Configuring Avaya Identity Engines Ignition Guest Manager

Release 9.1
NN47280-501
Issue 05.01
March 2015

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You 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

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: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such 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 *Avaya Identity Engines Ignition Guest Manager Configuration* guide explains how to install, configure, and manage Guest Manager.

This guide is written for Guest Manager administrators as an aid to perform the following tasks:

- Install Guest Manager
- Configure guest authorization policies
- Create provisioner accounts for your front desk personnel
- Teach front desk personnel how to create and manage guest user accounts in Guest Manager

Related resources

Documentation

See the following related documents.

Title	Purpose	Document number
Avaya Identity Engines Ignition Server Getting Started	Installation and simple configuration	NN47280–300
Avaya Identity Engines Ignition Server Administration	All configuration options	NN47280–600
Configuring and Managing Avaya Identity Engines Single-Sign-On	Configuration, management, and deployment	NN47280–502
Avaya Identity Engines Ignition CASE Administration	Installation, configuration, and deployment	NN47280–603
Avaya Identity Engines Ignition Access Portal Administration	Installation, configuration, and deployment	NN47280–604
Avaya Identity Engines Ignition Analytics	Installation, configuration, and maintenance	NN47280–601

Table continues…

Title	Purpose	Document number
Avaya Identity Engines Ignition Server Release Notes	Reference	NN47280–400

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.

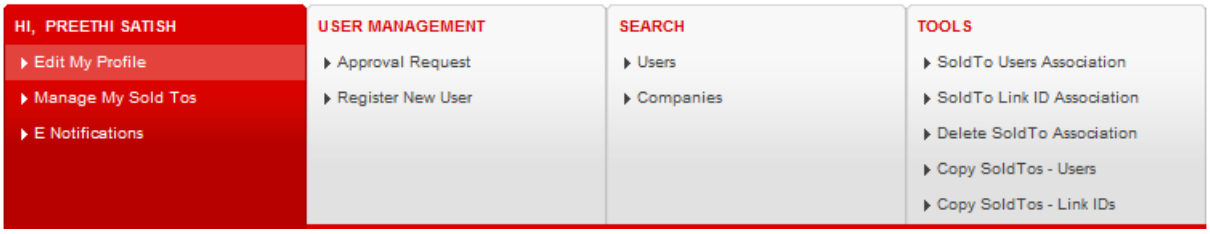
About this task

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 8800.

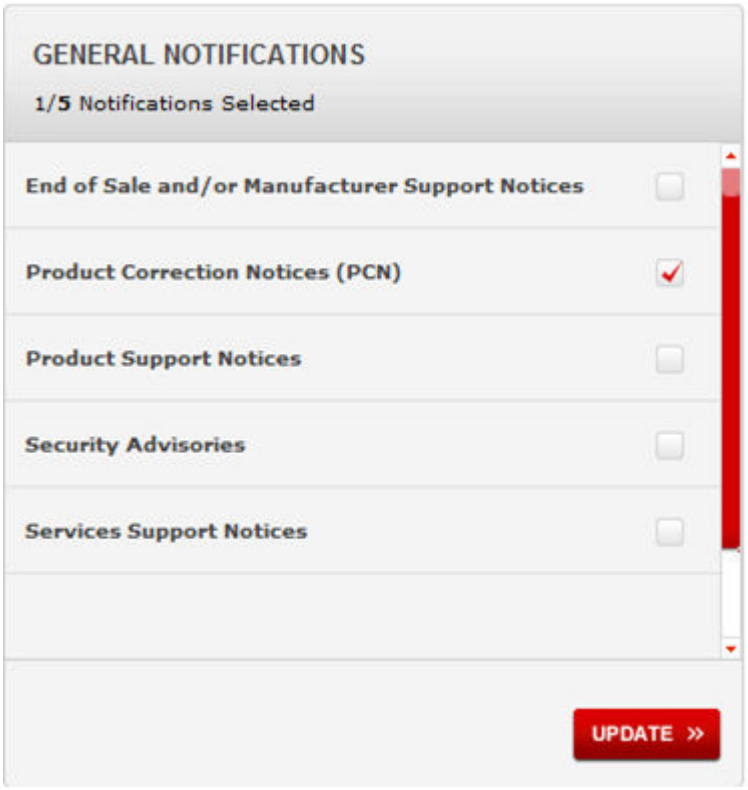
Procedure

1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Click **MY PROFILE**.

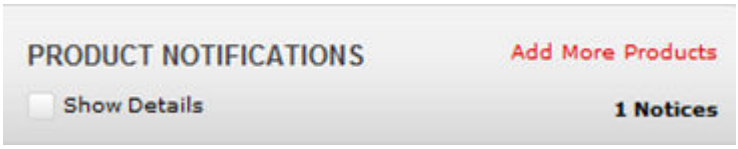
4. On the site toolbar, click your name, and then click **E Notifications**.



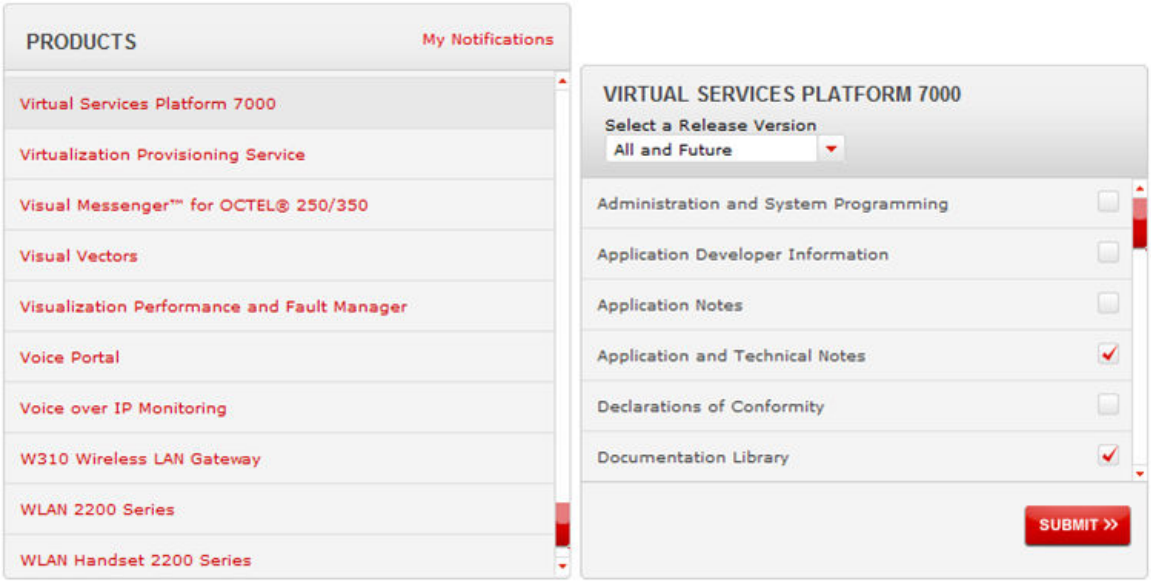
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.



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



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



11. Click **Submit**.

Searching a documentation collection

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

Before you begin

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

Procedure

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

- Include Comments

6. Click **Search**.

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

Support

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

Chapter 2: New in this release

With the increase of global security concerns, corporations are moving away from the open network guest access that is available in many coffee shops. Corporations are moving towards controlled guest access. Avaya Ignition Guest Manager, a component of the Identity Engines portfolio, enables secure and controlled guest access.

The following sections detail what is new in *Avaya Identity Engines Ignition Guest Manager Configuration* for Release 9.1.

Guest Manager OVA

In Release 9.1, you deploy Guest Manager as a virtual machine and you do not need a separate Windows machine to install Guest Manager. The Guest Manager virtual appliance incorporates RHEL as the OS. It also incorporates VMware tools to enable the Guest Manager VM to be VMware vMotion friendly.

As of Release 9.1, Guest Manager is no longer available as a Windows application.

Sponsor approval workflow

This release introduces a sponsor approval workflow for self-service guest users. Administrators configure whether or not a sponsor's approval is required. If required, the guest user creates the self-service account and the account is approved by the sponsor before access is granted to the guest user. Administrators can also configure auto-approval or auto-denial if the sponsor is unavailable or does not provide an action.

When a guest user completes registration, the guest user receives a message (SMS/email) indicating that the request is pending approval of the sponsor. When the sponsor approves the request, the guest user receives a second message (SMS/email) indicating the account is available.

Self-service enhancements

The self-service template is simplified with fewer fields and more automation. Changes include:

- Guest Manager selects where to send account credentials (SMS or email or both) based on what information the guest user provides. For example, if the guest user provides a cell phone number, then an SMS message is sent. If the guest user provides an email address, then an email message is sent.
- Administrators can specify if the first and last names in the self-service template are mandatory, and if not mandatory, whether or not they are displayed on the self-service template.
- Administrators can also specify to use the email address or cell phone number as the user name.
- Administrators can specify a static password so login to Access Portal is possible with only the user name.
- Administrators can define a limit to the number of guest accounts that can be created for a given email or cell phone number.

Email SMTP configuration

In this release, the administrator can make the following changes to email SMTP configuration:

- Configure web-based mail servers, such as Gmail and Yahoo, as mail servers in the Guest Manager application.
- Configure the SMTP port number to be used by Guest Manager for SSL and non-SSL connections.
- Configure the SMTP server user name as an email address.
- Configure the system or custom certificate for SSL connection.

SMS gateway configuration

In this release, the administrator can

- specify if the SMS gateway list is displayed or hidden
- configure any SMS gateway as the default gateway

Guest Manager monitoring enhancements

The Guest Manager Administrator monitoring screens for Users and Devices are enhanced with new search options, new columns displayed, better paging options, and more.

Trouble Ticket

The Guest Manager Administrator interface now includes the **TroubleTicket** option on the main toolbar. Use **TroubleTicket** to generate a trouble ticket file that you can send to Avaya technical support in the event of a Guest Manager fault.

Additional Guest Manager enhancements

Guest Manager Release 9.1 incorporates the following additional enhancements:

- New **Guest Details** field in which the front desk Provisioner can add informative details about the visitor being granted guest access (for example, driving license information or company name).
- Import and Export functions play a critical role for upgrades to new future releases of Guest Manager. The administrator can export the configuration from Guest Manager and then import the configuration into a newly deployed Guest Manager VM.
- Removal of the underscore ("_") character from the automated generation of user names.
- Guest Manager self-service page is mobile friendly.
- Administrator can configure the displaying of the user name to the front-desk Provisioner and self-service Provisioner after guest users register their accounts.
- Administrator can configure the maximum number of enabled devices that a front-desk Provisioner or self-service Provisioner can provision.
- Administrator can display a comment/note to the device Provisioner.

Chapter 3: Guest Manager introduction

Avaya Identity Engines Ignition Guest Manager is a web application that lets front desk staff create and manage temporary network accounts for visitors. As the Avaya Identity Engines Ignition Server administrator, you are able to choose what degree of account creation authority you delegate to each receptionist, determine how quickly the guest accounts expire, and decide what parts of your network the guests can use.

Guest Manager application in context

The Ignition Server system for provisioning and managing guest network access consists of the following components:

- Guest Manager **Administrator Application** for managing provisioners and for performing bulk updates of guests and devices.
- Guest Manager **Provisioner Application** for managing guests and devices.
- Ignition Server virtual appliance, which authenticates and authorizes users who wish to connect to your network.
- Ignition Dashboard application, where you write the authorization policies that determine which users can connect to which parts of your network.
- *optionally*: Avaya Identity Engines Ignition Server CASE wizard software to help users configure their laptops to connect through 802.1X.
- *optionally*: Avaya Identity Engines Ignition Access Portal: web-based authentication virtual appliance to help users connect if their laptop is not equipped with 802.1X authentication software.

Types of accounts in your Ignition Server installation

Guest Manager is a tool for delegating administration. Guest Manager allows the Guest Manager administrator to designate other people (called *provisioners*) with the authority to create temporary user accounts (called *guest users*) that provide network access. The following are the types of users:

- *The Guest Manager administrator* uses Guest Manager to create *provisioners*, and the Guest Manager administrator is the only person who can create provisioners. Often, the same person

who acts as the Ignition Server Administrator acts as the Guest Manager administrator, but each account has its own user name and password. There is only one Guest Manager administrator account. This user account is stored internally in Guest Manager and cannot be mapped to an existing user account in the Ignition Server or elsewhere. You can change its account login name and password as explained in Setting the Administrator Username and Password on page 69.

- The *SOAP API user credentials* allow Guest Manager to connect to the Ignition Server. See Making SOAP settings on the Ignition Server on page 55.
- The *Ignition Server Administrator* uses Ignition Dashboard to set up guest authorization policies and to determine certain application settings such as the SOAP API settings. This user account is stored internally in Ignition Server and cannot be mapped to an existing user account in the Ignition Server or elsewhere.
- A *provisioner* is a person who creates and manages guest user accounts and device records in Guest Manager. For example, if you want to give your company's receptionist the ability to hand out temporary passwords for wireless access, you would define that receptionist as a *provisioner*.
- Each provisioner account is stored either in the Ignition Server internal store or in your LDAP or Active Directory store. Your installation can store provisioners in both places at once.
  - To create provisioner accounts in the Ignition Server internal store, see Creating a Provisioner access policy on page 47. We refer to internally stored provisioners as *internal provisioners*.
  - To have Guest Manager authenticate provisioners against your LDAP or AD store, see Creating a provisioner from an account in an LDAP or AD store on page 119.
- *A portal provisioner* is a provisioner bound to an Ignition Server self-provisioning portal. With a self-provisioning portal in place, guests can create their own guest user accounts, which are then owned by the portal provisioner who owns the portal where the guest account was created. See Creating a Self-Provisioning service on page 97.
- A *guest user* is a visitor or other temporary user to whom you grant specific limited rights to use your network. A provisioner uses the Guest Manager application to create any number of guest user accounts. Guest user accounts are stored as users in the internal store on the Ignition Server and cannot be mapped to existing user accounts on LDAP or Active Directory stores or elsewhere. See Provisioner application: Managing guests and devices on page 134.
- A *user* is any user that Ignition Server can authenticate. The account for such a user can reside in an LDAP directory, an Active Directory store, or in the Ignition Server internal store. Guest users are a subset of users, and the Guest Manager application can view and update *only guest users* and *provisioners*; you cannot view other types of users through Guest Manager.
- A *device record* stores the details of a guest user's device so that Ignition Server can enforce rules that allow a guest to connect only using his or her own device. See Creating a device record on page 148.

When you log into Guest Manager, you must log in either as the Guest Manager administrator or as a provisioner. The actions you can perform in Guest Manager, and the extent of access to the keystore on the Ignition Server appliance, depend on whether you are logged in as the Guest Manager administrator or as a provisioner.

The Guest Manager web application requires an active link to an Ignition Server appliance.

The Guest Manager administrator role

The **Guest Manager** administrator manages the Guest Manager application. There is one Guest Manager administrator account. You cannot disable this account, but you can change its user name and password. The Guest Manager Administrator:

- Creates and manages the provisioner accounts.
- Configures Guest Manager application settings.
- Connects Guest Manager to the Ignition Server appliance. The Guest Manager application must be connected in order for Provisioners to use it. As Administrator, you must make sure this connection is up.
- Optionally, the Guest Manager administrator can delete expired guest user accounts and can export guest user accounts to file.

Provisioners role

Provisioner users manage guest users. Each provisioner employs the Guest Manager application to create, modify, and delete guest users. Provisioners own the guest users that they create.

Only the Guest Manager administrator can add and delete provisioner accounts.

Important:

Manage and delete Provisioner accounts only from the Guest Manager application, not from the Ignition Dashboard application.

Guest users

A guest user account has the following attributes:

- **Account details**: User name and password for the temporary account.
- **Personal data**: First name, last name, e-mail address, and mobile telephone number of the user.
- **Access duration**: When the account should be activated, and for how long.
- **Auto expiry deletion**: The option to select whether or not the guest account is automatically deleted once it expires.

- **Notification settings**: Where to send an e-mail or SMS message notification informing that the guest account has been created. The notification contains the guest user name and password and is usually sent directly to the guest.

Guest user example

The following is an example of a guest user provisioning form that is ready to be submitted in order to provide guest access for Johnnie Taylor. His account is valid for 5 days starting on the **Activate Account On** date, and his provisioner has selected to turn on **Delete on Expire**. Both the guest and the provisioner for the guest account receive electronic confirmation of the creation of this account.

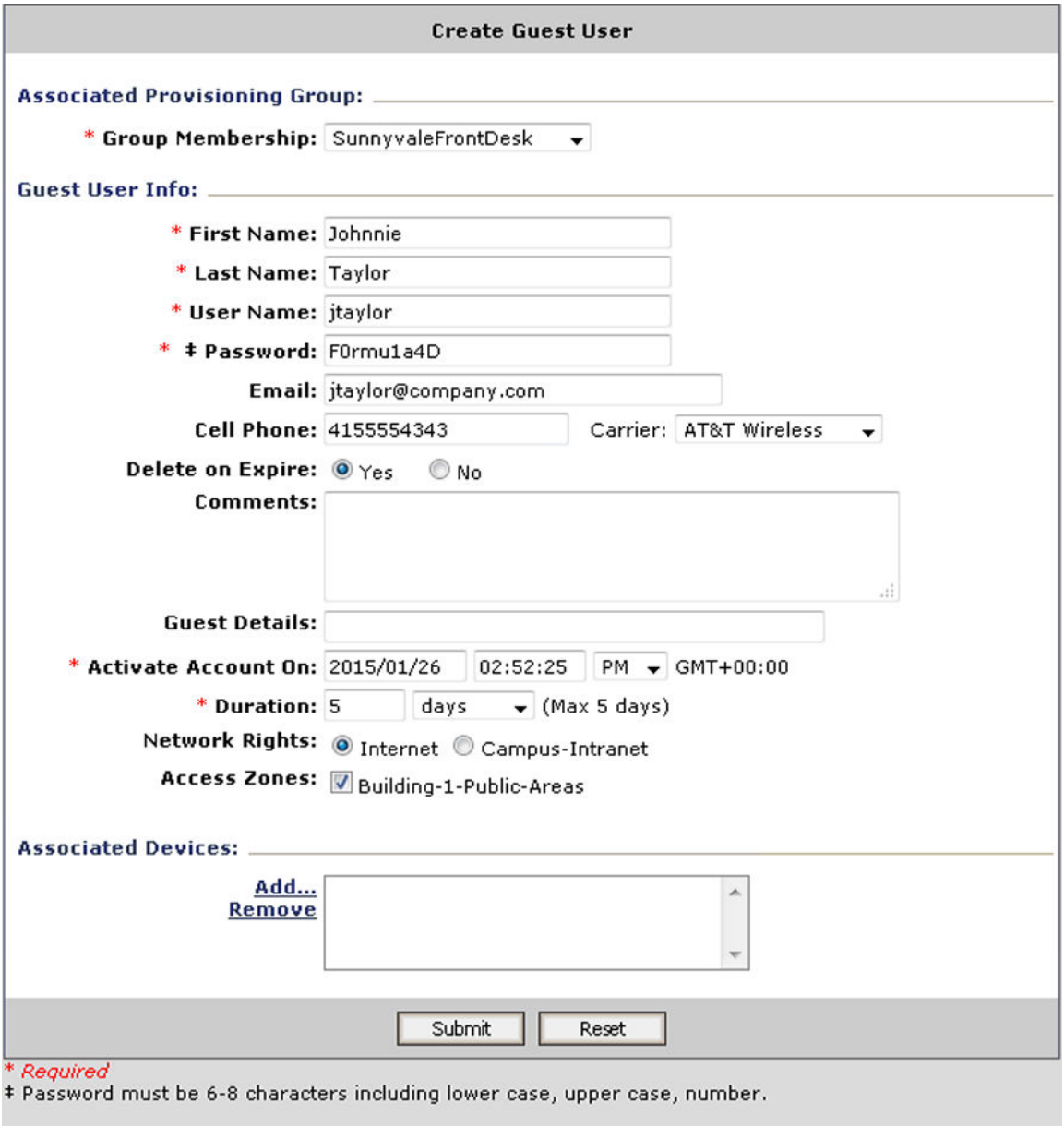


Figure 1: Create Guest User window

Device example

Guest Manager allows you to create device records and assign them to guest users for the purpose of limiting users to using only certain devices, such as, for example, allowing each guest to connect using only his or her own laptop. Also, you can create rules that assign each device to the appropriate VLAN, part of the network, or physical location in your facility. The following figure is an example of a device creation window.

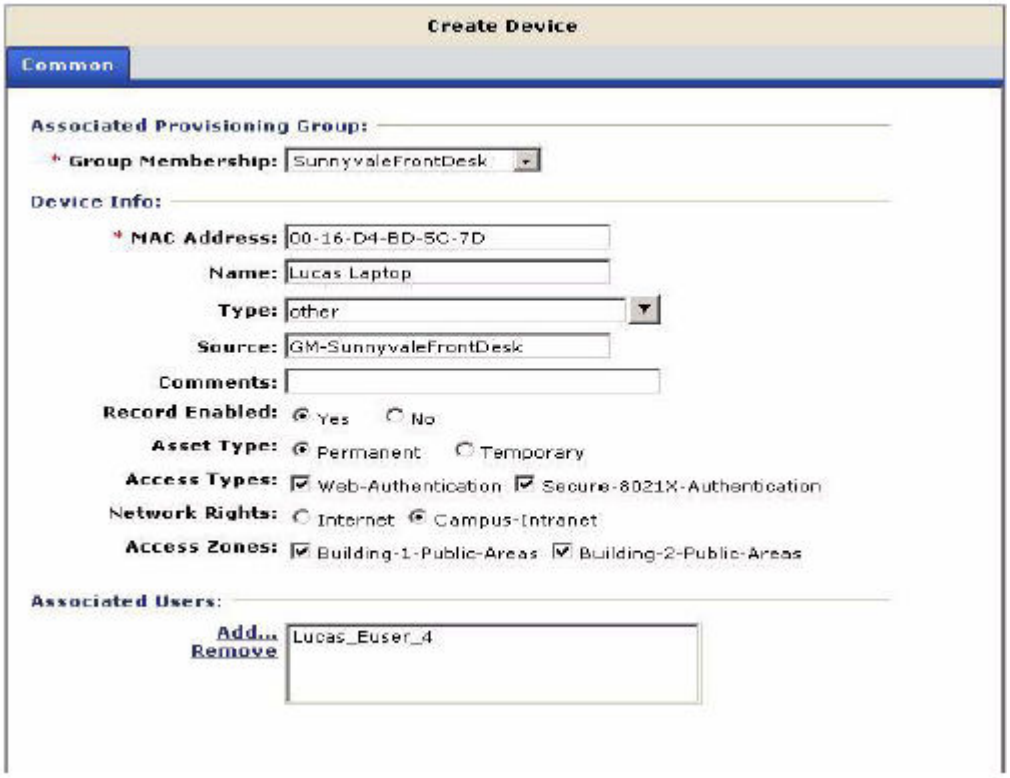


Figure 2: Create Device window

Once a provisioner has created a guest user account and a device record and associated the two, Ignition Server can enforce rules that allow the guest to connect *only using his or her own device*. Such rules are called *asset correlation policies*, and you must configure them in Ignition Dashboard. For more information, see *Avaya Identity Engines Ignition Server Administration*, NN47280-600.

You can create device records individually:

- Creating a device record on page 148
- Bulk importing device records from a file on page 149

Chapter 4: Installing Guest Manager

This chapter describes how to install Avaya Identity Engines Ignition Guest Manager. You install Guest Manager as a virtual appliance on a VMware ESXi 5.1 or 5.5 server.

System requirements

To install Guest Manager, you need:

- A running Ignition Server appliance, reachable on the network from where you run Guest Manager. The SOAP interface must be enabled on the Ignition Server.
- Guest Manager (VMware ESXi 5.1 or 5.5 server)
- An installation of the Ignition Dashboard management application on a PC. Make sure you also have a copy of the *Avaya Identity Engines Ignition Server Administration*, NN47280-600.

Ignition Server compatibility

Guest Manager 9.1 is only compatible with version 9.1 of the Ignition Server appliance.

VMware ESXi server requirements

Hardware platforms supported by VMware's ESXi server version 5.1 and up are required. See HTTP://WWW.VMWARE.COM/ for a list of supported hardware platforms for ESXi.

See the *Avaya Identity Engines Release Notes* for information about release-specific Guest Manager VM minimum system requirements (memory, CPU, disk space, interfaces).

Installation on a VMware ESXi server is done using an OVA file that already incorporates the OS FreeBSD.

Warning:

Avaya provides Guest Manager 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, RHEL specific, or any third-party vendor package or 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.
- Avaya determines which VMware Tools to install and configure. When required, Avaya provides these tools as part of the installation package. Avaya provides these tools because 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.

Turn off automatic VMware Tools updates if you have enabled them. Refer to the following instructions to disable automatic updates.

Preventing automatic VMware Tools updates

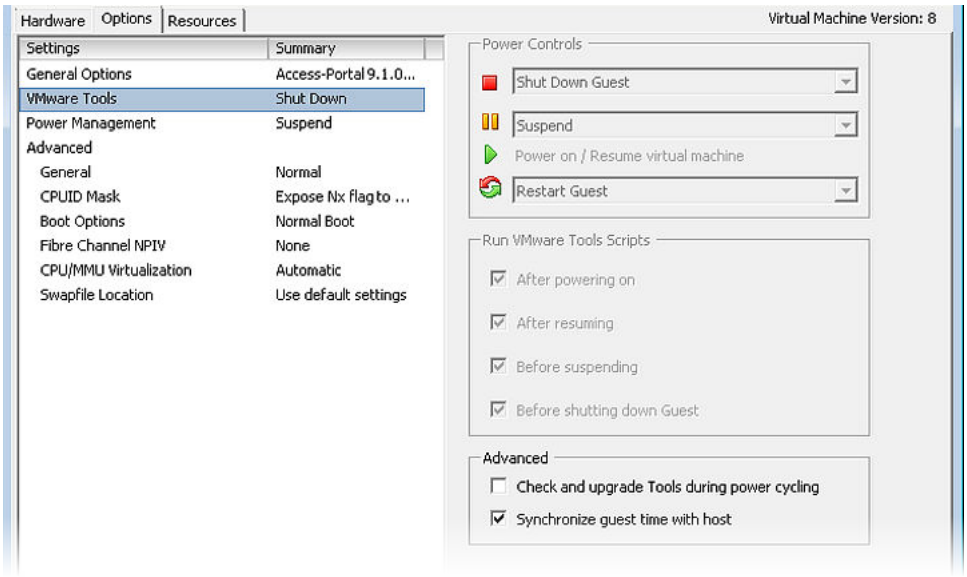
Avaya recommends that you prevent automatic VMware Tool updates and use only the tools that are delivered bundled with the installation package.

To prevent automatic VMware Tools updates:

Procedure

1. Use the vSphere client to log in to the ESXi Server.
2. Go to **Getting Started** > **Edit Virtual Machine Settings** > **Options** > **VMware Tools** > **Advanced**, and ensure the **Check and upgrade Tools during power cycling** check box is not selected. This is the supported setting.

