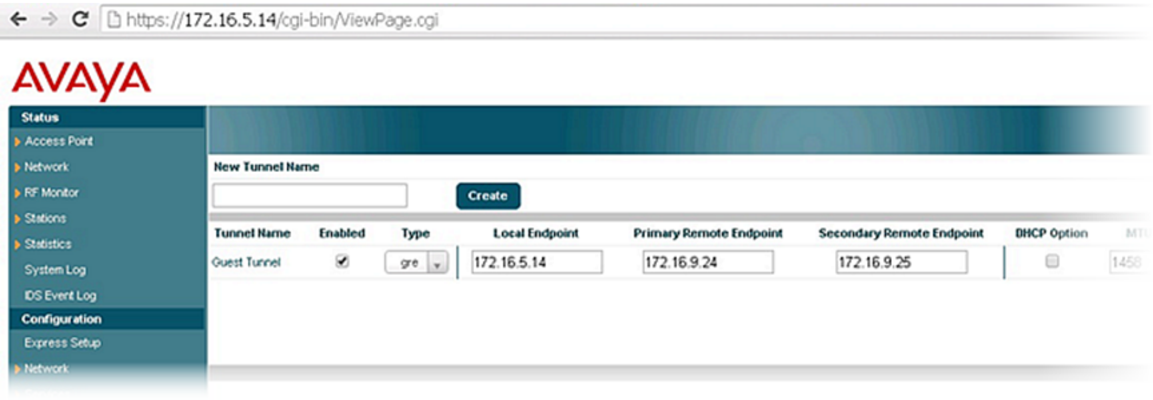
7. To configure multiple VLANs on ESXi Server. For more information, see Configuring VLAN on ESXi Server mapping to IGT IN-interface on page 80.

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



Tunnel Name	Enabled	Type	Local Endpoint	Primary Remote Endpoint	Secondary Remote Endpoint	DHCP Option	MTU
Guest Tunnel	☑	gre	172.16.5.14	172.16.9.24	172.16.9.25	□	1458

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.

For more information on Web interface based troubleshooting options, see Troubleshooting Guest Tunneling Appliance on page 71.

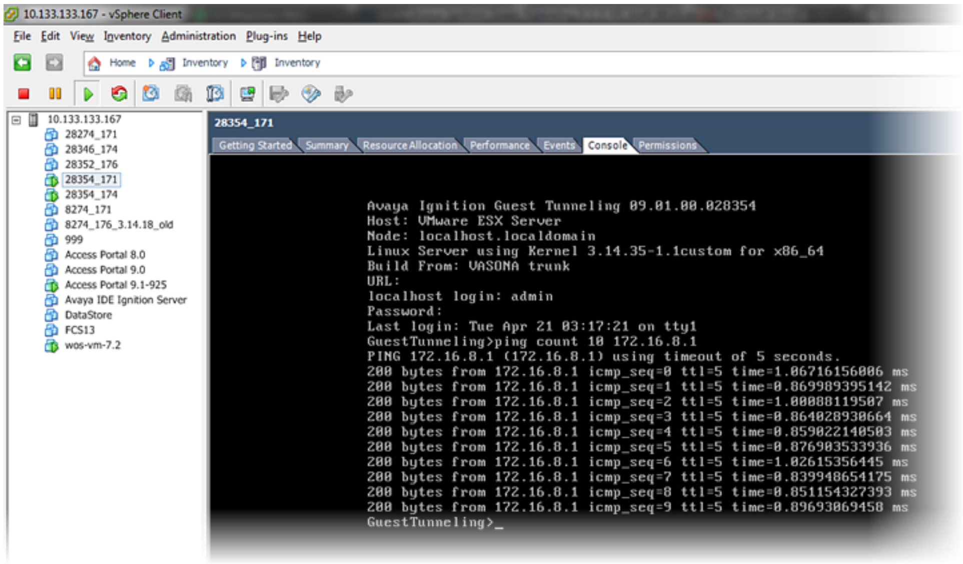
Verifying the connectivity for IGT appliance

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`



```
Avaya Ignition Guest Tunneling 09.01.00.028354
Host: VMware ESX Server
Node: localhost.localdomain
Linux Server using Kernel 3.14.35-1.1custom for x86_64
Build From: VASONA trunk
URL:
localhost login: admin
Password:
Last login: Tue Apr 21 03:17:21 on tty1
GuestTunneling>ping count 10 172.16.8.1
PING 172.16.8.1 (172.16.8.1) using timeout of 5 seconds.
200 bytes from 172.16.8.1 icmp_seq=0 ttl=5 time=1.06716156006 ms
200 bytes from 172.16.8.1 icmp_seq=1 ttl=5 time=0.869989395142 ms
200 bytes from 172.16.8.1 icmp_seq=2 ttl=5 time=1.00088119507 ms
200 bytes from 172.16.8.1 icmp_seq=3 ttl=5 time=0.864028930664 ms
200 bytes from 172.16.8.1 icmp_seq=4 ttl=5 time=0.859022140503 ms
200 bytes from 172.16.8.1 icmp_seq=5 ttl=5 time=0.876903533936 ms
200 bytes from 172.16.8.1 icmp_seq=6 ttl=5 time=1.02615356445 ms
200 bytes from 172.16.8.1 icmp_seq=7 ttl=5 time=0.839948654175 ms
200 bytes from 172.16.8.1 icmp_seq=8 ttl=5 time=0.851154327393 ms
200 bytes from 172.16.8.1 icmp_seq=9 ttl=5 time=0.89693069458 ms
GuestTunneling>_
```

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.

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.

Q6: **Redirection to login page fails after reboot/restore:**.

A6:

1. Refresh the browser page or open a new instance.