3. Click **OK**.



Checking the VMware Tools status (ESXi 5.1 and up)

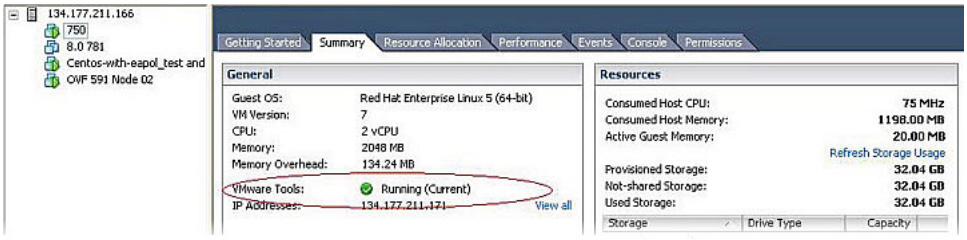
The **Summary** tab of the VM describes the VMware Tools status.

To check the VMware Tools status on an ESXi (5.1 and up) server:

Procedure

1. Use the vSphere client to log in to the ESXi Server.
2. Go to the **Summary** tab.

   After a fresh install, the VMware Tools status displays as “VMware Tools: Running (Current)”.



Note:

VMware Tools may show as not installed. This is a known VMware issue where VMware Tools may not be detected correctly on certain hardware. However, this does not interfere with the functioning of the tools—it is a display issue only.

Network configuration for Guest Manager-based authentication

Guest Manager has three network interfaces:

- **Admin** The Admin interface provides connectivity to the Guest Manager's administrator and provisioner web sessions. By default, this interface is also used for handling the connection with Ignition Server.
- **Service A** Depending on the network deployment, Ignition Server can be in a separate network. You can use Service A exclusively for handling the connection with Ignition Server (use interface and route commands).
- **Service B** is for future use.

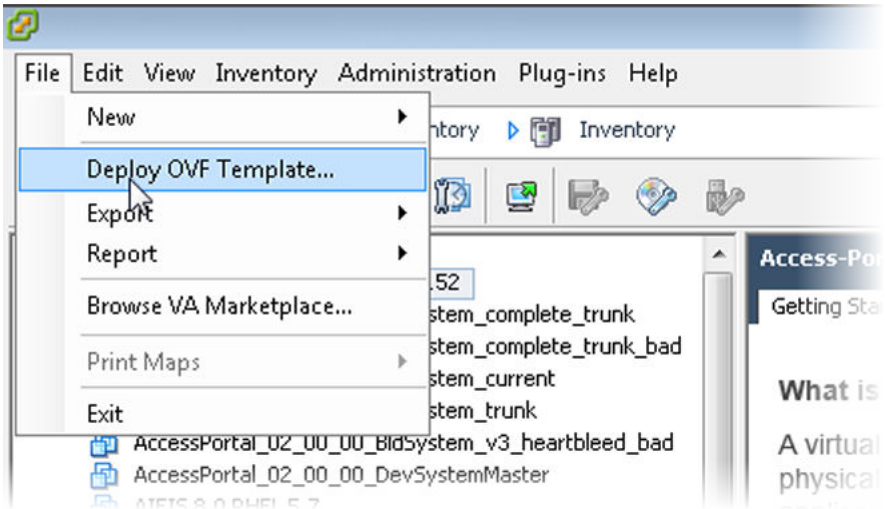
Installing the Guest Manager virtual appliance

About this task

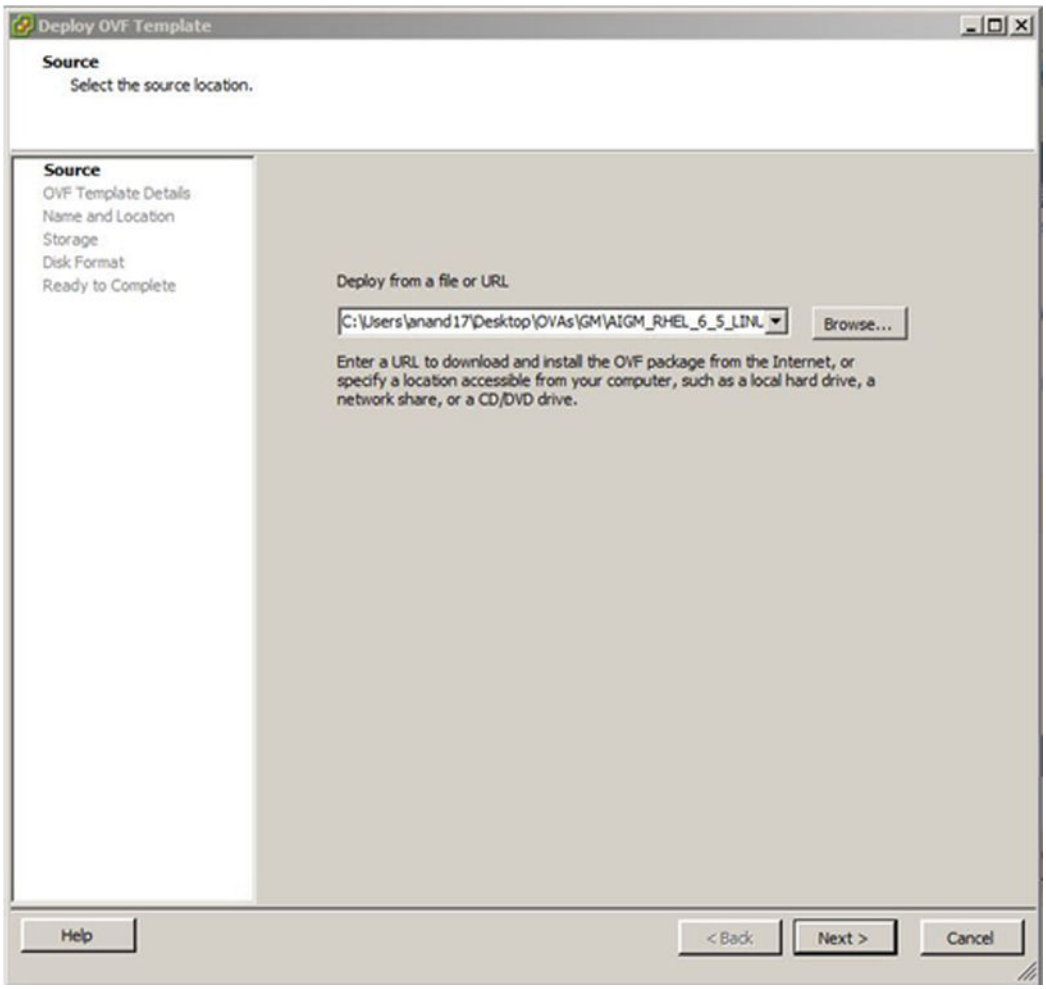
Avaya recommends that you use VWware vSphere Client to import the VM into your system. Start the VWware vSphere Client and log in to the ESXi server on which you want to install Guest Manager. Use the **Virtual Appliance Deploy OVF** option.

Procedure

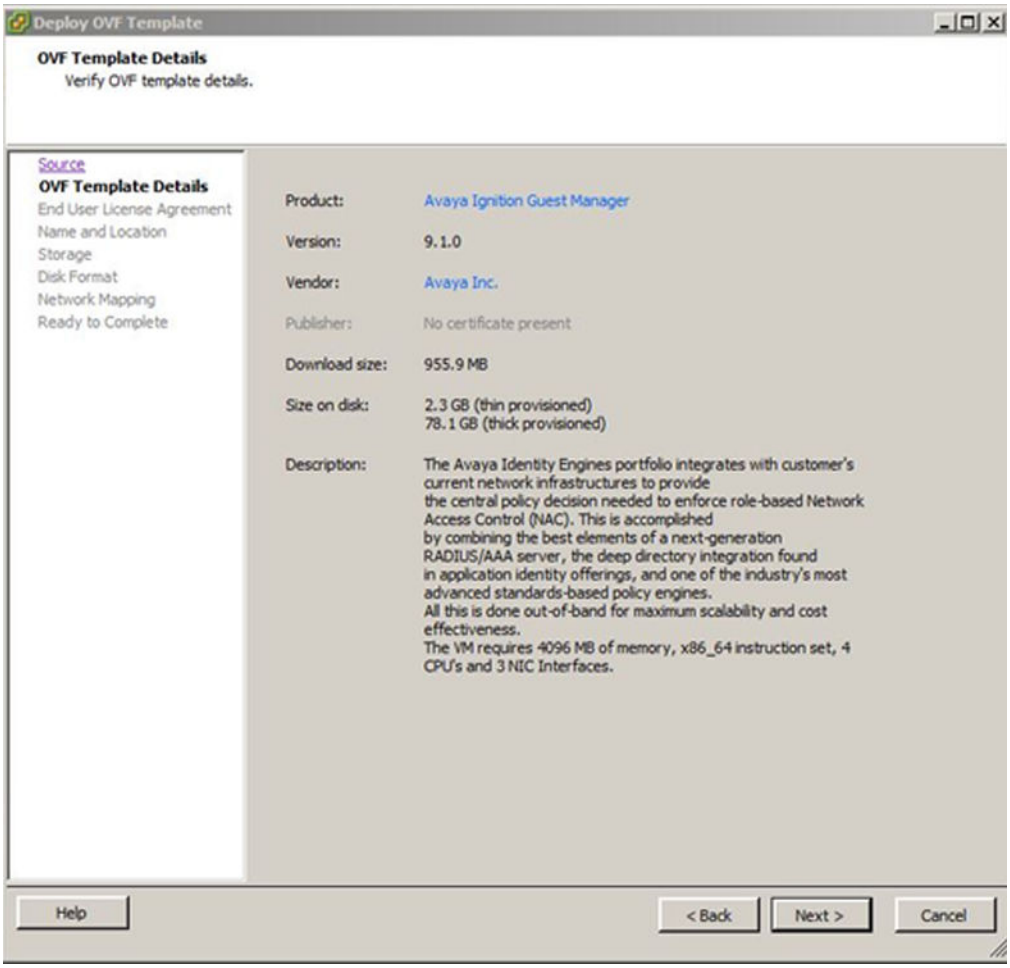
1. From the VSphere Client, select **File** > **Deploy OVF Template**.



2. On the Source screen, select the location from which you want to import the Guest Manager virtual appliance and click ***Next***.

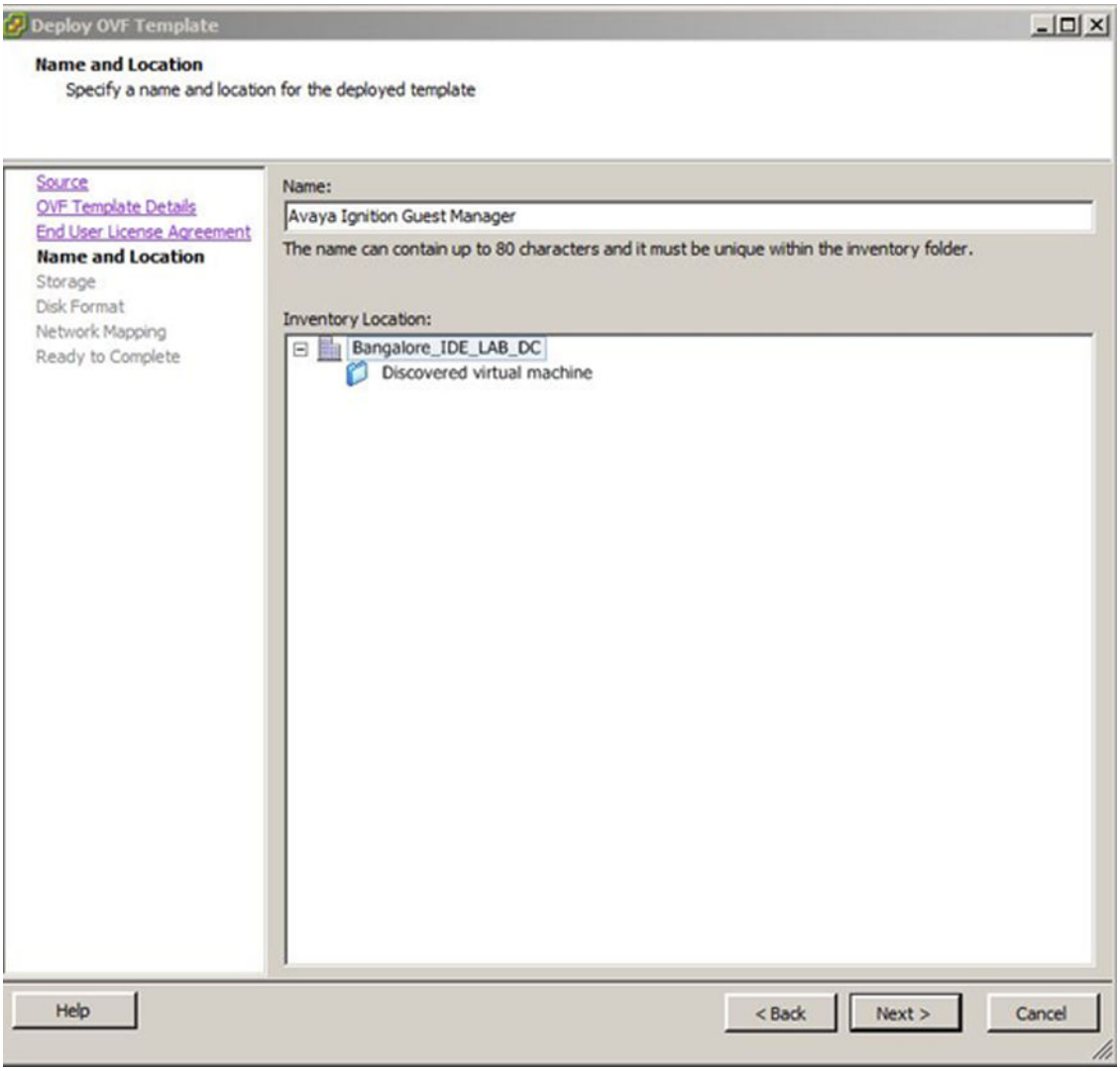


3. On the OVF Template Details screen, review your settings. Click **Back** to make changes, or click **Next** to continue.

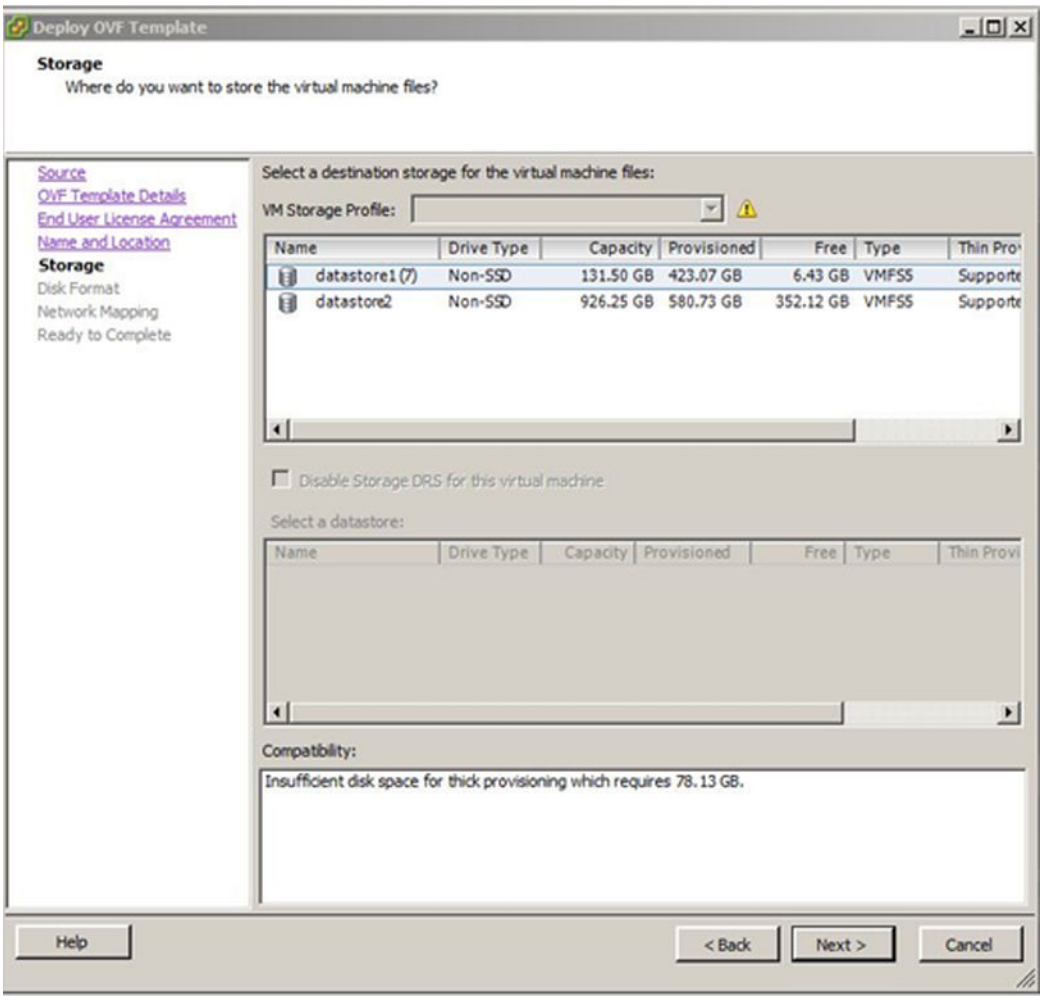


4. On the End User License Agreement screen, click **Accept** to accept the license and click **Next**.

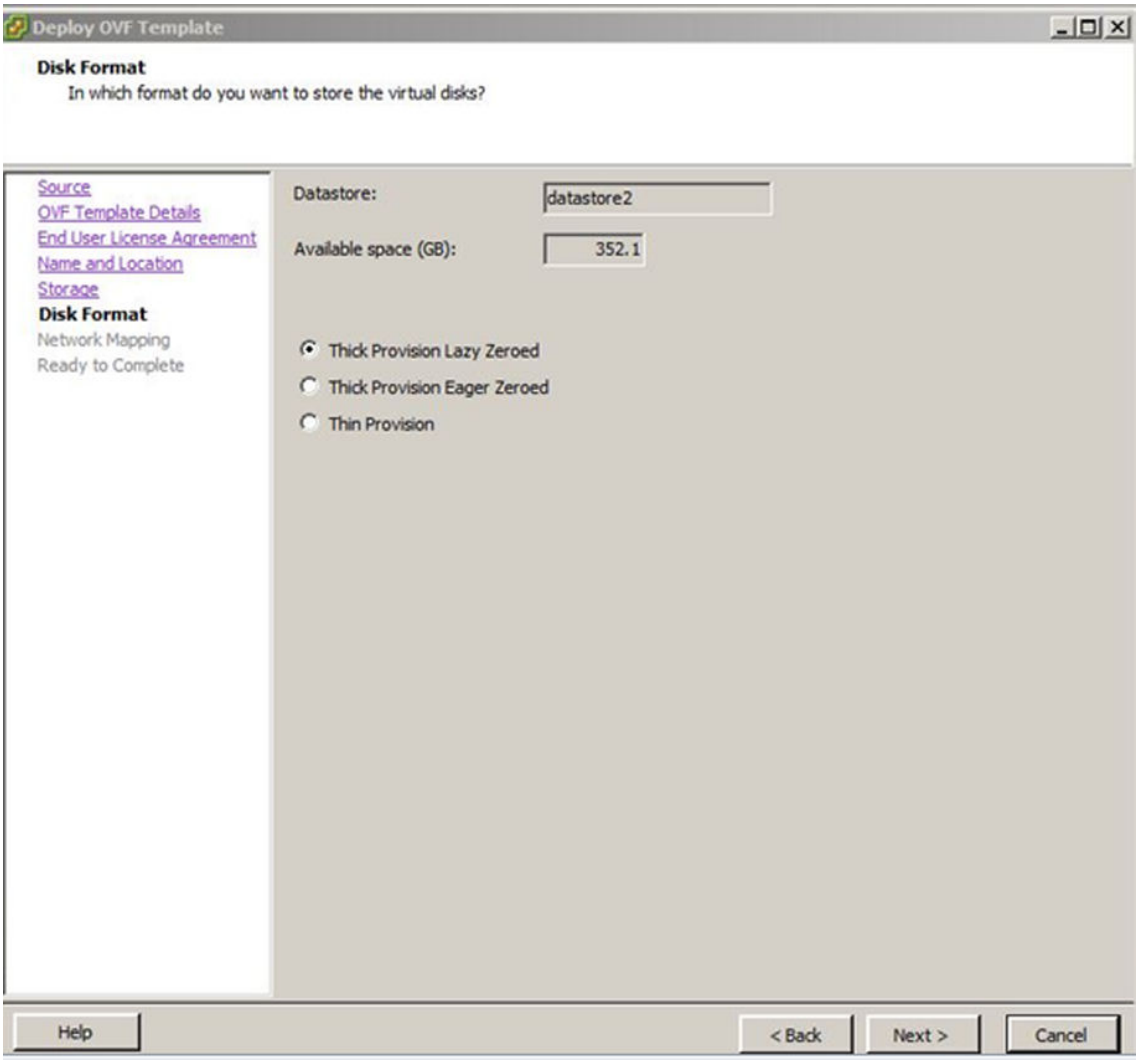
5. On the **Name and Location** screen, enter a name for the virtual machine and select the destination ESXi server. Click **Next**.



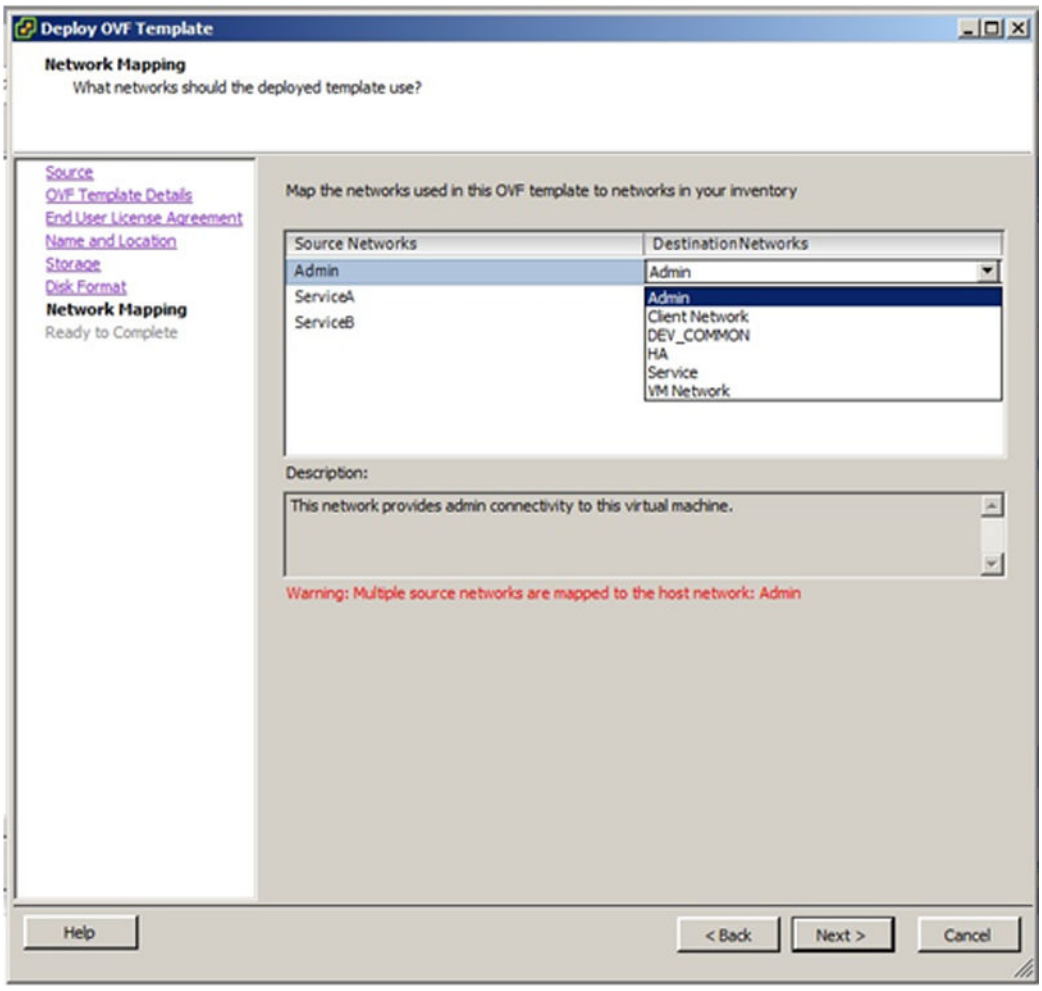
6. On the **Storage** screen, select the location where you want to store the files for the virtual appliance (requires approximately 79 GB) and click **Next**.



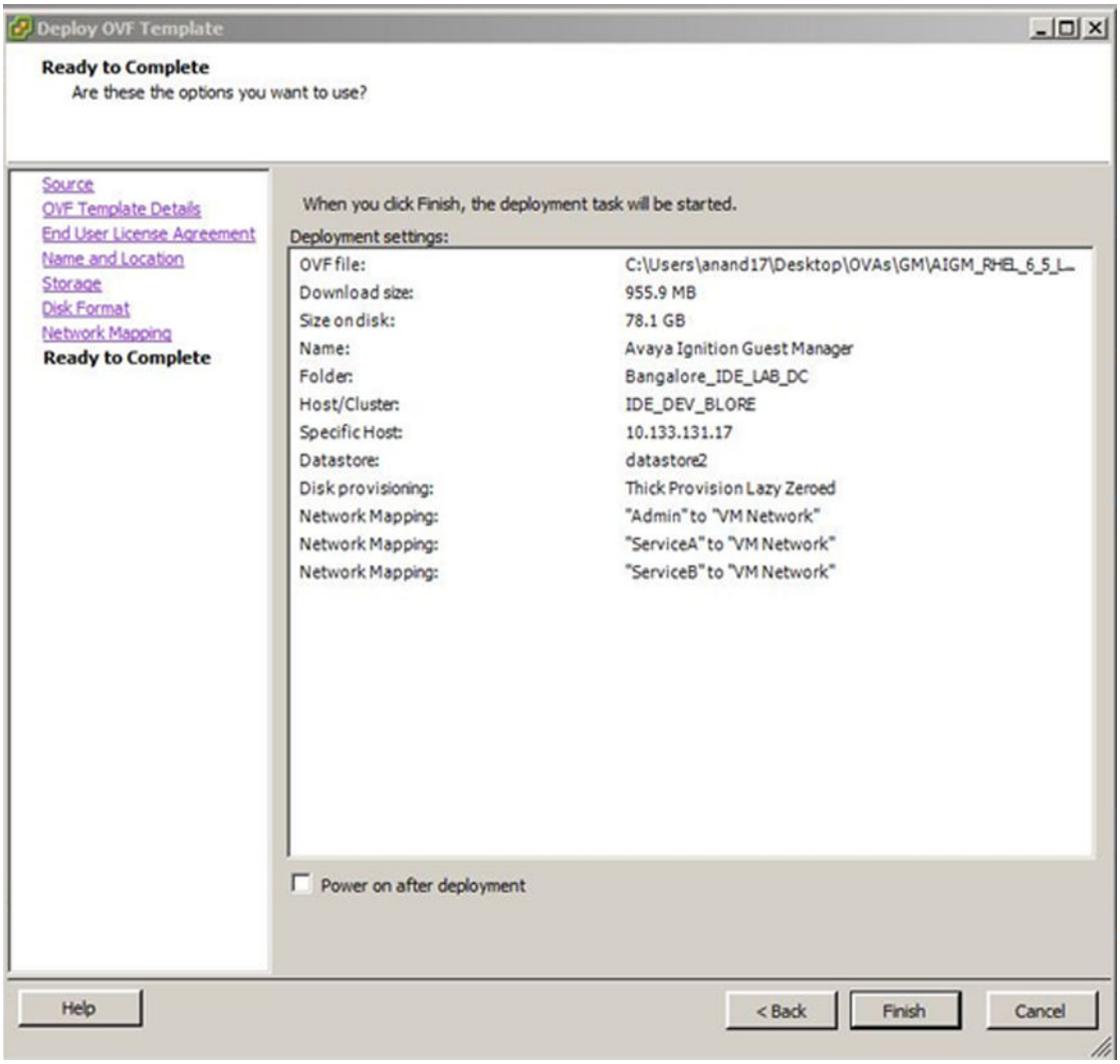
7. On the Disk Format screen, select a format in which to store the virtual machine's virtual disks and click **Next**.



8. On the Network Mapping screen, associate the Guest Manager network interfaces to the correct VM network, based on your site configuration.



9. On the Ready to Complete screen, review your settings. Use the **Back** button to make any changes or click **Finish** to start the import.



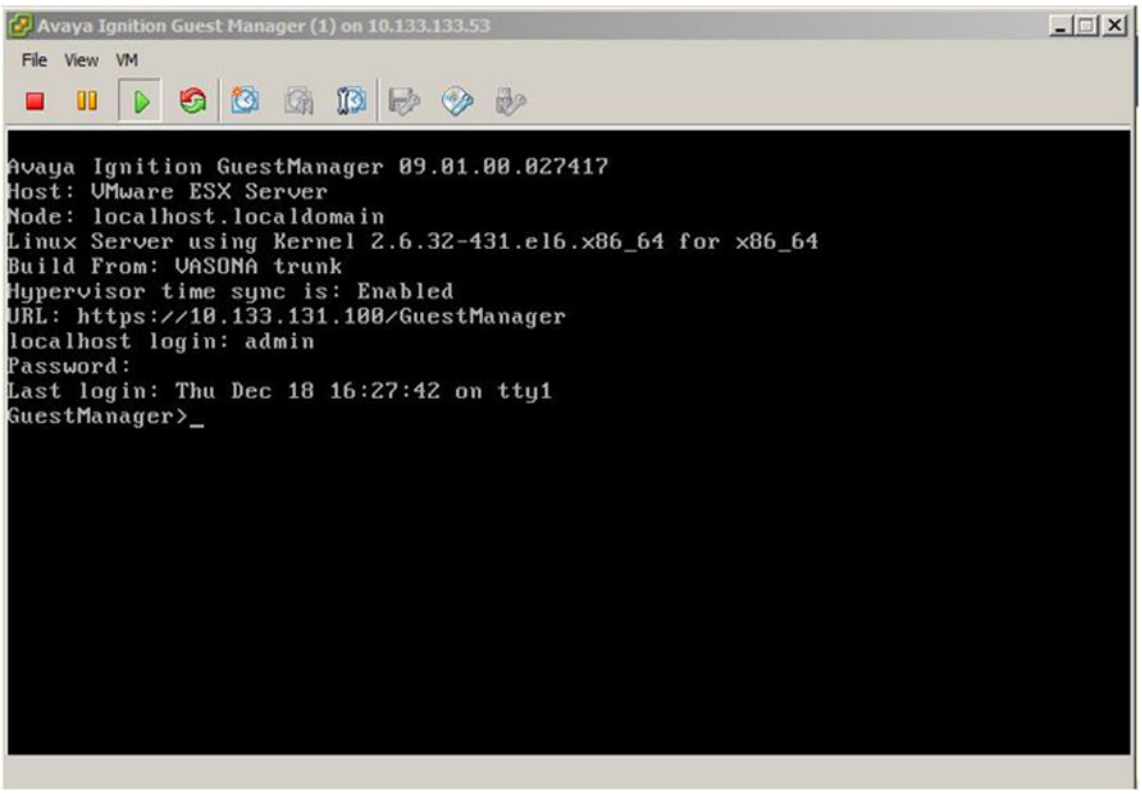
Configuring the Guest Manager virtual appliance

About this task

After the import completes, configure the VM settings. This is the minimum configuration required to start Guest Manager.

Procedure

1. Power on the VM and launch the Guest Manager console. Enter the username and password. The default username is `admin` and the default password is `admin`.



2. From the Guest Manager console, configure the IP address and subnet mask for the Admin port (eth0).

   Enter `interface eth0 ipaddr <ip_address/netmask in bits>`.

3. Configure the route from the Admin port (eth0) to the gateway.

   Enter `route add <subnet><[prefix|netmask]> <gateway_ip> [<interface>]`.

4. Configure the DNS settings.

   Enter `dns server primary NNN.NNN.NNN.NNN`.

5. Restart the Tomcat service.

   a. Enter `tomcat stop`.

   b. Enter `tomcat start`.

6. Enter `httpd restart`.

Configure HTTP and HTTPS connections

By default, Guest Manager supports HTTPS access only and comes with a default certificate to be used with HTTPS access. You can make the following changes:

- Configure HTTP access only
- Configure HTTPS access only and add a custom certificate to be used for HTTPS access
- Configure both HTTP and HTTPS access

Important:

You must enter an `httpd restart` for any changes related to HTTPD to take effect.

Configuring HTTP access

About this task

By default, Guest Manager supports HTTPS access only. You can configure Guest Manager to support HTTP access only.

Procedure

1. Log in to the Guest Manager VM as admin.
2. Enter `httpd listen http <interface>`.
3. Enter `httpd restart`.

Configuring HTTPS access

About this task

Guest Manager comes with a default certificate to use with HTTPS access. You can add a custom certificate to use with HTTPS access.

Important:

If you add a custom certificate, note the following:

- The only protocols supported for the URL are HTTP, HTTPS, and FTP.
- The URL must point to the file location directly and not through a proxy server.
- Make sure that the imported certificate/key does not have an associated password.
- Make sure that the FTP server is an anonymous FTP server (that is, no user name/password needed).

Important:

Guest Manager HTTPS mode supports only TLSv1 and above.

Procedure

1. Log in to the Guest Manager VM as admin.
2. Add a custom certificate. Enter
   a. `certificate installkey <url> [Display Name]`
   b. `certificate installcert <url> [Display Name]`

   The display name is optional. If you do not specify a display name, the file name is used as the display name. The name can have white space but must be enclosed in single or double quotes.
3. Configure HTTPS. Enter `httpd listen https <interface>`.
4. Enter `httpd key <Display Name>` where Display Name is the display name given when you installed the key. The name can have white space but must be enclosed in single or double quotes.
5. Enter `httpd cert <Display Name>` where Display Name is the display name given when you installed the certificate. The name can have white space but must be enclosed in single or double quotes..
6. Enter `httpd restart`.

Configuring HTTP and HTTPS access

About this task

Configure both HTTP and HTTPS access.

Procedure

1. Log in to the Guest Manager VM as admin.
2. Enter `httpd listen https <interface>`.
3. Enter `httpd allow http https`.
4. If you want to change the key for the HTTPS connection, enter `httpd key <Display Name>` where Display Name is the display name given when you installed the key. The name can have white space but must be enclosed in single or double quotes.
5. If you want to change the certificate for the HTTPS connection, enter `httpd cert <Display Name>` where Display Name is the display name given when you installed the certificate. The name can have white space but must be enclosed in single or double quotes..
6. Enter `httpd restart`.

Chapter 5: Configuring Guest Manager

This chapter shows the Avaya Identity Engines Ignition Guest Manager administrator how to launch Guest Manager for the first time, how to connect it to the Avaya Identity Engines Ignition Server appliance, and how to make application settings. When setting up Guest Manager for the first time, *you must follow the sequence of steps listed in this chapter*, unless the text states that the step is optional.

Command Line Interface

The Guest Manager command line interface (CLI) provides a limited set of administrative actions that you can perform on Guest Manager.

The CLI has a default timeout of 5 minutes.

Command	Description
certificate	Use to manage certificates.
dns	Configure the DNS setting.
exit	Exit the Guest Manager CLI.
halt	Halt the running system and power off the Guest Manager virtual machine.
httpd	Control the httpd server.
interface	Configure the interface settings.
passwd	Change the administrator account password.
reboot	Reboot the Guest Manager virtual machine.
reinit	Reinitialize the Guest Manager virtual machine to factory defaults.
route	Configure the route settings.
show certificates	Shows information about the certificates and keys in the certificate/key database.
show dns	Show the current DNS setting.
show httpd	Show information about the configuration and state of the httpd web server.
show interface	Show the current interface settings for a specific port or ports..

Table continues…

Command	Description
show route	Show the active routes in the system.
sshd	Enable or disable the sshd service.
tomcat[start|stop]	Control the Tomcat server.

certificate

The **certificate** command manages certificates.

Important:

HTTP, HTTPS, and FTP are the only supported protocols for the URL.

The URL must point to the file location directly and not through a proxy server.

Make sure that the imported certificate or key does not have an associated password.

Make sure that the FTP server is an anonymous FTP server (that is, no user name/password needed).

Syntax

```
certificate [installkey, installcert, delete, list, timeout, rebuild]
```

installkey <URL>[Display name]	Install the key. The URL-supported protocols are http, https, and ftp. Display name is optional. If you do not specify the display name, the file name is used for the display name.
installcert <URL>[Display name]	Install the certificate. The URL-supported protocols are http, https, and ftp. Display name is optional. If you do not specify the display name, the file name is used for the display name.
delete	Deletes the specified certificate or key.
list	Lists the installed certificates and keys.
timeout <NNN>	The transfer timeout value in seconds.
rebuild	Rebuilds the configuration database with only the default certificates.

Example

```
GuestManager>certificate
certificate [installkey,installcert,delete,list,timeout, rebuild]
            installcert <URL> [Display Name]
            installkey  <URL> [Display Name]
            URL supports protocols, http,https and ftp.
            Optional display name, if not specified the filename will be used.
            0 = No Timeout or 0 < timeout in second < 1000
            rebuild
```

show certificates

The **show certificates** command shows information about the certificates and keys in the certificate/key database. The command displays the name of the certificate, if deleting the certificate is allowed (you cannot delete the factory/default certificate), and if the item in the database is key or a certificate. It also displays the certificate and key that the httpd server is currently configured to use.

Syntax

```
show certificates
```

Example

```
GuestManager>show certificates
Name                                Delete Allowed  Type
Avaya Default Cert                  False           certificate
Avaya Default Key                   False           key

httpd is using certificate: Avaya Default Cert
httpd is using key        : None
GuestManager>_
```

dns

The **dns** command configures the DNS settings.

Syntax

```
dns server primary NNN.NNN.NNN.NNN

dns server secondary NNN.NNN.NNN.NNN

dns server <domain.com>

dns clear server all

dns clear server primary

dns clear server secondary

dns clear domain
```

Example

```
GuestManager>dns
dns server primary NNN.NNN.NNN.NNN
dns server secondary NNN.NNN.NNN.NNN
dns domain <domain.com>
dns clear server all
dns clear server primary
dns clear server secondary
dns clear domain
GuestManager>dns server primary 10.2.3.4
Reboot the GM VM to get updated DNS setting
GuestManager>_
```

show dns

The **show dns** command displays the current DNS settings, including the search domain, and the primary and secondary DNS server settings.

```
show dns
```

Example

httpd

The **httpd** command controls and configures the Apache HTTPD daemon. The httpd server is configured to automatically start at system boot time. Use the control commands to configure and manage the httpd server. You cannot disable the server.

The configuration actions are key, cert, listen, allow, and deny. For a configuration action to take effect, you must enter an **httpd stop**, **httpd start**, or **httpd restart** command.

Syntax

```
httpd <start|stop|restart|listen [http|https] <interface [,<interface>...]|key|cert <cert
or key name> allow <http|[,https]>| deny <http|[,https]>
```

listen The httpd listen command sets the interfaces/internet addresses that the httpd server listens on. Currently, ports 80 (http) and 443 (https) are supported.

key The key action takes the key name and if it is found in the configuration database, sets the ssl.conf file to use the specified key.

cert The cert action takes the certificate name and if it is found in the configuration database, sets the ssl.conf file to use the specified certificate.

Example

```
GuestManager>httpd
httpd <start|stop|restart|listen [http|https] <interface>[,<interface>...]|key|c
ert <Cert or key name>
start
stop
restart
allow the http and/or the https protocol.
      allow http
      allow https or httpd allow http https
key <key name>
cert <cert name>
<key|cert name> is Name shown by the
show certificates command.
key/cert names with whitespace/spaces need to quoted.
single or double quotes are allowed.
listen [http|https] <interface>[,<interface>]
       http port 80, https port 443, not specified both port 80 and 443
       where interface is one or more of: Admin|ServiceA|ServiceB|all
       where interface is one or more of: eth<0..N>[,eth<0..N>|all

specify one or more of the follow:
eth0, eth1, eth2
GuestManager>_
```

show httpd

The **show httpd** command display information about the configuration and the state of the Apache httpd server.

Syntax

```
show httpd
```

Example

```
GuestManager>show httpd
httpd server enabled                    : True
httpd server active                     : True
http port enabled                       : False
https port enabled                      : True
httpd is using certificate              : Avaya Default Cert
httpd is using key                      : Avaya Default Key
httpd server is listening on https:     : Admin      192.168.220.5
httpd server is listening on https:     : ServiceA   172.16.220.5
httpd server is listening on https:     : ServiceB   10.10.220.5
Active listening addresses from netstat:
tcp 192.168.220.5:https       LISTEN
tcp 172.16.220.5:https        LISTEN
tcp 10.10.220.5:https         LISTEN
GuestManager>_
```

interface

The **interface** command configures the interface settings.

Important:

You must enter an `httpd restart` command after you configure the interface settings.

Syntax

```
interface <port> <[enable|disable|stats]|[ipaddr <A.B.C.D>/netmask in bits]>
```

port is one of eth0, eth1, eth2, or Admin, ServiceA, ServiceB

Example

show interface

The **`show interface`** command displays interface information for a specific port or ports. If you do not provide a port, all of the ports in the operating system are shown. Separate the ports with white space or commas.

Syntax

```
show interface [port[,port]...]
```

port is one of eth0, eth1, eth2, or Admin, ServiceA, ServiceB.

Example

```
GuestManager>show interface
Name: Admin  IP Address: 10.33.131.19       Netmask/Prefix: 24
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:0c:29:e7:8b:1d brd ff:ff:ff:ff:ff:ff
    inet 10.33.131.19/24 scope global eth0
    inet6 fe80::20c:29ff:fee7:8b1d/64 scope link
       valid_lft forever preferred_lft forever

Name: ServiceA IP Address: 172.16.220.5       Netmask/Prefix: 255.255.255.0
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:0c:29:e7:8b:27 brd ff:ff:ff:ff:ff:ff
    inet 172.16.220.5/24 brd 172.16.220.255 scope global eth1
    inet6 fe80::20c:29ff:fee7:8b27/64 scope link
       valid_lft forever preferred_lft forever

Name: ServiceB IP Address: 10.10.220.5        Netmask/Prefix: 255.255.255.0
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:0c:29:e7:8b:31 brd ff:ff:ff:ff:ff:ff
    inet 10.10.220.5/24 brd 10.10.220.255 scope global eth2
    inet6 fe80::20c:29ff:fee7:8b31/64 scope link
       valid_lft forever preferred_lft forever
```

route

The **route** command adds static routes to the system.

Syntax

```
route add|delete <subnet><[prefix|netmask] <gateway_ip> [<interface>]
```

Example

```
GuestManager>route add 0.0.0.0/0 10.133.133.1
GuestManager>_
```

show route

The **show route** command displays the operating system routing table in the same format as the RedHat Linux operating system at the Unix shell.

Syntax

```
show route
```

Example

```
GuestManager>show route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.33.131.0     *               255.255.255.0   U     0      0        0 eth0
10.10.220.0     *               255.255.255.0   U     0      0        0 eth2
172.16.220.0    *               255.255.255.0   U     0      0        0 eth1
```

sshd

The **sshd** command lets you enable or disable sshd service.

Syntax

```
sshd <enable|disable>
```

Important:

In Release 9.1, only `sshd enable` and `sshd disable` are supported. The optional interface and port parameters will be supported in a future release.

Example

```
GuestManager>sshd
sshd <enable|disable> [<interface> <port>]
Note: <port> must be between 1 and 65535 inclusive.
Interface may be "all" or a specific interface.
If you want to have sshd on multiple interfaces
issue sshd enable for each interface
to enable sshd on multiple interfaces.
disable only requires the interface or "all".
The following interfaces are available:
     where interface is one of the following:
     Admin, ServiceA, ServiceB
     eth0, eth1, eth2
```

tomcat

The **tomcat** command lets you start, stop, or view the status of the Tomcat service that is hosting the Guest Manager web application.

Syntax

```
tomcat <start|stop|status>
```

To restart the Tomcat service, enter

1. `stop tomcat`
2. `start tomcat`

Example

```
GuestManager>tomcat
tomcat <start|stop|status>

GuestManager>tomcat start
Starting tomcat6: [  OK  ]

GuestManager>tomcat status
tomcat6 (pid 2170) is running...[  OK  ]
```

About usernames and passwords

Important:

Configuring and using Guest Manager requires a number of different Ignition Server administrative accounts:

- **Guest Manager administrator**: The principal administrator of the Guest Manager application. Only the Guest Manager administrator can configure Guest Manager and create Provisioners. By default, the user name and password for the Guest Manager administrator are admin/admin. After installation, make sure you change the password as shown on Setting the Administrator Username and Password on page 69.
- **Guest Manager virtual appliance administrator**: These are the credentials that you use to configure the Guest Manager virtual appliance. By default, the user name and password for the Guest Manager virtual appliance administrator are admin/admin.
- **Ignition Server SOAP API user credentials**: These are the credentials the Guest Manager application uses to connect to the SOAP API on the Ignition Server appliance. Instructions for this appear in the section Making SOAP settings on the Ignition Server on page 55.
- **Ignition Server administrator**: The administrator who runs Ignition Dashboard and manages the Ignition Server appliance. You need these credentials in order to configure the Ignition Server appliance and to create guest user authorization policies.
- **Guest Manager provisioners**: These are the login accounts of front desk personnel who create and manage guest users in Guest Manager. Their user accounts can be stored locally in Ignition, or they can be accounts in your LDAP or AD user store.

For additional information on the various accounts used to configure and run Guest Manager, see Types of accounts in your Ignition Server installation on page 18.

Launching Guest Manager

This section describes how to launch Guest Manager to check that it has been installed correctly. At this point in the configuration procedure, you can run Guest Manager but you cannot connect it to the Ignition Server appliance because the connection settings have not been made.

Guest Manager is made up of two applications:

- **Administrator Application**: The application that the Guest Manager administrator uses to configure Guest Manager and to create provisioner accounts. Only the Guest Manager administrator can use it.
- **Provisioner Application**: The application that provisioners use to create guest users.

Connect to the Administrator Application as described in the following procedure.

Procedure

1. Open a web browser and point the web browser to the Guest Manager Administrator application at https://<server_name>/GuestManager/admin.
2. Enter the login credentials of the Guest Manager administrator. By default, these are:
   - Username: `admin`
   - Password: `admin`

   If your browser asks whether you want it to remember your password, you must choose the option that prevents the browser from storing passwords for the site. On most browsers, you choose the option, “Never for this site.” Allowing the browser to retain passwords for the Guest Manager application is not secure, and it can cause your browser to display misleading password update messages when you edit users.
3. Click **Login**.

   The Guest Manager administrator window displays. You are now successfully logged in to Guest Manager as the Guest Manager administrator. At this point Guest Manager is not connected to an Ignition Server appliance.
4. Change the administrator password.

   In the toolbar on the left, click on **Administration** > **Account**. In the Administrator Account screen, click on **Administrator Password:** `Change`. Type your current and new passwords and then type your new password again in the **Confirm Password** field. You can also change the Administrator User Name. Click **Submit**.

   Important:

   When using Guest Manager, *do not* use your browser’s Refresh command to update a page. Instead, click the appropriate command button on the left side of the window to reload the page. *Do not* open a link in a new tab at any time.

Next steps

Do one of the following:

- If your provisioner accounts will be stored on the Ignition Server only (that is, if you will create all of your provisioners in Guest Manager), you can skip the following policy sections and go immediately to Installing the SOAP certificate on page 53.
- If any of your provisioner accounts are stored in LDAP or AD, go to Creating a Provisioner access policy on page 47.

Creating a Provisioner access policy

This section explains how to create a policy that gives certain users in your LDAP or Active Directory (AD) store the right to act as provisioners in Guest Manager. This policy is called a “provisioner access policy” or a “Guest Manager access policy.” Your provisioner access policy

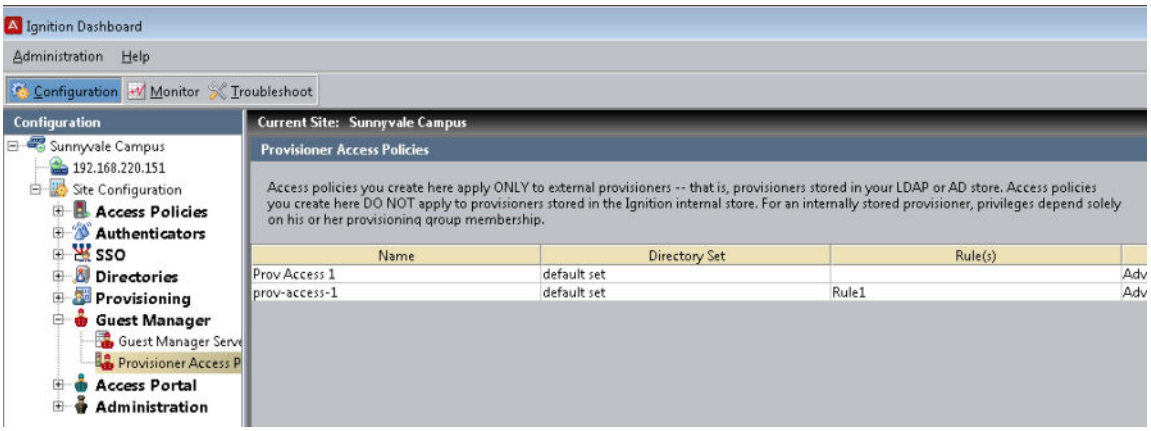
determines how Ignition Server looks up provisioner accounts in LDAP or AD, and what type of provisioner access it grants to each provisioner.

Provisioner access policies do not apply to internal provisioners (provisioners stored in the Ignition Server internal store). If you plan to use only internal provisioners, skip this section and go to Making RADIUS Settings on the Ignition Server on page 58.

Follow this procedure to configure LDAP or AD authorization of your provisioners.

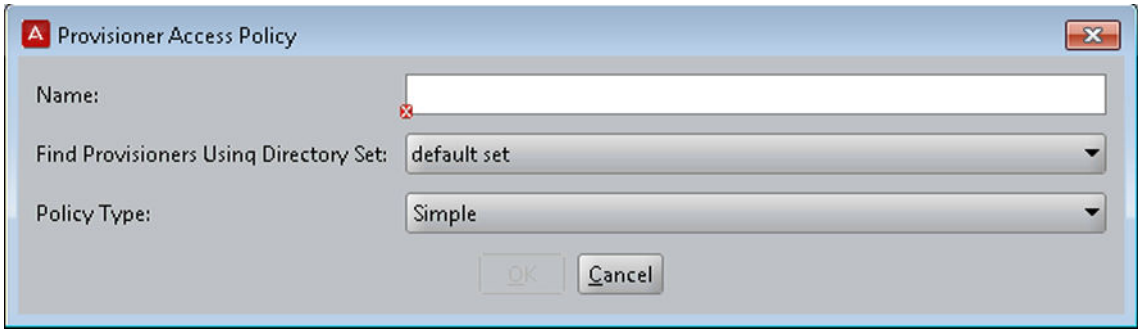
Procedure

1. Create the directory services, directory sets, and virtual groups that let Ignition Server look up your provisioners and find the groups that contain them. In Ignition Dashboard (not Guest Manager), do the following:
   - Create a directory service for each LDAP or AD store that holds provisioner accounts. If a directory service is already in place for the desired LDAP or AD store, use that one. For instructions, see the section “Connecting to Active Directory” or the section “Connecting to an LDAP Service” in *Avaya Identity Engines Ignition Server Administration*, NN47280-600.
   - In Ignition Dashboard, create a directory set that contains the directory service(s) you just created. If a suitable directory set is already in place, use that one. For instructions, see the section “Directory Sets” in *Avaya Identity Engines Ignition Server Administration*, NN47280-600.
   - Create a virtual group for each group in AD or LDAP whose provisioners you wish to treat as a distinct group of provisioners in Guest Manager. For instructions, see the section “Virtual Groups” in *Avaya Identity Engines Ignition Server Administration*, NN47280-600.
2. Create the provisioner access policy in Ignition Dashboard:



   - Click the **Configuration** tab in Ignition Dashboard and, in the tree, open the **Guest Manager** node. Click **Provisioner Access Policies** and then click **New**.

     The provisioner access policies are only needed for LDAP- and AD-stored provisioners, not for internal provisioners (provisioners kept in the Ignition Server internal store). Internal provisioners are granted privileges based on their provisioning group membership, assigned as described in Managing provisioning groups on page 126.
   - In the Provisioner Access Policy window, type a **Name** for this policy.



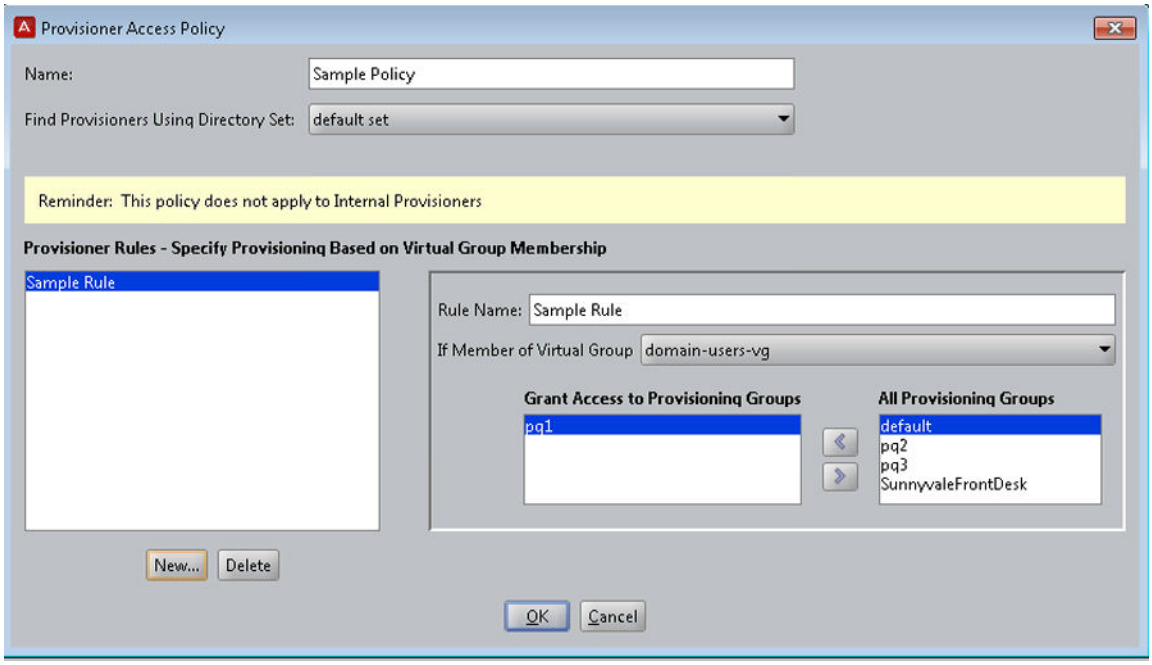
- In the **Find Provisioners Using Directory Set** drop-down list, choose the directory set you created or found in Step 1 on page 48.
- In the **Policy Type** drop-down list, choose **Simple** or **Advanced**.

  A Simple policy lets you map each virtual group to one or more provisioning groups; an Advanced policy lets you consider more criteria. If you choose Simple, continue to follow this procedure. If you choose **Advanced**, go to Creating an Advanced Provisioner access policy on page 51.
- Click **OK**.

  The **Provisioner Access Policy** window displays. This window lets you write rules that assign each provisioner to one or more provisioner groups.

  When a provisioner logs in, Ignition Server checks the provisioner access policy to set the rights of the provisioner. The policy consists of rules. Each rule checks whether the provisioner is a member of a virtual group, and, if so, it assigns the provisioner to a corresponding provisioning group or set of provisioning groups.

  Membership in a provisioning group sets the rights of the provisioner, including what resources the provisioner can grant access to and the maximum period of validity for guest accounts the provisioner creates.



3. Working in the Provisioner Access Policy window, write the rules that form your provisioner access policy:
   - Below the **Provisioner Rules** list, click **New**.
   - In the **Create New Rule** window, type a name for the rule and click **OK**.
   - In the panel on the right, in the **If Member of Virtual Group** field, choose a virtual group (you found or created the virtual groups in 1 on page 48).
   - In the **All Provisioning Groups** list, click on the provisioning group that corresponds to the virtual group you just selected. Click the left-pointing arrow button to add that group to the **Grant Access to Provisioning Groups** list.
   - *Optionally*, choose additional groups from the **All Provisioning Groups** list and click the left-pointing arrow button to add them to the list. A provisioner can be a member of more than one provisioning group.
   - *Optionally*, if you need to map more virtual groups, click **New** again and add more rules.
4. Click **OK**.

   Your policy is complete.
5. *Optionally*, if you run multiple installations of Guest Manager, you have the option of creating a unique policy for each installation, if needed. To do this, click **New** at the bottom of the **Access Policies** panel and repeat the procedure to create another provisioner access policy.

Next steps

Go to Installing the SOAP certificate on page 53.

Creating an Advanced Provisioner access policy

This section explains how to create a provisioner access policy with complex rules that assign provisioner rights. If you do not understand provisioner access policies, read the section, Creating a Provisioner access policy on page 47, before you create your advanced policy.

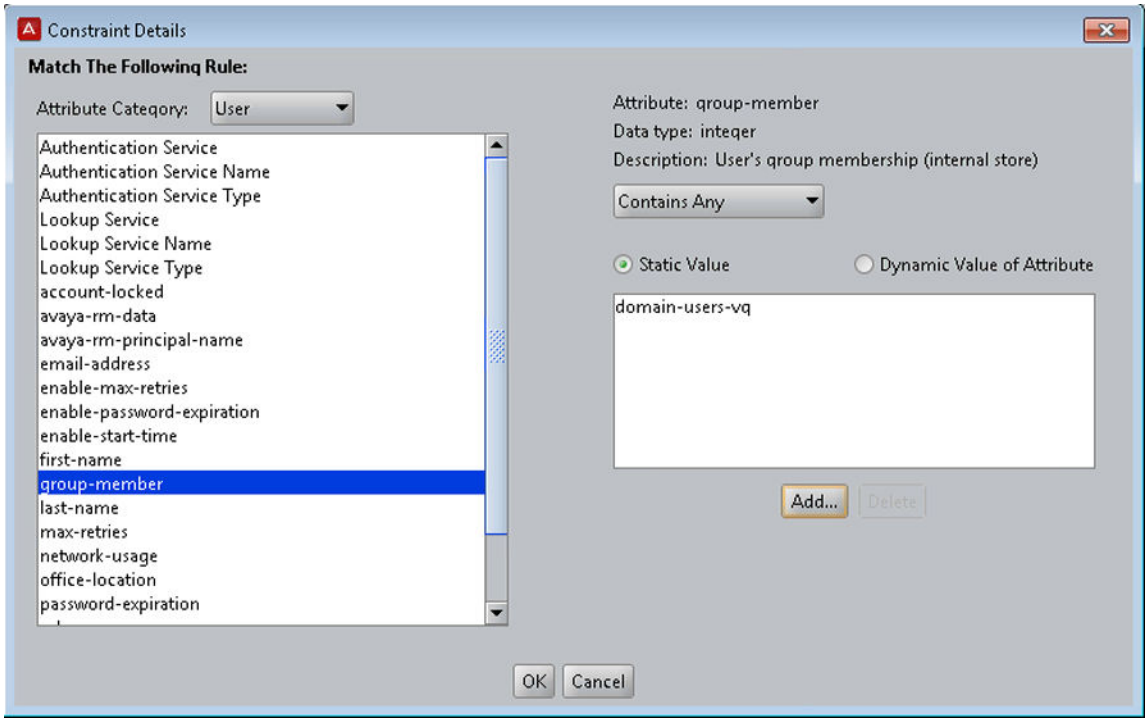
Follow these steps to set up advanced, rule-based authorization for you LDAP or AD-stored provisioners.

Procedure

1. Create the directory services, directory sets, and virtual groups that contain your provisioner accounts. See the Creating a Provisioner access policy on page 47 for instructions.
2. Create the provisioner access policy in Ignition Dashboard. In Dashboard's **Configuration** tree, open the **Guest Manager** node and click on **Provisioner Access Policies**.
3. Click **New** at the bottom of the window.
4. In the Provisioner Access Policy window, enter a name for this policy. In the **Find Provisioners Using Directory Set** drop-down list, choose the directory set that contains your provisioners.
5. In the **Policy Type** drop-down, choose **Advanced**.
6. Click **OK**.

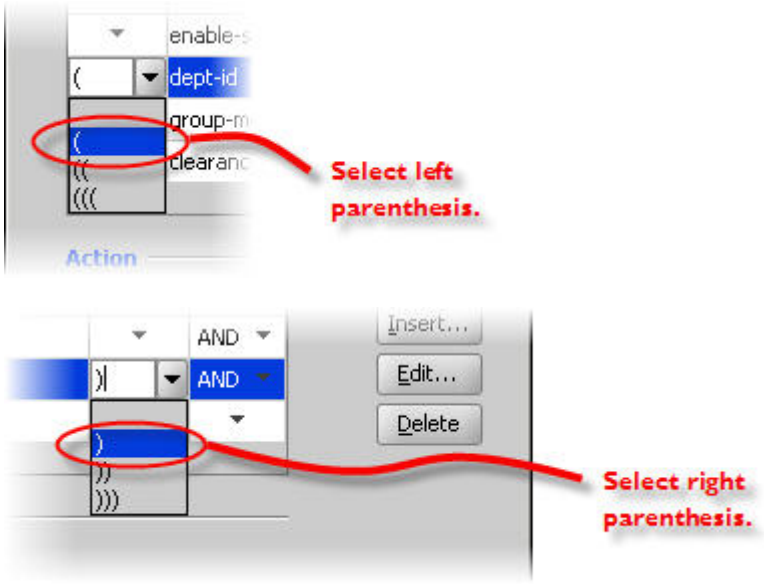
   The Edit Provisioner Access Policy window appears. This window lets you write rules that assign each provisioner to one or more provisioner groups.
7. In the Authorization Policy section of the window, click **Edit**.

   The Edit Authorization Policy window appears. The left side of the window lists the rules that form your policy, and the right side of the window lets you edit a rule. The Constraint table shows the logical statement that must be satisfied to allow or deny access to the provisioner. You use the AND/OR conjunctions to assemble a series of tests into a constraint.
8. Below the **Rules** list, click **Add**.
9. In the New Rule window, give the rule a **Name** and click **OK**.
10. To add decision logic to your rule, add one or more constraints in the Constraint table. Each **constraint** tests the value of an attribute. If there are multiple constraints, join them into a single logical statement using the AND and OR conjunctions and, if needed, parentheses. Follow the steps below:
    - On the left side of the Edit Authorization Policy window, make sure you have highlighted the name of the **Rule** you want to edit.
    - To the right of the **Constraint** table, click the **New** button. The Constraint Details window appears.



- In the **Attribute Category** drop-down list, choose the type of attribute you want to test. For explanations of the types, see *Avaya Identity Engines Ignition Server Administration*, NN47280-600.
- Choose the attribute: After you select a type, the list box below the **Attribute Category** field shows the available attributes that match the type you selected. Click on the name of the attribute whose value the constraint should test. In the upper right corner, the window displays the **Data type** of the attribute.
- In the drop-down list just below the **Data type** field, choose the comparison operator, such as, *Equal To* or *Contains*. This dropdown list contains the operators appropriate to the data type of the attribute you have selected.
- Provide the comparison value by doing one of the following:
  - If you want to compare the attribute value with a fixed test value, tick the **Static Value** radio button and type or choose the comparison value in the field below that.
  - If you want to compare the attribute value with a value retrieved from another attribute, tick the **Dynamic Value of Attribute** radio button. In the field just below that, choose the attribute category ((User, System, or Authenticator). In the next field, choose the attribute that should provide the comparison value. The list of attributes contains only those attributes whose data type matches the data type of the attribute on the left side of the constraint.
- Click **OK** to close the Constraint Details window.
- In the Edit Authorization Policy window, next to the **Constraint** table, click the **New** or **Insert** button to add more constraints. **New** adds a constraint at the end of the list, and **Insert** adds it above the currently selected row.

- Add parentheses as necessary to group constraints. To do this:
  - In the **Constraint** section of the Edit Authorization Policy window, find the first constraint to be grouped.
  - Click in the field to the left of the constraint, and click the down-arrow to show the list of parentheses. Click on an appropriate opening parenthesis mark to select it.
  - Find the last constraint to be grouped. Click in the field to the right of the constraint, and click the down-arrow to show the list of parentheses. Click on an appropriate opening parenthesis mark to select it. Click the constraint to complete your entry.



- Use the **AND** and **OR** conjunctions to form a logical condition statement.
- After you have finished adding constraints, click:
  - the **Allow** button to allow provisioners for whom rule evaluates to TRUE; or
  - the **Deny** button to disallow provisioners for whom rule evaluates to TRUE. For information on the precedence of Allows and Denies in Ignition, see “How Ignition Server Evaluates a User Authorization Policy” in the *Avaya Identity Engines Ignition Server Administration*, NN47280-600*Avaya Identity Engines Ignition Server Administration*, NN47280-600.

Installing the SOAP certificate

Guest Manager and the Ignition Server each have installed copies of a common *SOAP service certificate* to secure their communications. Guest Manager cannot connect without this. Your installation comes with a default certificate that is acceptable for test installations. In a production installation, you should replace both copies with your own certificate for added security. If you intend

to continue using the default certificate, you may skip this section and proceed to Making SOAP settings in Guest Manager on page 57.

Important:

Make sure that the certificate does not have a password associated with it. The certificate encoding format must be either DER-encoded binary X.509 or Base64–encoded X.509.

About this task

Use the procedure below to install a new SOAP service certificate in Ignition Server and Guest Manager. This procedure is optional, and you should only perform these steps if you are prepared to replace the certificate both on the Ignition Server and in Guest Manager.

Procedure

1. Run Ignition Dashboard and create and import your new certificate as explained in *Avaya Identity Engines Ignition Server Administration*, NN47280-600.
2. Designate your new certificate as the *SOAP service certificate* as explained in *Avaya Identity Engines Ignition Server Administration*, NN47280-600.
3. Get a copy of the SOAP service certificate. (Ask your Ignition Server Administrator for this if necessary.) The certificate must be saved in a text file, and:
   - The certificate file must contain one and only one PEM-encoded certificate.
   - In the file, the certificate starts with the line, “-----BEGIN CERTIFICATE-----” and ends with the line, “-----END CERTIFICATE-----”. Make sure there is no text before the “BEGIN” line and no text after the “END” line.
4. Open a web browser and point the web browser to the Guest Manager Administrator application at https://<server_name>/GuestManager/admin.
5. Enter your Guest Manager administrator login credentials and click **Login**. Do not allow the browser to remember your password.
6. Select **Administration** > **Connection** > **Certificate** from the navigation area of the Administrator Application.
7. Click the **Add Certificate** button.
8. In the Add Certificates window, click **Browse** to load the certificate file. In the browser window, select the file name and click **Open**.
9. In the **Alias For This Certificate field**, enter a short name for the certificate. You may use any name; Ignition Server uses this alias as a key to identify the certificate in the keystore.
10. Click **Submit**. Ignition Server adds the selected entry to Guest Manager’s **Trusted Certificates** list. The installed certificate resides in the Guest Manager keystore.

    Important:

    Do not confuse the *Guest Manager keystore* with the *browser keystore* and the certificates that secure HTTPS browser sessions. For information on setting up HTTPS security, see Configure HTTP and HTTPS connections on page 36.

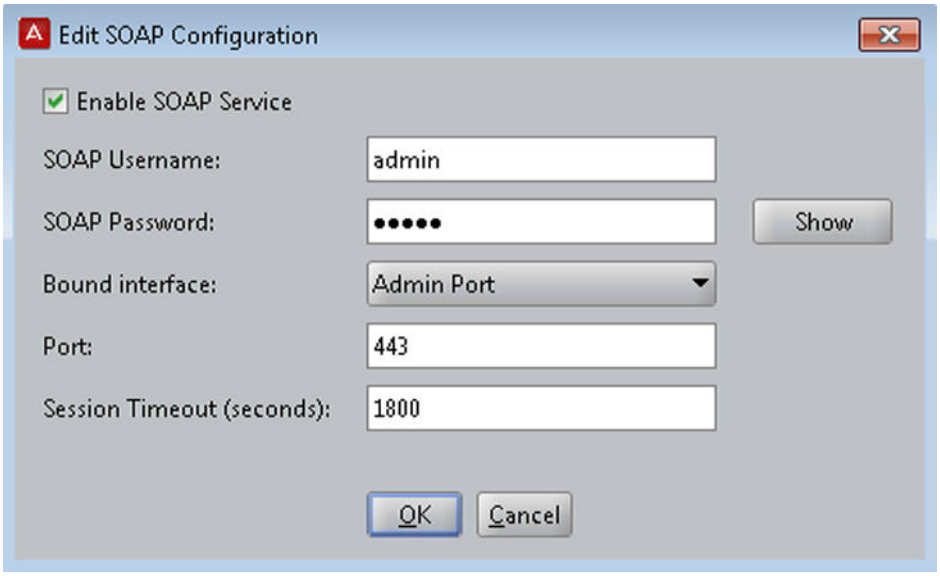
Making SOAP settings on the Ignition Server

In this and the next few sections, you will make the settings that allow Guest Manager and the Ignition Server to communicate. Guest Manager connects to the Ignition Server appliance through the appliance's SOAP service, and it authenticates provisioners using the appliance's RADIUS service. The sections below show how to enable the SOAP and RADIUS services on the Ignition Server appliance and how to connect Guest Manager to the appliance.

Follow the steps below to enable the SOAP service on the Ignition Server. This section is based on the instructions in the *Avaya Identity Engines Ignition Server Administration*, NN47280-600. Always check that document for the latest information on the SOAP service.

Procedure

1. Launch Ignition Dashboard (see Launching Ignition Dashboard on page 154) and log into your Ignition Server as administrator.
2. In Dashboard's Configuration Hierarchy panel, click the name of your site (by default, "Site 0").
3. In the Sites panel, click the **Licenses** tab. Make sure the licenses list contains a license called "Guest Manager". If this license is missing, you must add it. For instructions, see *Avaya Identity Engines Ignition Server Administration*, NN47280-600.
4. In the Sites panel, click the **Services** tab and click the **SOAP** tab. If there is no SOAP tab, it means your SOAP license is expired. See the preceding step.
5. Click on the **Edit** button in the SOAP tab. The Edit SOAP Configuration window appears.



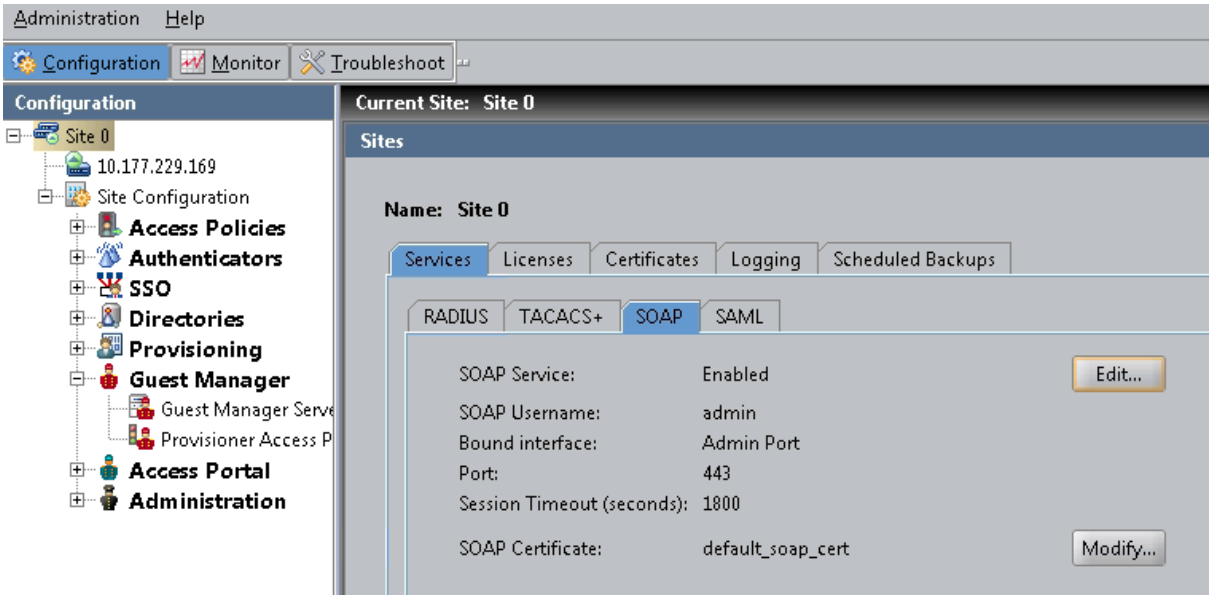
6. Edit the entries as follows, and make a note of these entries. You will use them to connect Guest Manager to the appliance in Make SOAP Settings in Guest Manager on page 57.
7. Set the SOAP connection parameters:
   - **Enable SOAP Service**: Check this check box to make the SOAP API service available.

- **SOAP Username**: This is the login name that Guest Manager and other SOAP API clients use to connect to the service. This is not an account in the internal store; by typing a name and password here, you are creating the SOAP user account. Do not use spaces or *hyphens*. Type only letters and numbers.
- **SOAP Password**: Password that SOAP user account uses to connect.
- **Bound Interface**: From the drop-down list, choose the Ignition Server Ethernet interface that is intended to handle SOAP traffic. You can bind the SOAP service to any port on the Ignition Server. If you are running an HA pair of Ignition Servers, you can choose to bind to a VIP interface. The VIP names are also listed in the drop-down list. For further information on using VIPs, see *Avaya Identity Engines Ignition Server Administration*, NN47280-600 .
- **Port**: Enter the port number to which API clients should connect. Traffic through this port is HTTPS traffic.
- **Session Timeout**: This is the SOAP*client timeout* setting. Enter the period, in seconds, after which the SOAP API connection is automatically reset. This timeout ensures that unused sessions are closed at the expiration of the timeout period, but it does not cause Guest Manager to become disconnected since Guest Manager automatically reconnects. Avaya recommends setting this interval to 1800 seconds. See SOAP Client Timeout Threshold on page 71.

  Important:

  Set the SOAP **Session Timeout** to a period of 180 seconds or longer. Setting it to a shorter period can result in Guest Manager being unable to load large sets of users.

8. Click **OK**.



The connection settings are complete. Next, start and connect Guest Manager as explained below.

Making SOAP settings in Guest Manager

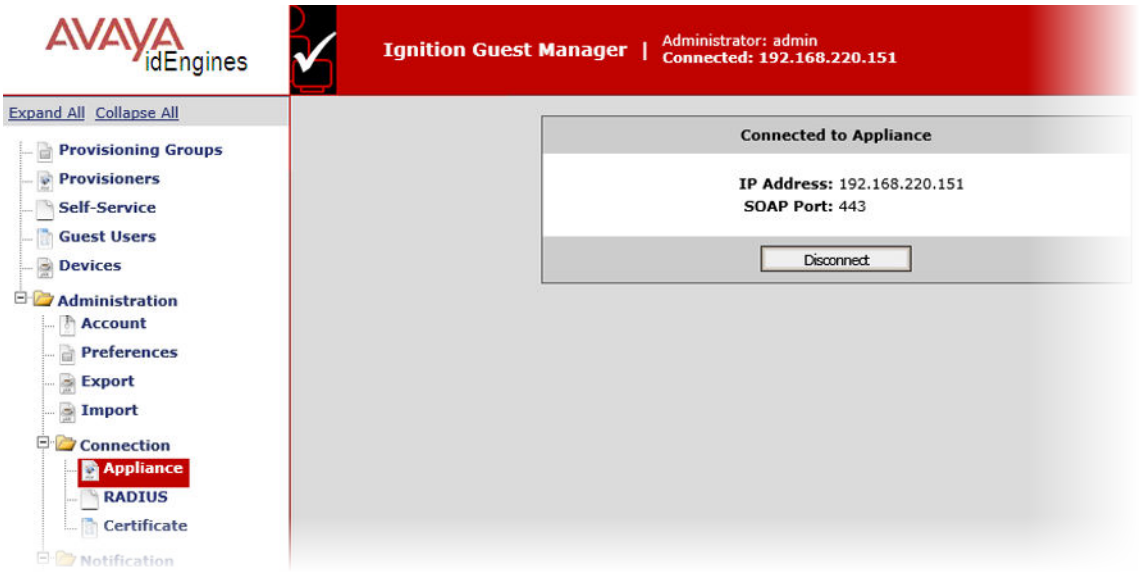
Specify your SOAP settings in Guest Manager.

Procedure

1. Open a web browser and point the web browser to the Guest Manager Administrator application at https://<server_name>/GuestManager/admin.
2. Enter your Guest Manager administrator login credentials (*admin/admin* is the default) and click **Submit**. Do not allow the browser to remember your password.
3. Click on **Administration** > **Connection** > **Appliance** in the toolbar of the Administrator Application.

   This command lets you connect to and disconnect from an Ignition Server appliance.
4. In the Login to Appliance screen, enter the SOAP service connection settings of your Ignition Server appliance. These are the settings you established in Making SOAP settings on the Ignition Server on page 55.
   - **IP Address**: Enter the IP address of the Ignition Server's Admin Port (or its VIP port if your SOAP service is bound to a VIP port). To find this IP address, launch Ignition Dashboard and look in the System Explorer window.
   - **SOAP Port**: Enter the HTTPS port of the appliance's SOAP service.
   - **Username** and **Password** for the Ignition Server SOAP API user account. These are the credentials you created in Making SOAP settings on the Ignition Server on page 55.
5. Click **Connect.**

   The **Connected to Appliance** screen appears confirming the appliance connection. Guest Manager displays the name of the appliance to which you are connected.



The connection disconnects after the timeout interval specified in Making SOAP settings on the Ignition Server on page 55.

Making RADIUS Settings on the Ignition Server

Create a *Guest Manager Server entry* in Ignition. This entry allows Ignition Server to recognize Guest Manager as a RADIUS authenticator that will be sending authentication requests.

When a provisioner logs into the Guest Manager Provisioner Application, the application uses RADIUS to authenticate the provisioner against the Ignition Server. Each provisioner account is stored either in the Ignition Server internal store or in your LDAP/AD store; in both cases, Guest Manager authenticates the provisioner by sending a RADIUS request to the Ignition Server.

To prepare for RADIUS authentication, you must set up the Guest Manager-Ignition Server connection as follows.

Procedure

1. Launch Ignition Dashboard if it is not running already, see Launching Ignition Dashboard on page 154.
2. In the main Dashboard window, click the **Configuration** button.
3. In the **Configuration** hierarchy tree, expand the **Guest Manager** node and click **Guest Manager Servers**. The **Guest Manager Server Summary** panel appears, displaying all the Guest Manager installations that can connect to this Ignition Server.
4. Click **New** near the bottom of the window.
5. In the Guest Manager Server Details window, type a **Name** for your Guest Manager installation, and type the **IP Address** of the machine on which you installed Guest Manager.
6. Enter a hard-to-guess string as your **RADIUS Shared Secret**. Make a note of your shared secret. You will need it when you set up the RADIUS connection.
7. In the **Provisioner Access Policy field**, choose the appropriate policy.
8. Click **OK**.
9. Make sure your firewall settings permit RADIUS traffic between Guest Manager and Ignition. Guest Manager uses RADIUS to authenticate provisioners. Your network must allow RADIUS (UDP) traffic to travel between the Guest Manager machine and the Ignition Server.

   The Guest Manager configuration in the Dashboard Configuration tree governs only Provisioner logins. That means that certain Guest Manager features, such as self-provisioning portals, are unaffected by these settings. Once you have deployed a self-provisioning portal, it will continue to function, regardless of changes you make to the Guest Manager configuration in the Dashboard Configuration tree.

Making RADIUS settings in Guest Manager

Ignition Server uses RADIUS to authenticate provisioners.

Procedure

1. In the Guest Manager Administrator Application, select **Administration** > **Connection** > **RADIUS**.
2. In the RADIUS configuration screen, type the **RADIUS port number** where the Ignition Server RADIUS service is running. By default, this is 1812.
3. In **Shared Secret** field, enter the shared secret. If the shared secret was previously set, click **Change**.
4. In the **Timeout** field, specify a period (in seconds) after which Guest Manager will retry the RADIUS login if it does not receive a response.
5. Click **Submit**.

Testing Guest Manager's RADIUS connection settings

Follow these steps to test your RADIUS setup.

Procedure

1. Create a provisioner account for yourself as explained in Creating a Provisioner access policy on page 47.
2. Open a web browser and point the web browser to the Guest Manager Provisioner application at https://<server_name>/GuestManager/provisioner.
3. In the Login screen, enter your provisioner **Username** and **Password**.
4. Click **Sign In**. If your login attempt fails, see Problem: Provisioner cannot login on page 152.

Setting up Email notification parameters

When provisioners create guest user accounts, the usual way to give the guest his or her new username and password is by email. Alternatively, you can send the credentials in an email to your front desk receptionist, for example, who prints them and passes them to the guest.

Important:

You can use a public mail server such as Gmail or Yahoo as the SMTP server; however, there are some limitations with these web-based SMTP servers. Emails sent using Web-based SMTP servers are likely to be marked as spam by mail clients including Outlook. Guest users need to be made aware of this so that they do not overlook the mail.

Yahoo's SMTP comes with a strict limit of 500 outbound emails per day (and each message can be sent up to 100 recipients), to prevent spammers from using it for their unsolicited messages.

Gmail's SMTP comes with severe sending limits to prevent spammers from using its outgoing server to blast out garbage emails. The boundary is 100 recipients a time and 500 messages per day. If you cross this restriction, Google blocks your account.

Procedure

1. Launch the Guest Manager Administrator application.
2. Select **Administration** > **Notification** > **E-mail**.
3. On the Email SMTP Configuration page, check the **Enable Sending of Email Notification** check box. With this feature turned on, Guest Manager sends guest users, provisioners, and/or others an email notification when guest user accounts are created and/or updated.
4. In the **From Address** field, type the email address that will appear in the “From” line of the messages that Guest Manager sends. For example, user provisioning notifications might contain a **From Address** such as guestreception@idengines.com. This address appears in all types of emails that Guest Manager sends.
5. In the **Server** field, enter the fully-qualified domain name or the IP address assigned to the mail server that will transmit email notifications from Guest Manager.

   You can enter a public main server such as Gmail or Yahoo as the SMTP server.
6. For SSL connections, in the **Use SSL** field, select **Yes** and do the following:
   a. In the **SSL certificate** field, check **Custom** to import the SMTP server certificate (**Administration** > **Connection** > **Certificate**). When you successfully import the certificate, this certificate is used to establish trust with the SMTP server.

      Important:

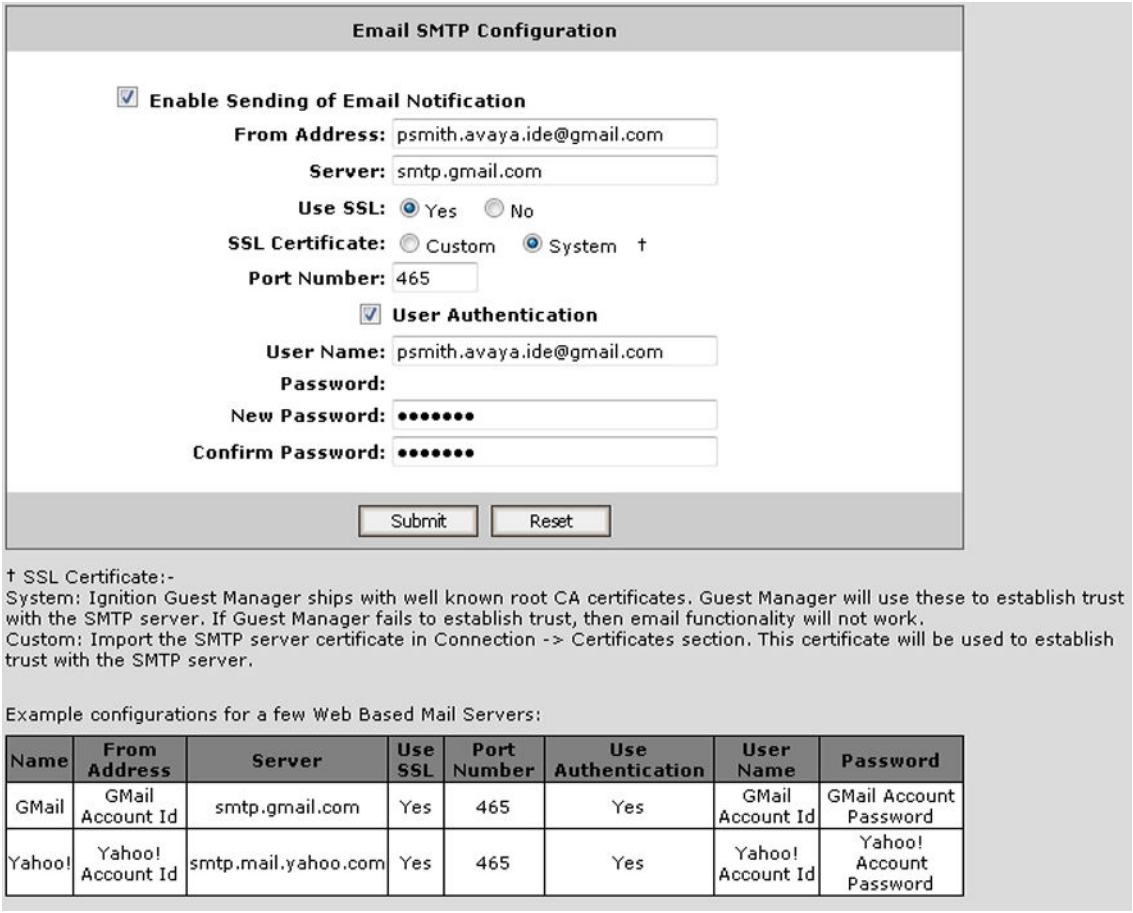
      Make sure that the certificate does not have a password associated with it. The certificate encoding format must be either DER-encoded binary X.509 or Base64–encoded X.509.

   b. In the **SSL certificate** field, check **System** to use the well-known root certificates shipped with Guest Manager to establish trust with the SMTP server. If Guest Manager fails to establish trust, the email functionality does not work.
   c. Enter the SMTP port number to be used by Guest Manager for the SSL connection.
7. For non-SSL connections, in the **Use SSL** field, select **No** and enter the SMTP port number to be used by Guest Manager for the non-SSL connection.
8. If your SMTP server requires authentication, check the **User Authentication** check box and, in the **User Name** and **Password** fields, type the login credentials of the SMTP server user. (Click **Change** to expose the password fields.)

   The SMTP server name can be an email address.
9. Click **Submit**.

Make sure you set up an appropriate email notification template as shown in Writing SMS and Email templates for account notifications on page 121.

Example



† SSL Certificate:-
System: Ignition Guest Manager ships with well known root CA certificates. Guest Manager will use these to establish trust with the SMTP server. If Guest Manager fails to establish trust, then email functionality will not work.
Custom: Import the SMTP server certificate in Connection -> Certificates section. This certificate will be used to establish trust with the SMTP server.

Example configurations for a few Web Based Mail Servers:

Name	From Address	Server	Use SSL	Port Number	Use Authentication	User Name	Password
GMail	GMail Account Id	smtp.gmail.com	Yes	465	Yes	GMail Account Id	GMail Account Password
Yahoo!	Yahoo! Account Id	smtp.mail.yahoo.com	Yes	465	Yes	Yahoo! Account Id	Yahoo! Account Password

Setting up SMS notification parameters

Guest Manager can be set to send each guest user his or her login name and password via an SMS text message to a mobile phone. To enable this feature, you must first configure the carrier gateway settings that tell Ignition Server how to send SMS messages to each mobile service provider.

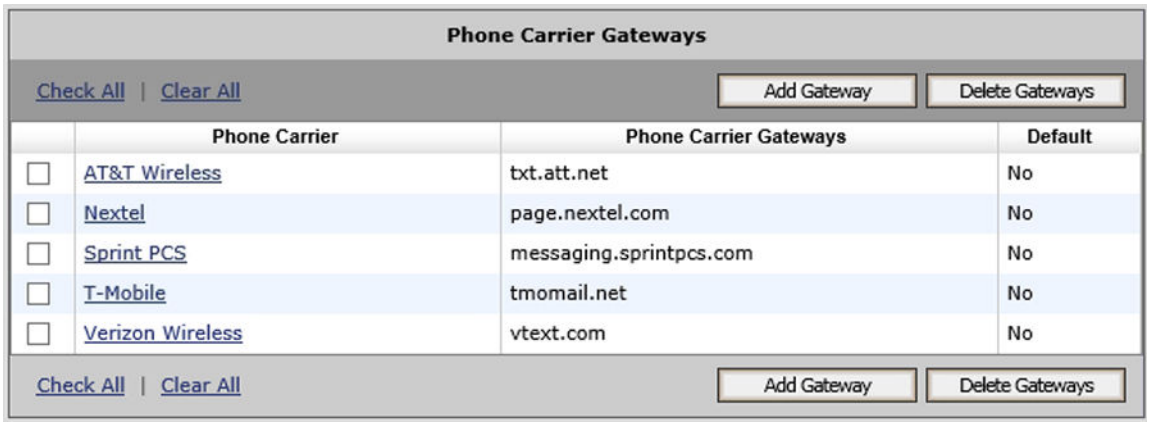
Important:

If you configure a default gateway, the default gateway is used to send SMS messages to each mobile service provider.

Procedure

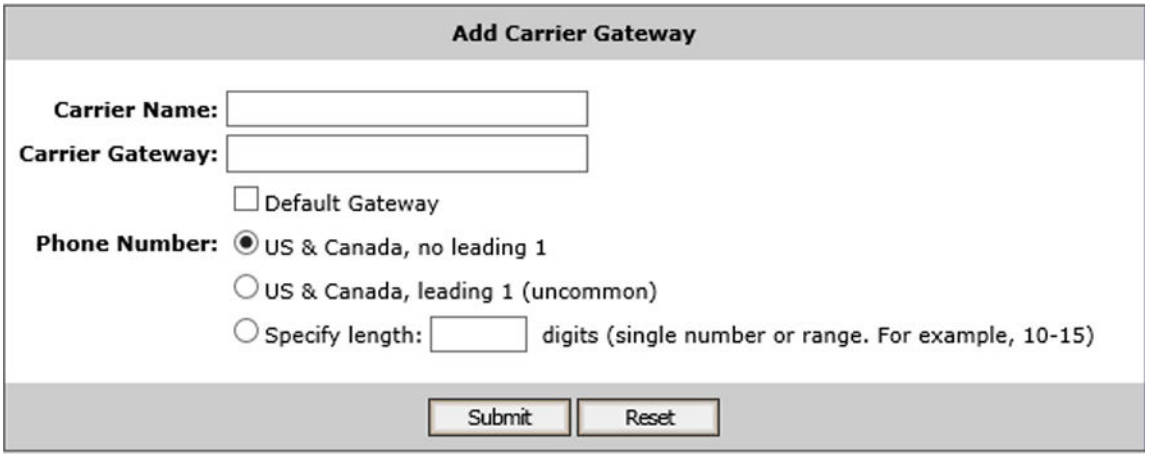
1. Launch the Guest Manager Administrator application.
2. Click **Administration** > **Notification** > **SMS Gateways**.

The Phone Carrier Gateways window shows the gateways that have been configured. You must configure a gateway for each mobile phone provider to whom Guest Manager will send login details.



3. To add a gateway, click **Add Gateway**. In the Add Carrier Gateway window, do the following:
   a. In the **Carrier Name** field, enter the carrier name.
   b. In the **Carrier Gateway** field, enter the carrier gateway address.
   c. If this is the default carrier gateway, check the **Default Gateway** check box.

      You can have only one default SMS gateway. If you select this gateway as the default, a warning message indicates that any previously configured default will be overridden. If you do not specify a default gateway, the first gateway in the list becomes the default gateway.
   d. Check the **Phone Number** format.
   e. Click **Submit**.



4. To edit an existing gateway, click its name. In the Edit window, make the appropriate changes and click **Submit**.

Make sure you set up an appropriate SMS notification template as shown in Writing SMS and Email templates for account notifications on page 121.

Exporting and importing Guest Manager configurations

You can export and import Guest Manager configurations. This capability enables you to port Guest Manager configurations between multiple Guest Manager deployments. You can also export the Guest Manager configuration from a previous version and import it into a new version for upgrades. In future releases of the Guest Manager, you will upgrade to a new releases of the Guest Manager by deploying a new VM and importing the configuration of the previous VM into the new VM.

The configurations you can export and import include:

- Appliance configurations
- RADIUS configurations
- User certificates
- HTTPD Web server configuration (HTTP, SSL, and so on)
- User preferences
- All Guest Manger configuration SMTP, SMS Gateway, KeyStore certificates.

Note:

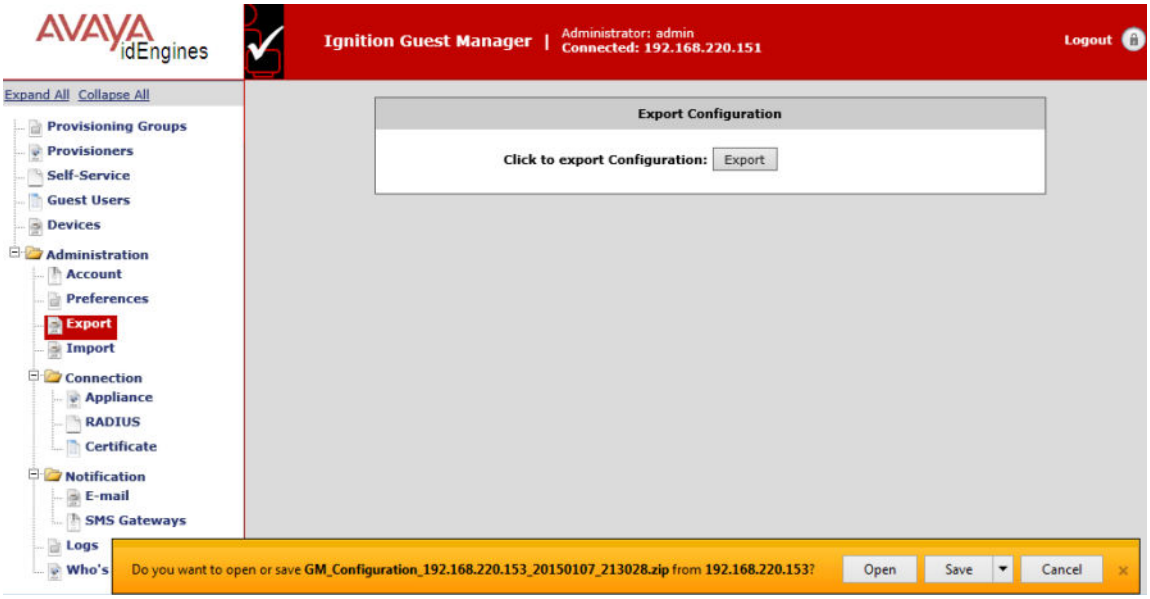
Guest Users, Devices, Provisioners, Self-Service Provisioner, and Provisioner Group configuration are stored on the Ignition Server and are not part of the Guest Manager export/import function.

Exporting a Guest Manager configuration

You can export a Guest Manager configuration.

Procedure

1. From the Guest Manager Administrator Application, click **Administration** > **Export**.
2. Click **Export** to export the configuration.
3. In the File Download Window, click **Save**.



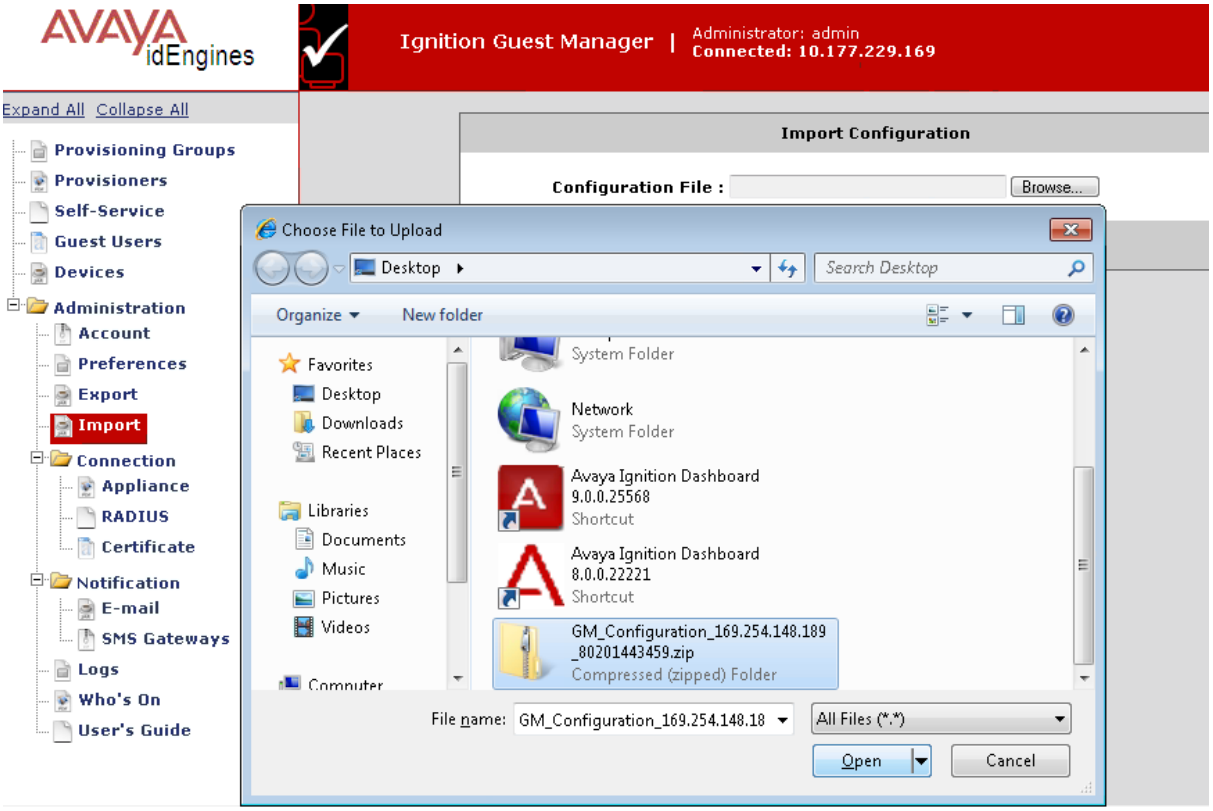
4. In the **Save As** window, browse to where you want to save the configuration zip file and click **Save**.
5. In the Download Complete window, click **Close**.

Importing a Guest Manager configuration

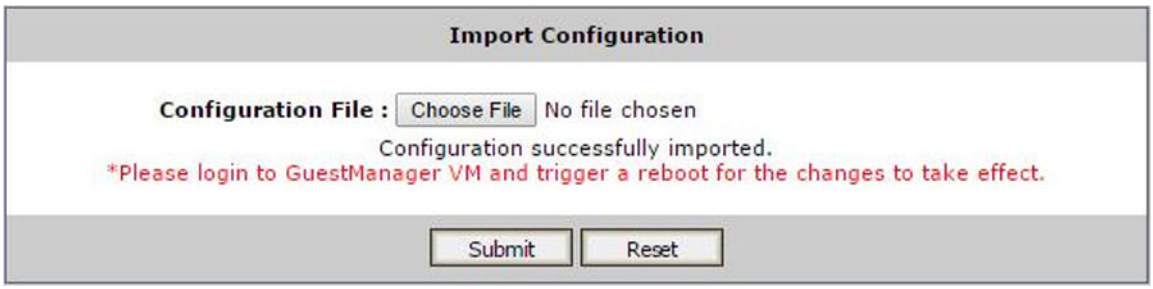
You can import a Guest Manager configuration.

Procedure

1. From the Guest Manager Administrator Application, click **Administration** > **Import**.
2. On the **Import Configuration** page, click **Browse**.
3. In the **Choose file** window, select your configuration zip file, and click **Open**.



4. On the Import Configuration page, click **Submit**. The Guest Manager Administrator Application displays the following successful import message:



5. Log on to the Guest Manager VM and perform a reboot through the CLI for the changes to take effect. See Command Line Interface on page 38.

Chapter 6: Managing Guest Manager

This chapter is intended for the Avaya Identity Engines Ignition Guest Manager Administrator and describes how to manage the Guest Manager applications. If you are a provisioner, you may skip this chapter and proceed to Provisioner application: Managing guests and devices on page 134.

Important:

When using Guest Manager, *do not* use your browser's Refresh command to update a page. Instead, click the appropriate command button on the left side of the window to reload the page. *Do not* open a link in a new tab at any time.

Running the Guest Manager Administrator application

Procedure

1. Open a web browser and point the web browser to the Guest Manager Administrator application at https://<server_name>/GuestManager/admin.
2. Enter your Guest Manager Administrator login credentials and click **Submit**. The default login is `admin/admin`.

   The Guest Manager Administrator application appears.

   Warning:

   Do not allow the browser to remember your password. Allowing the browser to retain passwords for the Guest Manager application is not secure and causes misleading "password update" messages from the browser when you edit users.

If you act as both Administrator and Provisioner

Often, during initial set-up, you will want to act in two roles: as the Guest Manager Administrator and Provisioner.

You must have two accounts: the Guest Manager Administrator account and a Provisioner account. Only the Guest Manager Administrator may run the Administrator Application, and only provisioners may run the Provisioner Application. See Guest Manager application in context on page 18.

Use the following steps to switch between the applications.

Warning:

Identity Engines recommends that you *do not connect* your browser simultaneously to both the Administrator and Provisioner Applications.

Procedure

1. Log out of the current application.
2. Point your browser to the desired Guest Manager application.
   - To switch to the Administrator Application, go to: https://<server_name>/GuestManager/admin
   - To switch to the Provisioner Application, go to: https://<server_name>/GuestManager/provisioner
3. Type your user name and password, and do *not* allow the browser to remember your password.

Restarting Guest Manager

Procedure

1. Log in to the Guest Manager virtual appliance and launch the Guest Manager console. Enter the username and password.
2. Enter `tomcat stop`.
3. Enter `tomcat start`.
4. To restart the httpd server, enter `httpd restart`.
5. Reconnect to the Avaya Identity Engines Ignition Server as described in Connecting Guest Manager to the Ignition Server Appliance on page 67.

Connecting Guest Manager to the Ignition Server Appliance

Guest Manager must be connected to allow provisioners to create and edit guest user accounts and to allow the Guest Manager Administrator to manage provisioners. Guest Manager *need not* be connected to allow guest users to use their accounts.

Guest Manager does not automatically connect to the Ignition Server upon start-up. The connection indicator at the top of the Administrator Application window displays “Disconnected” when there is no connection.

Connect Guest Manager to the Ignition Server as follows:

Procedure

1. Run the Guest Manager Administrator Application.
2. Log in as the Guest Manager Administrator. Do not allow the browser to remember the password.
3. Click on **Administration > Connection > Appliance** in the main toolbar of the Administrator Application.
4. In the **Login To Appliance** window, type the **Username** and **Password** of the Ignition Server SOAP API user account. The **Host** and **Port** settings should have been set already. If they are not set or set incorrectly, see Making SOAP settings on the Ignition Server on page 55.
5. Click **Connect**.

   Once you have made the connection, provisioners may begin using the Provisioner Application, and you may begin managing and creating provisioners.

Disconnecting Guest Manager from the Ignition Server Appliance

Procedure

1. Run the Guest Manager Administrator Application.
2. Log in as the Guest Manager Administrator. Do not allow the browser to remember your password.
3. Click **Administration > Connection > Appliance** in the main toolbar of the Administrator Application.
4. In the Connected To Appliance window, click **Disconnect**.

   Once you log out of the Ignition Server appliance, Guest Manager is no longer connected, the Provisioner Application cannot be used, and the self-provisioning portals cannot be used.

Setting the Administrator Username and Password

The default login username and password for the Guest Manager Administrator are

- **User Name**: `admin`
- **Password**: `admin`

Use the steps below to change the username or password of the Guest Manager Administrator. Do not confuse this account with the Ignition Server Administrator account or with the provisioner accounts. See page Guest Manager introduction on page 18 for details.

Procedure

1. Run the Guest Manager Administrator Application.
2. Log in as the Guest Manager Administrator. Do not allow the browser to remember your password.
3. Click on **Administration > Account**.
4. On the Administrator Account window, if required, edit the **User Name**.
5. To edit the **Password**, do the following:
   a. Click the **Change** link in the Password field.
   b. Type the **Current Password**.
   c. Type the **New Password**.
   d. Type the new password again in the **Confirm Password** field.

   Important:

   Avaya strongly recommends that you change the Guest Manager Administrator password after you have completed the initial setup of Guest Manager.
6. Click **Submit**.

Editing E-mail notification settings

You may set up the e-mail notification settings as explained in Setting up Email notification parameters on page 59.

Editing SMS Notification Settings

Creating SMS Gateways

You can set up SMS notification settings as explained in Setting up SMS notification parameters on page 61.

Deleting SMS Gateways

Avaya recommends that you *do not delete any gateway*, as there may be guest user accounts that rely on the gateway you delete. If you delete a gateway that a guest account relies on, then that guest will not receive notifications of changes to his account.

Procedure

1. Make sure the gateway you will delete is not currently in use by any guest user on the system.
2. Run the Guest Manager Administrator Application.
3. Click **Administration > Notification > SMS Gateways**.
4. Click the check box of the gateway to be deleted.
5. Click **Delete Gateways**.

Configuring Timeout settings

Guest Manager application sessions automatically disconnect if the period of inactivity exceeds the applicable timeout threshold.

Provisioner Idle Timeout Threshold

The provisioner idle timeout period causes the Guest Manager Provisioner Application to disconnect after a period of inactivity, after which the provisioner must log in again to use the application. You must set this timeout threshold in the provisioning group. See Creating a provisioning group on page 105.

Setting Administrator Session Timeout Threshold

The administrator HTTP session timeout period causes the Administrator Application to disconnect after a period of inactivity, after which the Guest Manager Administrator must log in again to use the application.

1. Run the Guest Manager Administrator Application.
2. Click **Administration > Account**.
3. In the **Timeout** field, type the period in minutes after which the administrator will be forced to re-authenticate to continue using Guest Manager.
4. Click **Submit**.

SOAP Client Timeout Threshold

The SOAP client timeout setting is the interval at which the Guest Manager-Ignition Server connections are cleaned up. Guest Manager does not become unusable when the timeout period expires. Instead, after disconnecting due to SOAP client timeout, Guest Manager reconnects automatically when a user resumes using the application.

Setting the SOAP Client Timeout period

Follow the instructions in Making SOAP settings on the Ignition Server on page 55.

Restoring a timed out server connection

In most cases Guest Manager will reconnect automatically. If it does not reconnect, reconnect it manually as explained in Connecting Guest Manager to the Ignition Server Appliance on page 67.

Logs

The default name for the log files of Guest Manager takes the form, GuestManager.log, GuestManager.log.1, GuestManager.log.2, and so on.

Viewing the log files

The **Administration** > **Logs** button in the main toolbar of Guest Manager lets you view the logs. Click the numbers at the bottom of the screen to page through the files.

Figure 3: Contents of the GuestManager.log File

Chapter 7: Setting guest authorization policies

At guest login time, Avaya Identity Engines Ignition Server checks the guest user's password and then checks the organization's authorization policy to determine whether the guest will be granted access to the requested network resource. This chapter describes how to set up authorization policies. The steps shown in this chapter must be performed using Ignition Dashboard. You need an Ignition Server Administrator login to use Dashboard.

If you are in a hurry to create some guest users, you can skip most of the policy setup procedure. See Creating a minimal authorization policy on page 96.

Setting authorization policies for guest users

Authorization policies for guest users consist of two main components: the access *constraint check boxes* that optionally appear on the Create Guest User page and the *underlying policies* on the Ignition Server that enforce these constraints.

Access constraint check boxes on the Create Guest User page

Provisioners use the Create Guest User page of Avaya Identity Engines Ignition Guest Manager to create guest accounts and, optionally, set access rights for each guest. The center of this page lists the access constraints the provisioner can apply to each guest user. Each check box corresponds to an internal user group on the Ignition Server. The Guest Manager Administrator determines which check boxes each provisioner sees.

In the example implementation outlined in this chapter, the Create Guest User page appears as shown below.

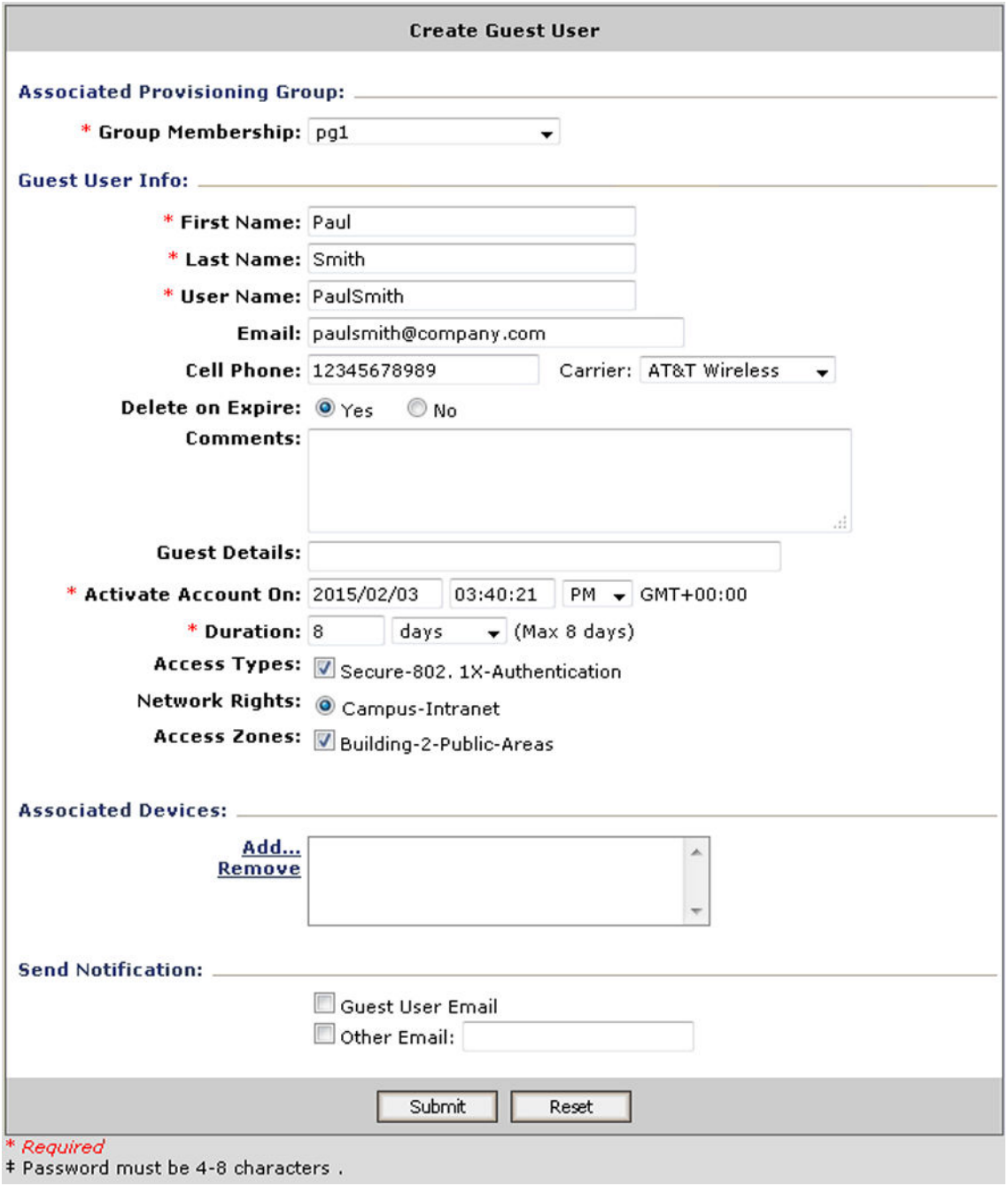


Figure 4: Example Guest User Provisioning Form

Three classes of access constraints are available:

- **Access Type**: The mechanisms of network access the guest user is permitted to use, such as wired, wireless, or secured wireless. To create an access type, create an internal user group in Ignition Dashboard with its type set to **accessType**. The provisioner may tick more than one **Access Type** check box to let the user connect in multiple ways.

- **Network Rights**: The network realm to which the guest user has access, such as the Internet only, or the southeast regional sales department VLAN. To create a network right, create an internal user group in Ignition Dashboard with its type set to **networkRight**. The provisioner may only tick one **Network Right** check box, because the user must be assigned to one and only one VLAN or segment of the network.
- **Access Zones**: The physical locations at which the guest user can connect to the network. Each is typically the location of a switch or access point. To create an access zone, create an internal user group in Ignition Dashboard with its type set to **accessZone**. The provisioner may tick more than one **Access Zone** check box to let the user connect from multiple locations around the facility.

The access constraint check boxes are optional. If you create no accessType, networkRight, or accessZone groups in Ignition, then no constraint check boxes will appear for that category or categories in the Create Guest User window.

Authorization policies

To set up the guest authorization policies you will enforce with Guest Manager, you write authorization policies in Ignition Server just as you would for any other user. Authorization policy decisions are made on the basis of a user's membership in virtual groups. This document explains how to set up an example policy. For additional information, see *Avaya Identity Engines Ignition Server Administration*.

Mapping internal user groups to virtual groups

While the access constraint check boxes are based on *internal user groups*, your authorization policies are based on *virtual groups*. For this reason, you must map each internal user group to a virtual group before you start writing your authorization policies.

When you create your internal user groups, give them names that will make sense to your provisioners. For example, you might use "Bldg1-Front-Lobby."

Sample authorization policies to be used in this chapter

This section describes the example settings for a local internal user store configuration of the Ignition Server appliance to support a simple use of the Ignition Guest Manager application. The section Step-by-step configuration in Ignition Dashboard on page 77 shows you how to make these settings in Ignition Dashboard.

The Example

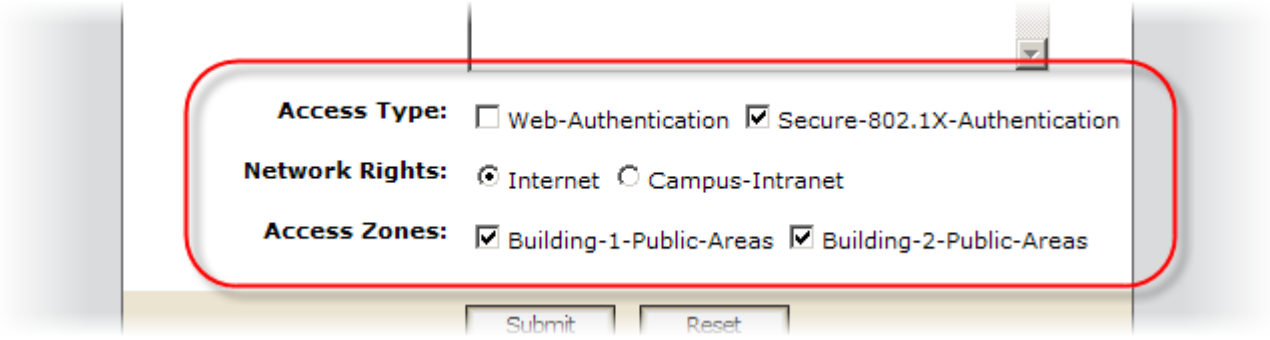
This example depicts a college campus guest authorization policy called “Chapel-Hill-Guest-Access.” When a guest arrives on campus, the provisioner creates a guest user account that determines the following:.

- whether the guest can authenticate through a web portal (“Web-Authentication”) or will be required to authenticate more securely using an 802.1X-equipped laptop (“Secure-802.1X-Authentication”)
- what parts of the network the guest can visit (“Internet” only or the “Campus-Intranet” which includes the local network and the Internet)
- which physical locations the guest can connect from (“Building-1-Public-Areas” and/or “Building-2-Public-Areas”)

To keep things relatively simple, we assume that the switches and access points in this example serve guest users only. You can set up Ignition Server to allow both guests and permanent users to connect via the same switches, but it requires more complex authorization and provisioning rules.

Access constraint check boxes

When a provisioner creates a guest user account, the provisioner places limits on the guest user’s network access using the access constraint check boxes of the Create User screen. Note, these check boxes only appear after you have created corresponding internal user groups in Ignition Dashboard. In this example, we will create a policy that supports the check boxes shown here:



The constraint check boxes that a provisioner sees in the Create Guest User screen of Guest Manager are generated from the internal user groups saved on your Ignition Server appliance. Each provisioner sees only those check boxes that the Guest Manager administrator has allowed him or her to see. The table below summarizes the groups we will use to create access constraint check boxes in this example.

Mapping internal user groups to virtual groups

Access constraint class / group type	Internal group name (Shown in the Create Guest User screen)	Virtual group to which internal group is mapped. (Used in policy rules)
Access Types	Web-Authentication	Web-Authentication
	Secure-802.1X-Authentication	Secure-802.1X-Authentication
Network Rights	Internet	Internet
	Campus-Intranet	Campus-Intranet
Access Zones	Bldg-1-Public-Areas	Bldg-1-Public-Areas
	Bldg-2-Public-Areas	Bldg-2-Public-Areas

When creating guest users, the provisioner will see the internal user group (column 2, above) names in Guest Manager's Create User window. When setting policies, you will see the virtual group (column 3, above) names in Ignition Dashboard's User Authorization Policy window.

Typically you will have a 1:1 mapping of internal user groups to virtual groups, as we do in this example. You may map many internal user groups to a single virtual group if you prefer.

Components of the authorization policy

The example guest user authorization policies are made up of the following, all created in Ignition Dashboard:

- **Service Category**: A service category is Ignition's way of collecting network edge devices (switches and wireless access points) into a set so you can apply common access policies to them. In the example, you will create a new service category called "Chapel-Hill-Guest-Access."
- **Directory Set**: A directory set tells Ignition Server where to find user accounts. In the example, you will create a directory set called "Guest User Access."
- **Policy Settings**: Each Ignition Server service category contains authentication, authorization, and VLAN provisioning policies. In the example, you will configure these in the "Chapel-Hill-Guest-Access" service category.

Step-by-step configuration in Ignition Dashboard

This section describes how to set up authorization policies on the Ignition Server to support the sample guest user provisioning scenario described in the section Sample authorization policies to be used in this chapter on page 75.

This procedure is optional. You can create and use guest accounts without authorization policies.

Procedure

1. Run Ignition Dashboard (Launching Ignition Dashboard on page 154) and log in as the Ignition Server Administrator.

2. Create the new internal user groups as follows.

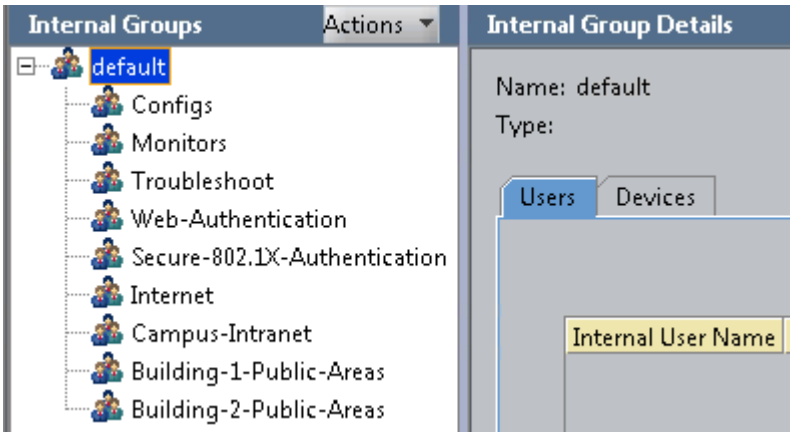
Access constraint type / group type	Internal user groups you will create
Access Types	Web-Authentication Secure-802.1X-Authentication
Network Rights	Internet Campus-Intranet
Access Zones	Building-1-Public-Areas Building-2-Public-Areas

   a. In the Ignition Dashboard main navigation tree, click **Directories**: In**ternal Store**: **Internal Groups**. The application displays the Internal Groups panel.

   b. In the **Internal Groups** pane, right-click on the root group (usually called “default”) and select **Actions**: **Add New Internal Group**. The application displays the Add a New Internal Group dialog, where you name the new internal group:

      - Enter the **Internal Group Name**, “Web-Authentication”.
      - In the **Type** field, specify the group type (also known as the access constraint class); this is also the name of the Access Constraint check box that will appear in the Guest Manager application. For the “Web-Authentication” group, specify a **Type** of “accessType”. This instructs Guest Manager to display the group in the Access Type section of the Create Guest User page.
      - Tick the **Automatically create** check box. (Note that if you wished to map multiple internal groups to one virtual group, you would leave this check box unticked now and map the groups manually later.)
      - Click **OK**. The Add New Internal Group window closes.

      The new internal group name appears in the Internal Groups panel. The corresponding virtual group can be seen in the Virtual Groups window. In Dashboard’s main navigation tree, click **Directories** > **Virtual Mapping** > **Virtual Groups**.

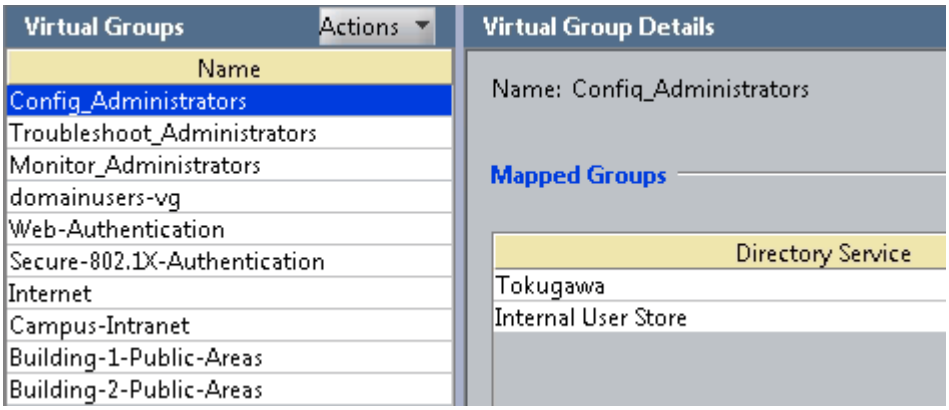


   c. Repeat Step 2 for the remaining internal groups to be created. If you are replicating the example, create all the groups listed in the preceding table.

Important:

Always click on the root or “default” group before you create each group. This ensures the root group is the parent of each group you create.

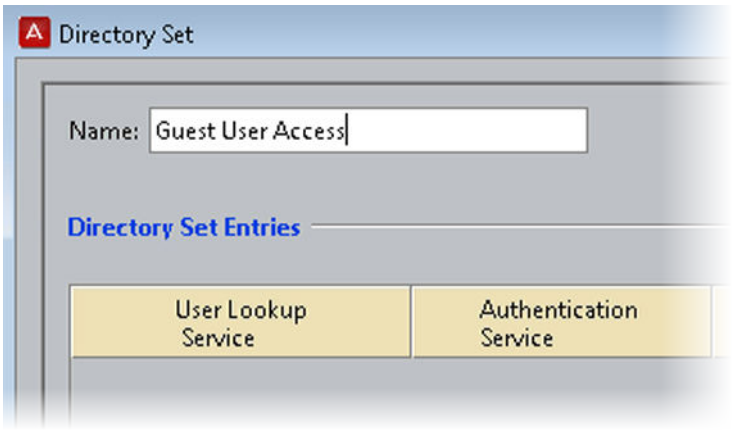
When you have added the final new internal group entry, the Internal Groups panel and the Virtual Groups panel will look similar to the figures.



3. Create a Directory Set for the guest users.

   Create a directory set that tells Ignition Server where to find guest user accounts. Since Ignition Guest Manager saves all guest users to the Ignition Server internal store, your directory set will include only the internal user store. For the example, create a directory set called “Guest User Access,” as shown below.

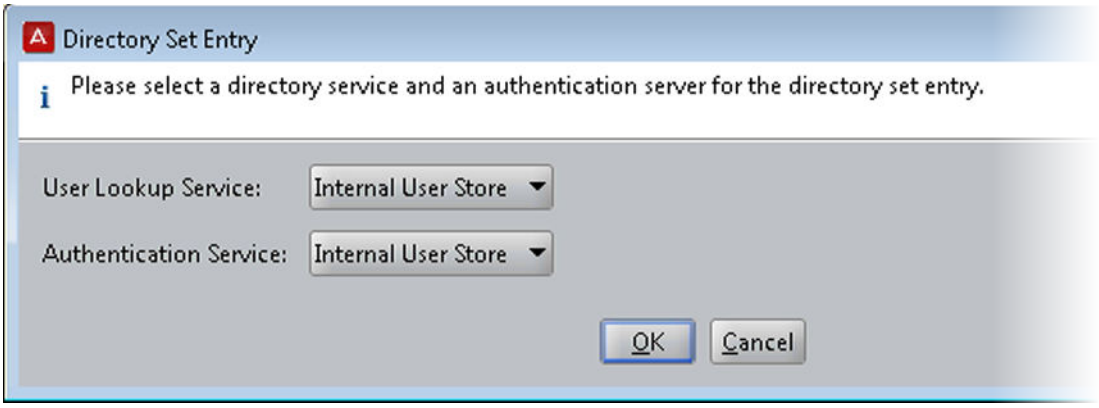
   a. In Ignition Dashboard’s navigation tree, select **Directories** > **Directory Sets**. The Directory Sets panel appears.



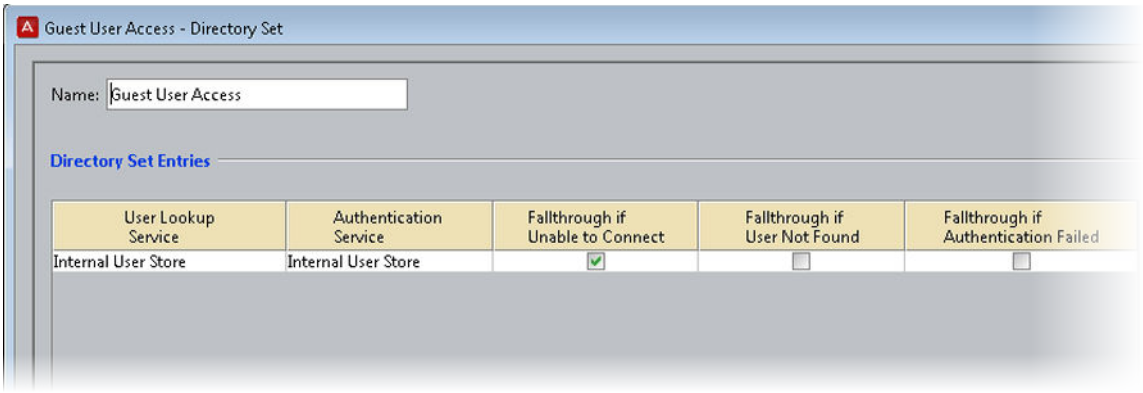
   b. Click the **New** button at the bottom of the window. The Directory Set window appears.

   c. Type in the name for the directory set (“Guest User Access” in the example). Click **Add**.

   d. Next, add the guest user directory to the directory set. In the Directory Set Entry window, select “Internal User Store” under **User Lookup Service**, and select “Internal User Store” under **Authentication Service**. Click **OK**.



The Directory Set window shows the details for the newly created directory set.



e. There is no need to set the fallthrough conditions for this example directory service. Click **OK**.

   Now that you have created Guest User Access as a directory set for the guest user(s), you can create the required service category and provide the identity routing using this directory set.

4. Create the Radius Access Policy

   Create the RADIUS access policy that will apply to your network-edge switches and access points. This policy controls access for users who connect through those switches. For this example we call the policy, “Chapel-Hill-Guest-Access.”

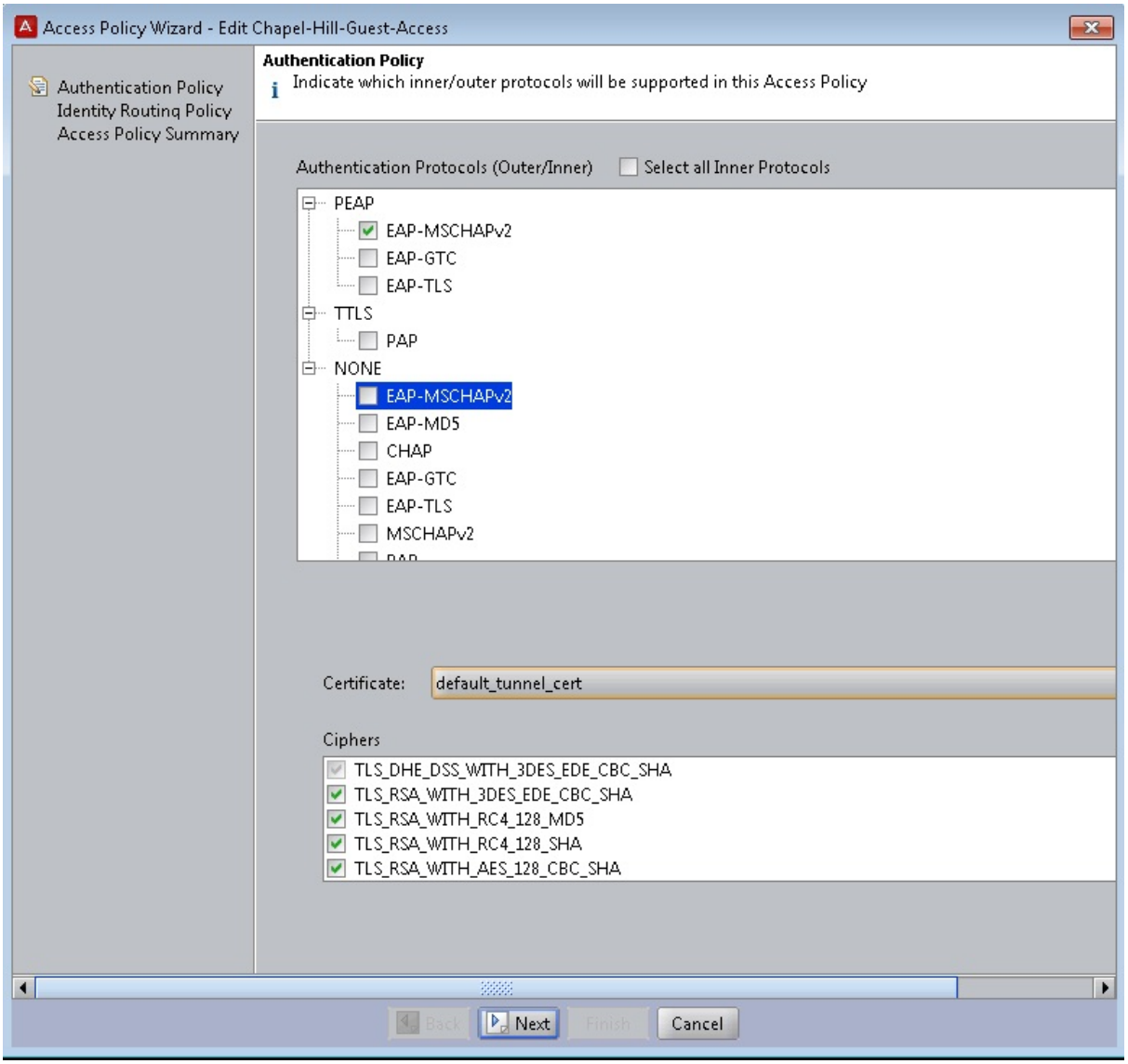
   a. In Ignition Dashboard’s main navigation tree, expand **Access Policies** and click on **RADIUS**. At the bottom of the main panel, click **New**.

   b. In the New Access Policy window, type the name, “Chapel-Hill-Guest-Access” and click **OK**.

   c. In the Access Policies panel, click the name of your new access policy and click the **Edit** button. The application displays the **Access Policy Wizard**.

5. Set up the Allowed Authentication Types.

   In next few sections, you will set up your guest authentication and authorization policies. First, set up your authentication policy as shown here:



In the Access Policy Authentication Policy tab, in the Authentication Protocols section, do the following:

- Under PEAP, tick *EAP-MSCHAPv2*
- Under NONE, tick *EAP-MSCHAPv2*, *MSCHAPv2*, and *PAP*
- Leave the **Certificate** and **Ciphers** fields set to their defaults.
- Click **Next**.

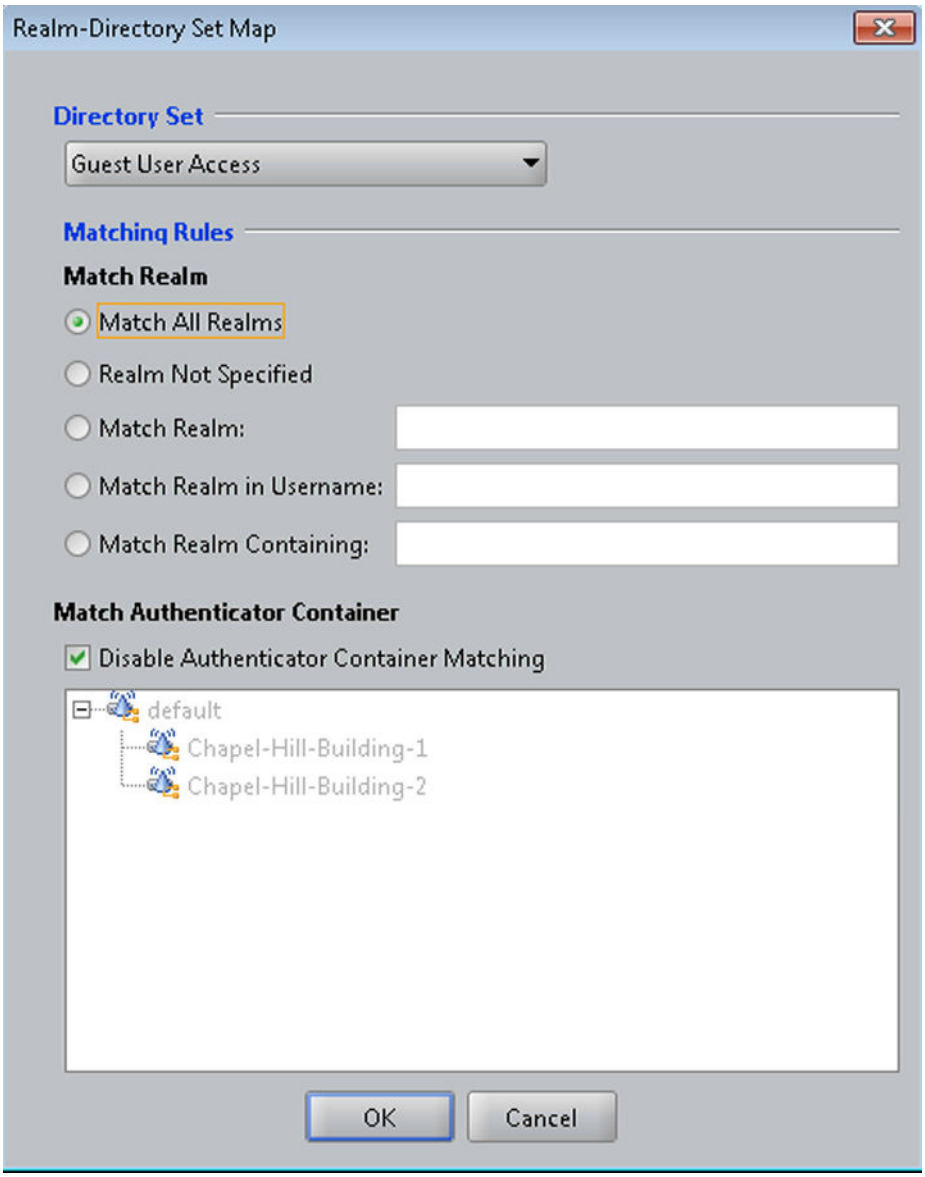
This policy allows users to authenticate with the EAP-MSCHAPv2 credential validation protocol in a PEAP tunnel, as well the EAP-MSCHAPv2, PAP, and MSCHAPv2 credential validation protocols with no outer tunnel.

6. Set up Identity Routing.

Set up your identity routing policy to point to the internal user store as follows:

a. The **Identity Routing Policy** panel appears. Below the **Realm-Directory Set Mapping** area, click **New**.

b. In the Realm-Directory Set Map window:

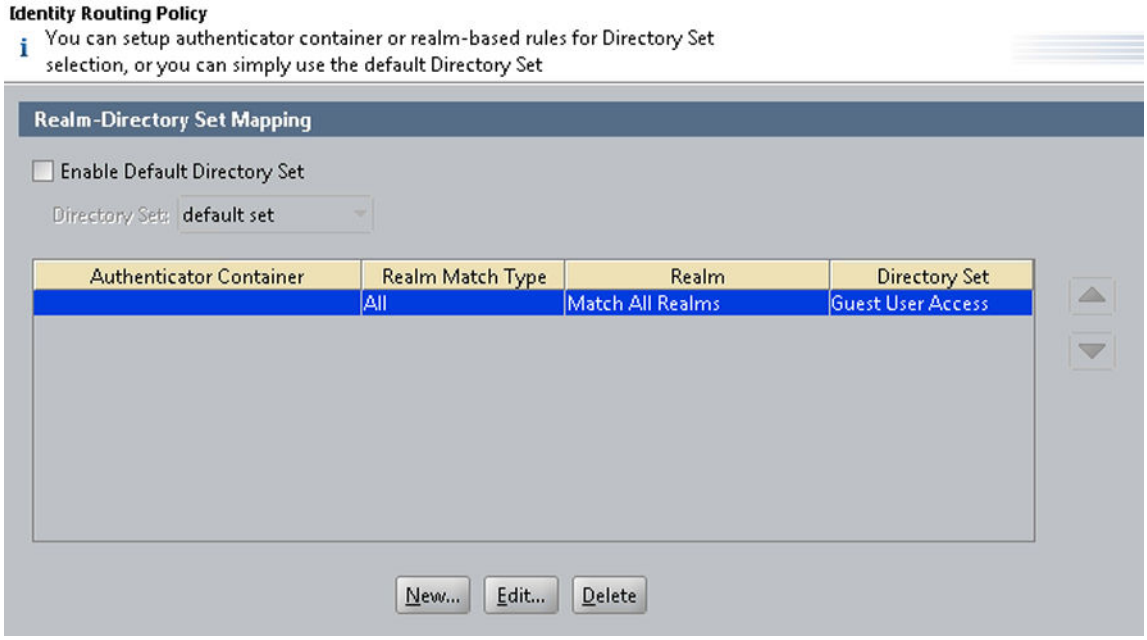


- In the **Directory Set** drop-down list, choose **Guest User Access**.
- In the **Realm** section, select **Match All Realms**.
- In the **Match Authenticator Container** section, tick the **Disable** check box.
- Click **OK**.

The directory set information is displayed in the Identity Routing Policy window.

c. Click **Next**.

d. Click **Finish**.



7. Create Your Authenticator Hierarchy to label your locations.

   Ignition Server allows you to categorize your authenticators in an Ignition Server authenticator hierarchy and then consider the authenticator's category label at user login time when making the authorization decision. For example, you might use the authentication hierarchy to label all switches in a residence hall with the label, “Building-1”, and then write a policy that allows only certain guests to log in through a “Building-1” switch. To set this up, you will create a hierarchy, create a record for each authenticator, and place the record at an appropriate location (called a “container”) in the hierarchy.

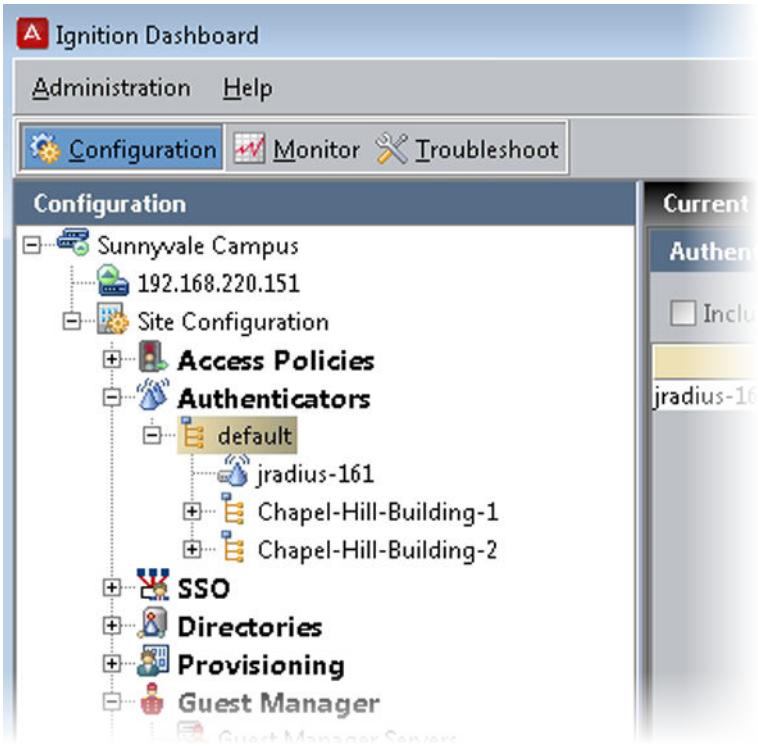
   For this example, our hierarchy consists of two *containers*: one for building one, and one for building two.

   Set this up as follows:

   a. In Dashboard’s main navigation tree, expand the **Authenticators** node. This displays the root node of your **Authenticator Container Hierarchy**. Click on the root node (usually called, “default”).

   b. In the **Actions** menu in the upper right, click **Add Container**.

   c. In the **Container Name** field, type the name of your first location. For this example, the name is “Chapel-Hill-Building-1”. Click **OK**.



d. Now add a container for your second location. In the **Container Hierarchy**, click the root or default node again. In the **Actions** menu,click **Add Container**.

e. In the **Container Name** field, type “Chapel-Hill-Building-2” (if you are following the example). Click **OK**.

8. Create your Authenticators.

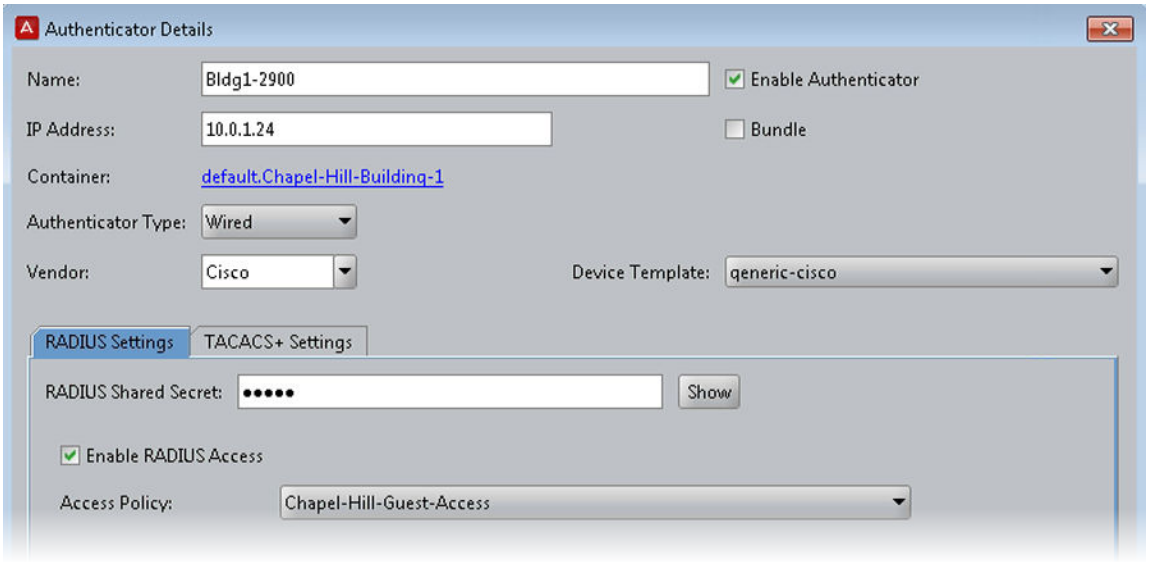
   Next, create an Ignition Server *authenticator record* for each switch, access point, and web authentication portal that guests will use. The authenticator record makes Ignition Server aware of the switch, and specifies how Ignition Server communicates with it.

   As you create each authenticator record, you will place it in an appropriate container in the authenticator hierarchy. By placing the authenticator in a container labelled with *Chapel-Hill-Building-1* or *Chapel-Hill-Building-2*, you are applying a location label to the authenticator. You will use these labels in your authorization rules to limit where users can log in.

   Follow these steps to create and label the authenticators:

   a. In Dashboard’s navigation tree, under the **Authenticators** node, click on the name of one of the authenticator containers you created.

   b. On the right side of the window, click **New** to add an authenticator.



c. In the Authenticator Details window, do the following:

- Tick the **Enable Authenticator** check box.
- Type a **Name** for the authenticator.
- Type its **IP Address**.
- The blue text of the **Container** field shows the authenticator container that owns this authenticator. Make sure this is set to “Chapel-Hill-Building-1” if you are following the example. If you wish to change it, click the blue text.
- In the **Authenticator Type** drop-down list, specify “Wired” for a switch, “Wireless” for a WLAN access point, or “Other” for a web authentication portal.
- In the **Vendor** field, specify the maker of your authenticator.
- In the **Device Template** field, take the default setting, or, if you have created a custom device template select its name.
- In the **RADIUS Settings** tab, type the **RADIUS Shared Secret** of your authenticator.
- Tick the **Enable RADIUS Access** check box.
- In the **Access Policy** drop-down list, choose *Chapel-Hill-Guest-Access*.
- Click **OK**.

Repeat the preceding steps for the other wired switches and wireless access points that guests will access in each building. Place your “Building 2” authenticators in the Chapel-Hill-Building-2 container in the container hierarchy.

9. *Optional*: Create a Device Template for the Authenticator.

This section is optional and is included to demonstrate how you can create a policy that grants a specific type of access to guests who log in through a certain authenticator. If you do not plan to do this, skip this section.

The preceding section showed how to label authenticators by placing them in authenticator containers. This section will show another way that Ignition Server lets you label

authenticators: by applying a custom Ignition Server device template to them. Your policy rules can then read the device template's name and use it to make access decisions.

For this example, we will create a device template called "600S" and apply it to the Ignition Server 600S web authentication portal (if one is available). Later, we will write a rule that uses this label to require that some guests log in via the portal, and another one that prevents certain guests from using the portal.

Set up the device template as follows:

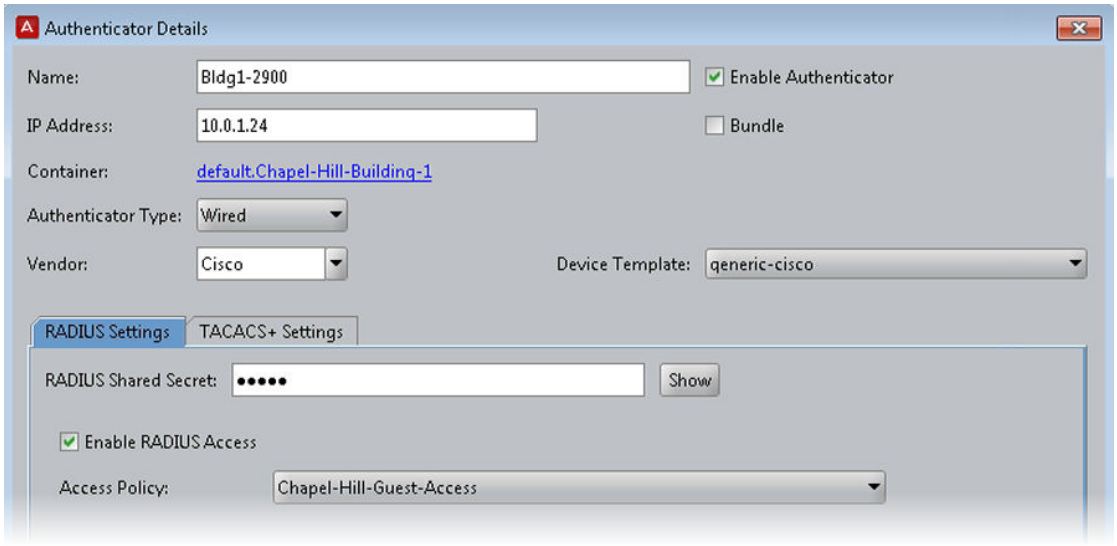
a. From the Dashboard main navigation tree, expand **Provisioning** > **RADIUS** > **Vendors/VSAs**.

b. In the **Vendors** list, scroll down, expand the **IdEngines** node, and click **Device Template**.

c. Click **New**.

d. In the New Device Template window, do the following:

- In the **Device Template Name** field, type "600S".
- For VLAN Method, tick **Use VLAN Label**.
- For MAC Address Source, select **Inbound-Calling-Station-Id**.
- Click **OK**.



e. Click **Done** to close the Edit Device Template window.

10. *Optional*: Create the Authenticator and apply the Device Template.

This section is optional and builds on the 600S example of the preceding section. If you do not plan to do this, skip this section.

In this section we will create the authenticator record for your 600S portal, and apply the 600S device template to it as a label. (As mentioned earlier, if your site does not have a 600S portal, you may use another portal or authenticator, instead.)

a. In Dashboard's navigation tree, under the Authenticators node, click on the name of the authenticator container that will contain your 600S device (in this example, click the container for Chapel-Hill-Building-1).

b. On the right side of the window, click New to add an authenticator.

c. Create your authenticator record, but with the following changes:

   - Choose an Authenticator Type of **Other**.
   - Set Vendor to **IdEngines**.
   - Select the Device Template, **600S**.

d. Click **OK**.

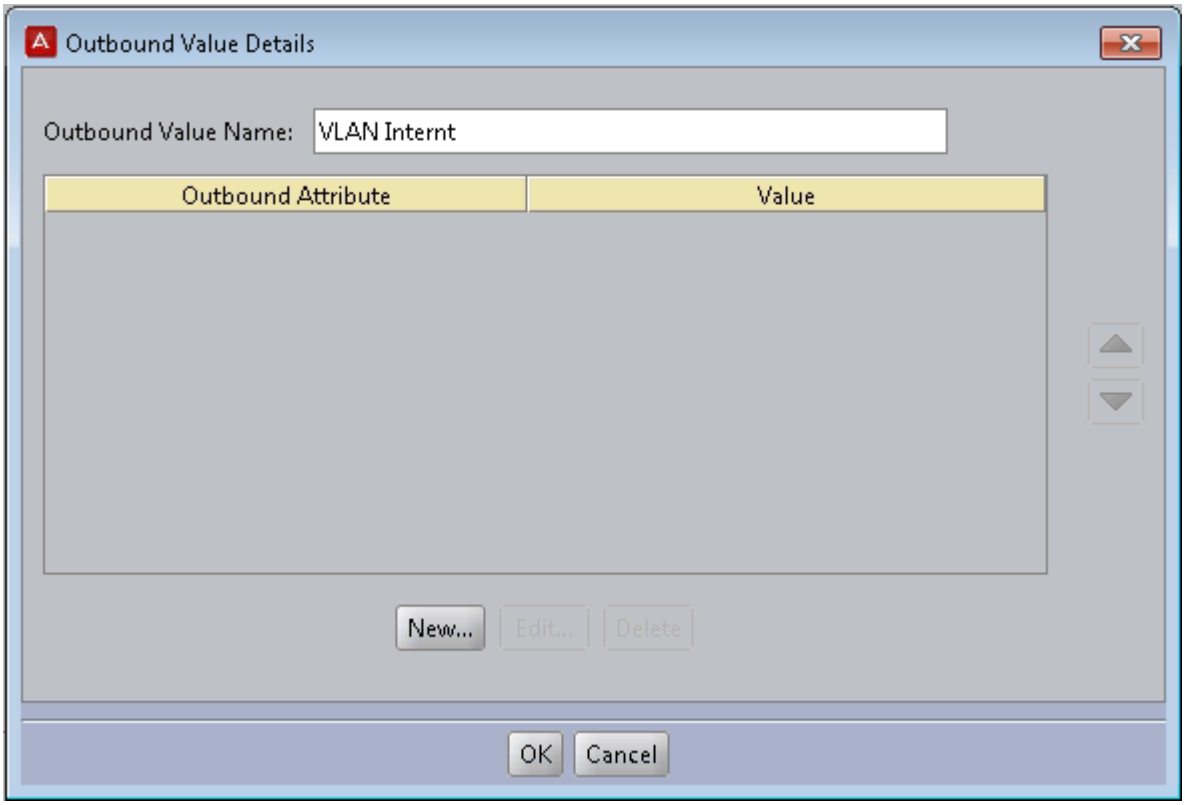
If you have additional 600S devices deployed, repeat these steps for each, taking care to place each device correctly in the container hierarchy. If following this example, add a 600S authenticator in Chapel-Hill-Building-2.

11. Create outbound values for assigning users to VLANS.

    When a guest user authenticates successfully, Ignition Server sends outbound provisioning values, or "outbound values" to the switch or access point, instructing it to place the guest user on the appropriate VLAN. This section shows you how to set up outbound values.

    This example assumes your switch gear is VLAN-capable and that you have set up two VLANs: one with a VLAN ID of "10" that offers Internet-only access (we'll call this one "VLAN Internet"), and one with a VLAN ID of "20" that offers access to the Internet and the campus network (we'll call this one "VLAN Intranet"). For information on setting up the VLANs, consult the documentation for your switch or access point.

    The steps below show you how to create an outbound value for each VLAN.For additional information on provisioning set-up, see *Avaya Identity Engines Ignition Server Administration*, NN47280-600.



a. In Dashboard's navigation tree, expand the **Provisioning** node and click Outbound Values. At the bottom of the **Outbound Values** panel, click **New**.

b. In the Outbound Value Details window, in the **Outbound Value Name** field, type `VLAN Internet`.

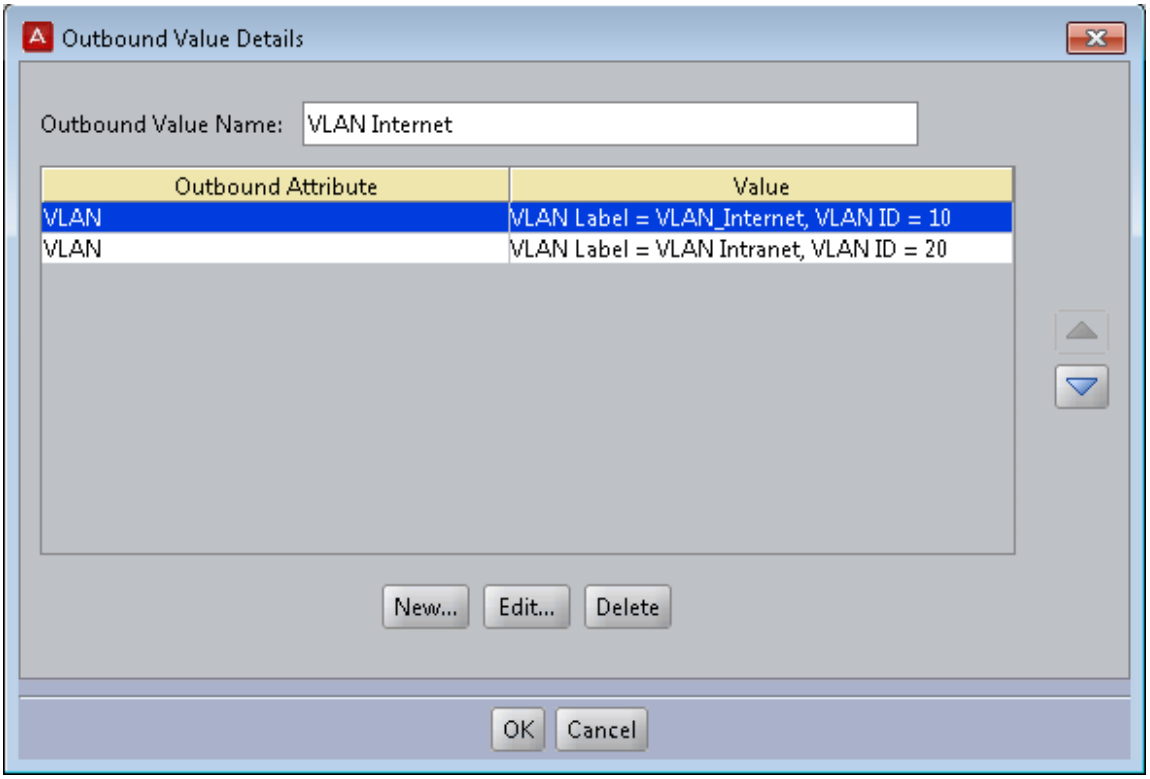
c. Below the **Outbound Attribute** table, click **New**.

d. The Outbound Value Instance window lets you add the name/value pair that this outbound value will send to the Ignition Server.

   - In **Choose Global Outbound Attribute** dropdown box, select **VLAN**.
   - Click the **Fixed Value** radio button.
   - In the **VLAN Label** field or **VLAN ID** field, type the label or number of the VLAN as it is configured in your switch or VLAN concentrator. In this example, we use a sample label of "*VLAN_Internet*" and a sample ID of "*10*".
   - Click **OK**.

e. In the Outbound Value Details window, click **OK**. Now your "VLAN Internet" outbound value is ready to use. Next, create the "VLAN Intranet" outbound value.

f. Create another outbound value, this time calling it "*VLAN Intranet*" instead of "*VLAN Internet*". Use the same steps you used to create the "*VLAN Internet*" value above. For this example, we use the VLAN Label, "*VLAN_Intranet*", and the VLAN ID, "20".



12. Sketch Out Your Guest Authorization policy.

    Next you will design the authorization policy that checks each guest user's access and, if the user is authorized, assigns the user to the appropriate VLAN. Recall that this example depicts a campus guest authorization policy with the following restrictions:

    a. **Access types**: The provisioner may give the guest the right to connect via web portal authentication ("Web-Authentication") only; to connect by secure 802.1X authentication ("Secure-802.1X- Authentication") only; or to connect via either method.

    b. **Network rights**: The provisioner may give the guest the right to access the Internet only; or the provisioner may give the guest the right to use the campus intranet (which includes the local campus network and the Internet).

    c. **Access zones**: The provisioner may give the guest the right to connect from Building 1's public areas only; to connect from Building 2's public areas only; or to connect from either location.

    Restrictions on **access types** are typically enforced by checking the type or properties of the authenticator (switch or AP) through which the user is connecting. Restrictions on **network rights** are typically enforced by provisioning the user onto a VLAN that offers access to only the allowed sections of the network. Restrictions on **access zones** are typically enforced by checking the location of the authenticator through which the user is connecting. In the sections that follow, we will create rules to enforce each restriction type, and we will assemble the rules into a complete guest authorization policy.

13. Write Authorization rules that limit *access types.*

In this example, each restriction set on the way a guest can connect aligns with a specific type of authenticator hardware. Essentially, we will check the type of authenticator that the user is attempting to connect through, and make our allow/deny decision based on that.

We need three rules for limiting access types: the first ensures that web-auth only users can only log in via the web authentication portal, the second ensures that 802.1X-only users can only log in via other 802.1X-equipped switches, and the third is a fail-safe to catch and reject users who are not labelled with an access type. The rules are described below.

The web authentication-only rule, "chkAccType-Webauth": First, we will write a web authentication-only rule that can be applied to a user, requiring that he or she authenticate via the Ignition Server 600S web portal (you may use any type of web portal for this). We will call this rule **chkAccType-Webauth**. (You can use any name you like, but we have kept the names short in this example to make them readable in the Ignition Server Policy Management window.)

In English, we can state this rule as follows: If the user has been flagged as Web-Authentication and not Secure-802.1X-Authentication, then check the model of the authenticator. If it is not "600S," then reject the user.

In the Policy Management window, the **chkAccType-Webauth** rule translates as follows: (Note that Ignition Server uses the "!" symbol to mean, "not," so that in this rule, "!=600S" means "is not 600S".)

```
IF (User.group-member is any one of [Web-Authentication] AND User.group-member is
not any one of [Secure-802.1XAuthentication] AND Authenticator.Authenticator
Device Model != 600S ) THEN Reject Without Outbound Values.
```

The procedure below provides step-by-step instructions for creating this rule. To skip this procedure and see the next rule description, turn to page 13.2.

Create the **chkAccType-Webauth** rule as follows:

a. In Ignition Dashboard's main navigation tree, expand Access Policies, expand **RADIUS**, and click the name of the policy your created in Step-by-step configuration in Ignition Dashboard on page 77.

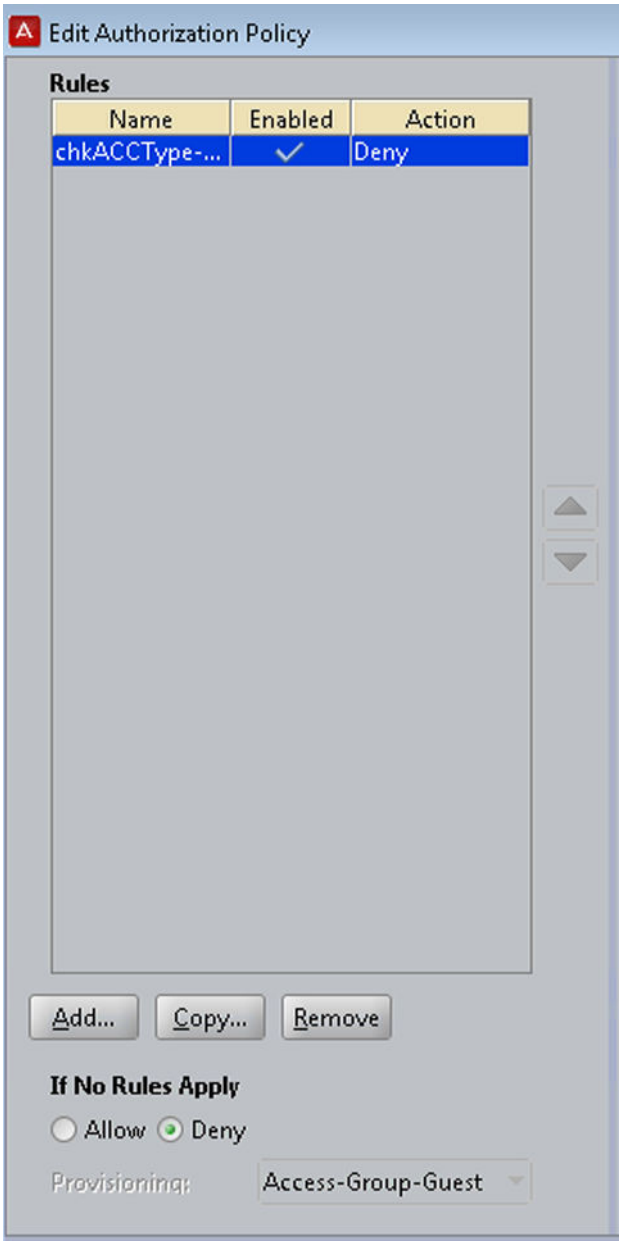
b. In the main part of the window, click the **Authorization Policy** tab.

c. In the upper right of the **RADIUS Authorization Policy** section, click **Edit**.

   Your policy will consist of a number of rules. Each rule allows or denies a user access based on an evaluation of the login request.

d. Begin creating your first rule by clicking the **Add** button under the **Rules** list of the Edit Authorization Policy window.

e. In the New Rule window, type a Name for the rule. Call this rule, “chkAccType-Webauth” and click **OK**.



f. In the **Rules** list of the Edit Authorization Policy window, click your new rule's name to select it.

When your rule is selected, the rest of the fields in this window (everything below the **Selected Rule Details** line) allow you to edit the Rule.

Your rule consists of *constraints* that can be ANDed and ORed together.It is a good idea to sketch out your desired constraints now. Bearing in mind that the limits applied to a guest user are expressed as “groupmember” attributes, and that the authenticator's model name is expressed as an “Authenticator Device Model” in Ignition, we can

express this rule as a phrase of three constraints: “If the User's groupmember is Web-Authentication AND the User’s group-member is not Secure-802.1X-Authentication AND the authenticator's Device Model is not 600S, then we should deny his or her access request.”

g. Click the **New** button next to the Constraint table to add the first of the three constraints. Add the constraint as follows:

   - In the Constraint Details window, select an Attribute Category of **User**.
   - A list of attributes appears below. In this list, click **group-member**.
   - On the right side of the window, you will describe the constraint to which the attribute's value will be compared. In the dropdown list on the right, select **Contains Any**.
   - Click the **Static Value** radio button.
   - Click **Add** to add the comparison value(s).
   - In the Add Value window, click the Add Group dropdown list and choose **Web-Authentication**.
   - Click **OK** to close the Add Value window.
   - Click **OK** to close the Constraint Details window.

h. In the Edit Authorization Policy window, go to the And/Or column in the Constraint table. In the row of your just-added constraint, select **AND** from the dropdown list.

i. Click the **New** button next to the Constraint table to add the second of the three constraints.

   Add the constraint as follows:

   - Select an Attribute Category of **User**.
   - In the list, click **group-member**.
   - In the dropdown list on the right, select **Does Not Contain Any**. This time we are just making sure that the user has been given the right to web auth and web auth only. If the user also has the right to use 802.1X authentication, then we do not want this Deny rule to fire.
   - Click **Static Value**.
   - Click the **Add** button below this.
   - In the dropdown list, choose **Secure-802.1X-Authentication**.
   - Click **OK** to close the Add Value window.
   - Click **OK** to close the Constraint Details window.

j. In the User Authorization Policy window, go to the And/Or column for the just-added constraint and select **AND** from the dropdown list.

k. Click the **New** button next to the Constraint table to add the last of the three constraints:

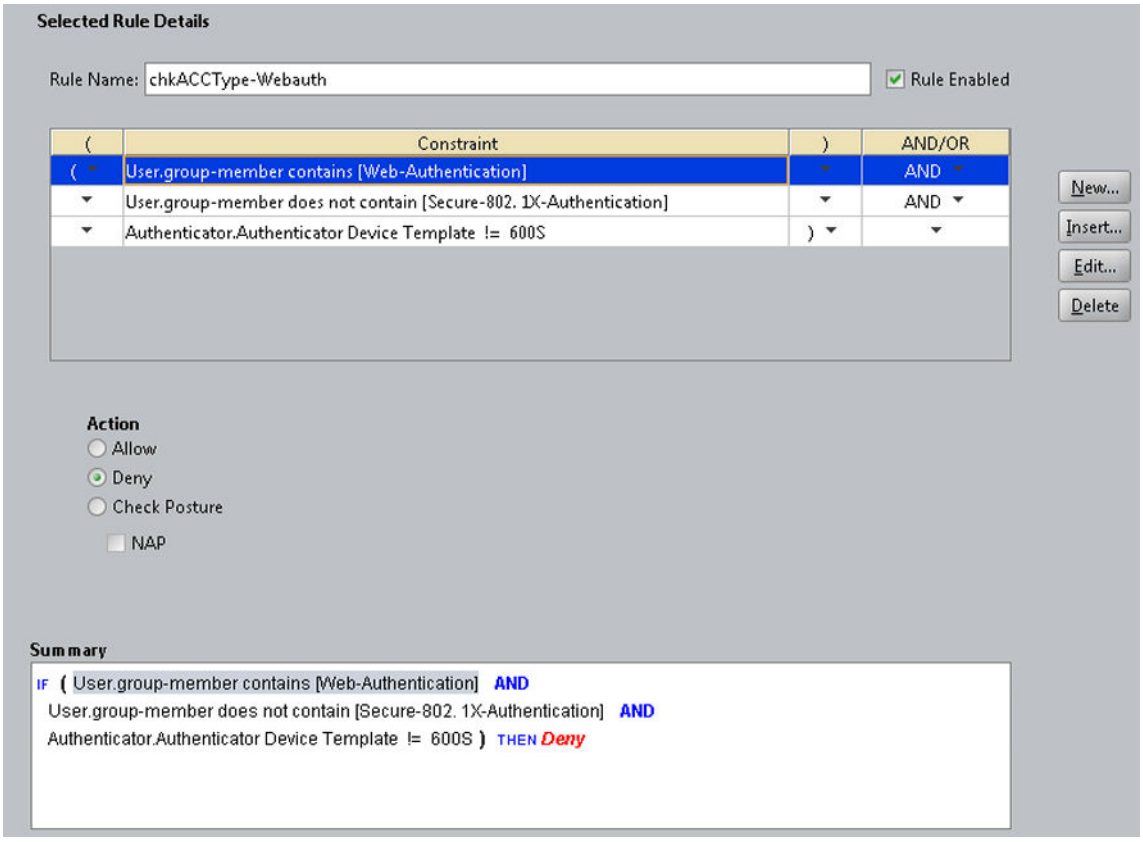
   - Select an Attribute Category of **Authenticator**.

- In the list, click **Authenticator Device Template**.
- In the dropdown list on the right, select **Not Equal To**.
- Click the **Static Value** radio button.
- In the dropdown list, choose **600S**.
- Click **OK** to close the Constraint Details window.

l. To complete the rule:

- In the Edit Authorization Policy window, click the **Deny** radio button.
- Click on the first constraint in the table, go to the left parentheses column, and select "(" from the dropdown list.
- Click on the last constraint in the table, go to the right parentheses column, and select ")" from the dropdown list.
- Under the **Action** section, click the **Deny** radio button.
- Your finished rule will look like the illustration shown below:

There is no need to close the window if you plan to add the rest of the rules now. You can continue adding rules by clicking the **New** button.



The sections that follow do not contain step-by-step instructions on writing the rest of the rules. To write them, follow the general steps you used previously for the

chkAccType-Webauth rule, and consult the *Avaya Identity Engines Ignition Server Administration*, NN47280-600.

The 802.1X authentication-only rule, "chkAccType-8021X": Second, we'll write an 802.1X authentication-only rule that can be applied to a user, requiring that he or she authenticate via 802.1X authentication. In our service category, only the 600S device allows web-based authentication, and all other switches and access points require 802.1X authentication. For this reason, we can write this rule as follows: If the user has been flagged as Secure-802.1XAuthentication and not Web-Authentication, then check the model of the authenticator. If it is "600S," then reject the user.

In the Policy Management window, the **chkAccType-8021X** rule translates to:

```
IF (User.group-member is any one of [Secure-802.1X-Authentication]
    AND User.group-member is not any one of [Web-Authentication]
    AND Authenticator.Authenticator Device Model = 600S )
THEN Deny.
```

The is-Empty rule, "chkAccType-isEmpty": Third, we'll write a rule that catches and rejects any user who has no access type designation. We can state this rule as follows: If the user bears neither the Secure-802.1XAuthentication flag nor the Web-Authentication flag, then reject him/her. In the Policy Management window, the chkAccType-isEmpty rule translates to:

```
IF User.group-member is not any one of
    [Web-Authentication,Secure-802.1X-Authentication]
THEN Deny.
```

14. Write Authorization rules that limit *Access Zones.*

    To limit the physical locations from which a user can connect, we will write a set of rules that check the authenticator's location in the Ignition Server container hierarchy. Recall that we labelled each switch and access point with a location label, by placing it in the hierarchy when we performed the steps on Create your authenticators on page 77.

    We need three rules for limiting user location:

    chkAccZone-Bldg1 checks if the user is limited to connecting from Building 1, and if so, makes sure she is authenticating via a switch in that building:

    ```
    IF ( User.group-member contains [Building-1-Public-Areas] AND
    User.group-member does not contain [Building-2-Public-Areas] AND
    Authenticator.Authenticator Container does not contain [Chapel-Hill-Building-1] )
    THEN Deny.
    ```

    chkAccZone-Bldg2 works just like the previous rule, but for Building 2:

    ```
    IF ( User.group-member contains [Building-2-Public-Areas] AND
    User.group-member does not contain [Building-1-Public-Areas] AND
    Authenticator.Authenticator Container does not contain [Chapel-Hill-Building-2] )
    THEN Deny.
    ```

    chkAccZone-isEmpty rejects any user who has no access zone rights:

    ```
    IF User.group-member is not any one of [Building-1-Public-
    Areas,Building-2-Public-Areas] THEN Deny.
    ```

Note that there is no rule for the case of a user who has rights to both Building 1 and Building 2. This is because we want a user with rights to both buildings to fall through this trio of rules without triggering a reject.

15. Write Authorization rules that limit *Network Rights.*

    The preceding rules can be thought of as filters because they are all Deny rules designed to reject users who are in violation of the guest authorization policy. If a user passes through the filter rules he or she arrives at the Allow rules, where if he or she has the right permissions he or she will trigger an Allow rule and be granted access.

    The final trio of rules, the *network rights* rules, contains one more filter rule and two Allow rules. We will limit the guest's network rights by placing him/her on a VLAN that offers access to only the appropriate sections of the network. Three rules are needed:

    chkNetwkRt-isEmpty finds and rejects users who have no network right assigned.

    ```
    IF User.group-member is not any one of [Internet,Campus-Intranet]
    THEN Deny.
    ```

    The final two rules are the *Allow rules*. They assign the user to the appropriate VLAN based on his or her group-member attribute. The attentive reader will notice there is no "AND *User.group-member is not any one of*" phrase as there was in some of the other rules. This phrase can be left out here because network rights are set via a radio button (as opposed to a series of check boxes which might all be ticked) in the Guest Manager window, so no user will be a group-member of both groups.

    chkNetwkRt-Internet assigns the user to VLAN 10 (also known as "VLAN Internet"):

    ```
    IF User.group-member is any one of [Internet]
    THEN Allow With Outbound Values VLAN Internet
    ```

    chkNetwkRt-CampusIntranet assigns the user to VLAN 20 (also known as "VLAN Intranet"):

    ```
    IF User.group-member is any one of [Campus-Intranet]
    THEN Allow With Outbound Values VLAN Intranet
    ```

16. Sort the rules to create your policy

    You can sort your rules in the following order to make them easier for you and your fellow network administrators to read:

    - chkAccType-Webauth
    - chkAccType-8021X
    - chkAccType-isEmpty
    - chkAccZone-Bldg1
    - chkAccZone-Bldg2
    - chkAccZone-isEmpty
    - chkNetwkRt-isEmpty
    - chkNetwkRt-Internet
    - chkNetwkRt-CampusIntranet

Sorting is not required in most cases, because Ignition Server always evaluates every rule in the set until it triggers a Deny or reaches the end of the set. If it reaches the end of the set and one or more Allows has been triggered, then the user is granted access.

The one case that requires a sorted rule set is this: If you have a rule set in which a user might trigger two (or more) Allow rules that set the same outbound attribute to different values, then Ignition Server will only send the first-triggered outbound value. For example, if a user triggered a rule assigning him or her to VLAN 10 and also triggered a subsequent rule assigning him or her to VLAN 20, then Ignition Server will assign him or her to VLAN 10.

Click **OK** to close the Edit Authorization Policy window.

Creating a minimal authorization policy

You may elect not to create user groups as explained earlier in this chapter. If you do this, then Guest Manager's Create Provisioner page and Create Guest User page will not display any access constraint check boxes, and your provisioners will not be able to set access constraints on guest users.

To create a minimal authorization policy (no access constraint check boxes will appear on the Guest User page), follow the instructions in the section *Avaya Identity Engines Ignition Server Administration*, NN47280-600.

Chapter 8: Setting Up Self-Provisioning

Avaya Identity Engines Ignition Guest Manager allows you to create two types of self-provisioning portals: Guest User and Device. A Guest User self-provisioning portal is a web site that allows users to self-register to create their own temporary network accounts. A Device self-provisioning portal is a web site that allows users to register a device. When you create a self-provisioning portal, Guest Manager deploys it as an application on the web server where Guest Manager is running. You will point arriving guests to the portal's URL so that they may use the self-registering feature.

Typically, an arriving guest will use a kiosk computer in an entry hall to fill out the self-provisioning portal page. When their account is created the portal sends the user his or her password in an email, SMS message, or to a front desk receptionist who can print it out.

As the Guest Manager administrator, when you create a self-provisioning portal you specify how long a self-provisioned account lasts, what network rights a user has, and the restrictions that are placed on the user's login conditions. A self-provisioned account appears as a guest user account in Ignition, and is managed like any other guest user account, as explained in Provisioner application: Managing guests and devices on page 134.

You may create as many self-provisioning portals as you need, but keep in mind that creating each portal causes a dedicated provisioner account to be created. This dedicated provisioner owns the guest accounts created through each portal.

Creating a Self-Provisioning service

Follow the steps below to create a self-provisioning portal.

Before you begin

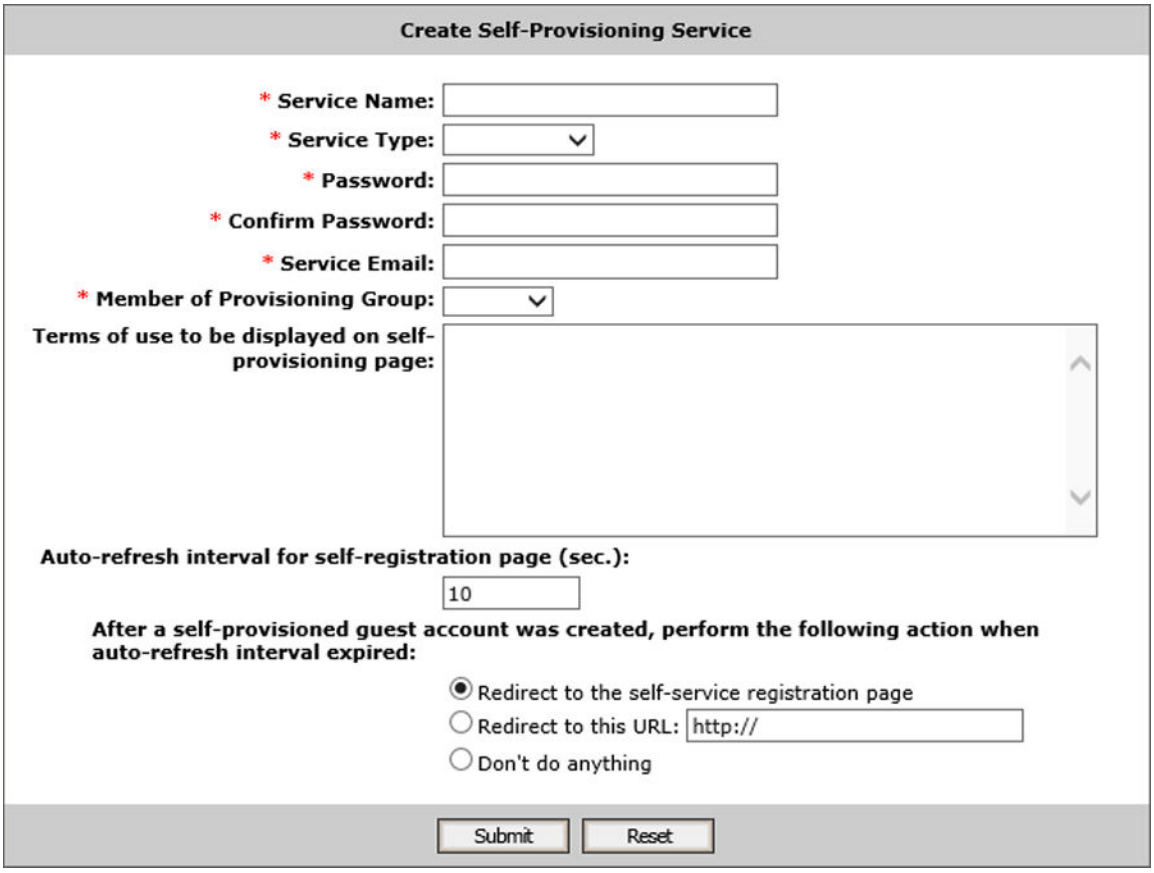
When you create a self-provisioning portal, Guest Manager deploys it automatically on the server where Guest Manager is running.

Make sure you have configured Guest Manager to send new guest users their guest account access details. Do one or both of the following:

- Set Guest Manager to send email notifications, as explained in Setting up Email notification parameters on page 59.
- Set Guest Manager to send SMS messages, as explained in Setting up SMS notification parameters on page 61.

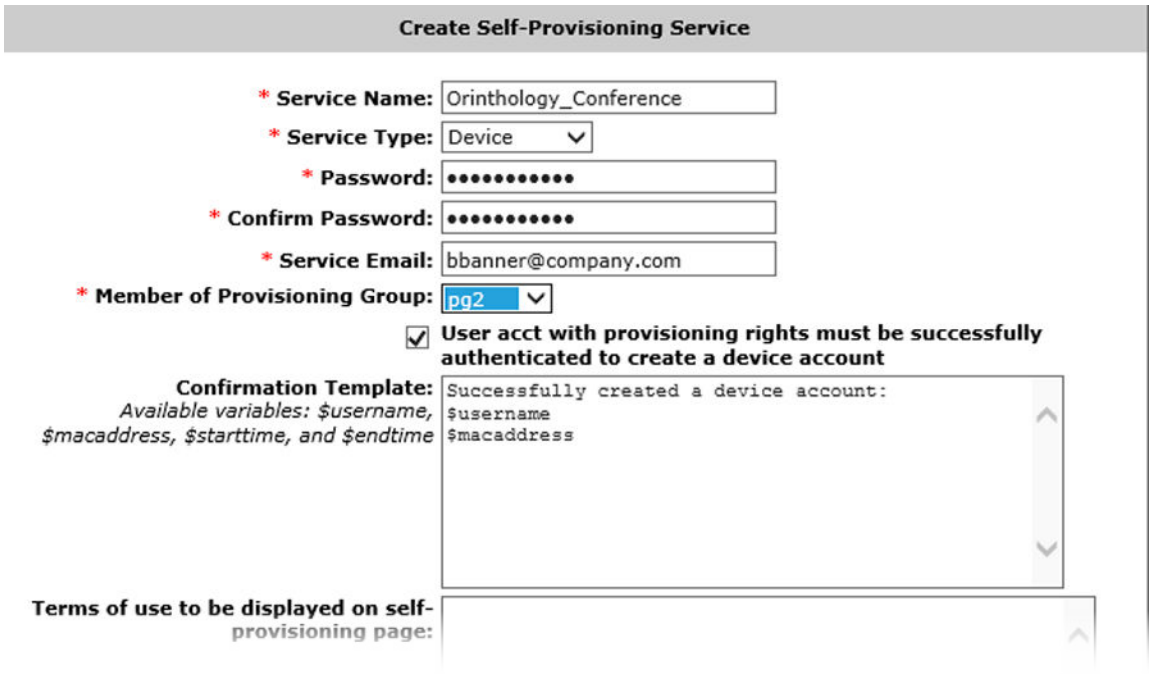
Procedure

1. Log in to the Administrator Application.
2. Click **Provisioners** from the main toolbar. Click **Action** and select **New Self-Provisioner**. The Create Self-Provisioning Service screen appears.



3. Set the portal's account details. The service you are creating will consist of a Self-Provisioning Service and the account, so you must provide the information needed to set up the service.
   - The **Service Name** is the name of the provisioner account that manages the portal and is also used as the URL for the portal. Only numbers and characters are allowed in the name. No spaces or periods may be used. The length of this name must be 30 characters or less.
   - The **Service Type** field has two options Guest User and Device. Select one of the two.
     - If you select **Device** as the Service Type, the **User acct with provisioning rights must be successfully authenticated to create a device account** check box appears. If you select this check box, only provisioners who are successfully authenticated are allowed to create a device account (that is, Guest users are not allowed to create a device account).
     - If you select **Device** as the Service Type, the **Confirmation Template** field appears. Use the **Confirmation Template** field to specify how the confirmation message

appears. **The Confirmation Template** field contains default variables to display the user name and MAC address as part of the confirmation message. You can add variables to display the start time and end time of the device account in the confirmation message.



- **Password** and **Confirm Password**: Set the provisioner's password in these two fields. Since Guest Manager encrypts the password, you should note your entry now for future reference.

  Important:

  Do not type single or double quotation marks in the password field. Doing so can cause the entered password to be clipped at the location of the first quotation mark.

- **Service Email**: Enter the email address of the provisioner.

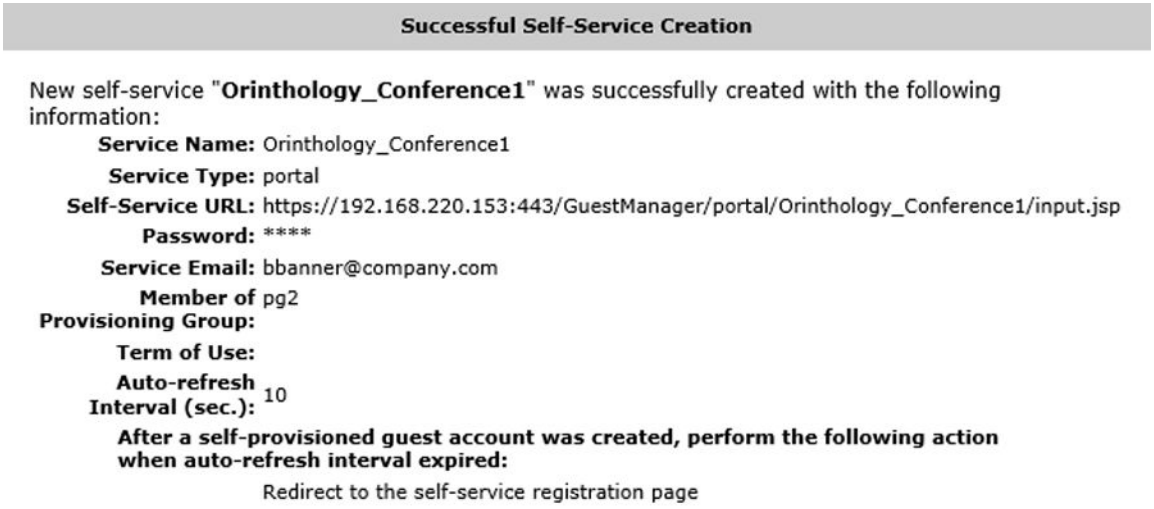
  If at any time you wish to reset all fields to the state they were in when you opened the window, click the **Reset** button.

4. In the **Member of Provisioning Group** drop-down list, choose the provisioning group that will set the permissions limits for guests created through this portal. Limits include life span of the guest accounts, allowed access zones, etc. To see the limits, click **Provisioning Groups** on the left and click on the provisioning group you want to view.

   If you are creating a Device portal, under the **Device** tab, ensure that you select the **Allow** radio button to give provisioners in this provisioning group the right to manage (create, edit, associate) devices.

5. In the **Terms of use to be displayed on self-provisioning page** field, enter the terms to be displayed on the Self Provisioning page.

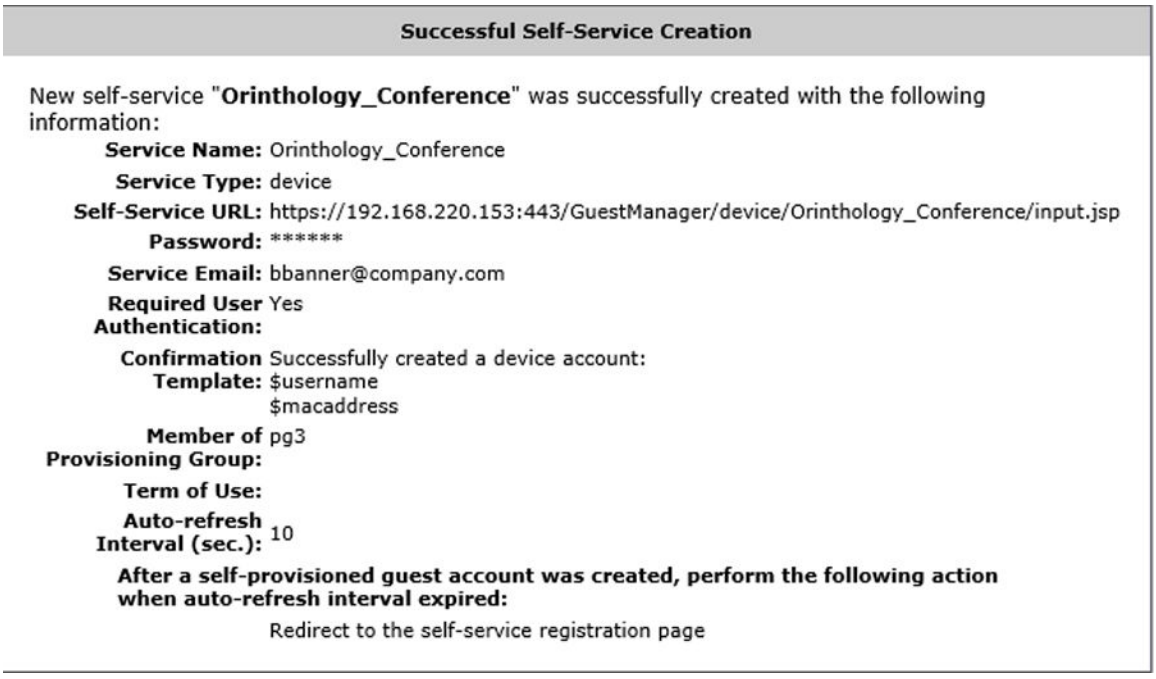
6. In the **Auto-refresh interval for self-registration page (sec.)** field, enter the value for the refresh interval.
7. In the **After a self-provisioned guest account was created, perform the following action when auto-refresh interval expired** field, select one of the options presented that meet your requirements.
8. Check your entries and click **Submit**. Guest Manager Creates the Self-Provisioning Service and the Portal Provisioner account.
9. If the provisioner is someone other than you, notify him or her of the new provisioner username and password.



Successful Self-Service Creation

New self-service "**Orinthology_Conference1**" was successfully created with the following information:

Service Name: Orinthology_Conference1
Service Type: portal
Self-Service URL: https://192.168.220.153:443/GuestManager/portal/Orinthology_Conference1/input.jsp
Password: ****
Service Email: bbanner@company.com
Member of Provisioning Group: pg2
Term of Use:
Auto-refresh Interval (sec.): 10
After a self-provisioned guest account was created, perform the following action when auto-refresh interval expired:
Redirect to the self-service registration page



Successful Self-Service Creation

New self-service "**Orinthology_Conference**" was successfully created with the following information:

Service Name: Orinthology_Conference
Service Type: device
Self-Service URL: https://192.168.220.153:443/GuestManager/device/Orinthology_Conference/input.jsp
Password: ******
Service Email: bbanner@company.com
Required User Authentication: Yes
Confirmation Template: Successfully created a device account:
$username
$macaddress
Member of Provisioning Group: pg3
Term of Use:
Auto-refresh Interval (sec.): 10
After a self-provisioned guest account was created, perform the following action when auto-refresh interval expired:
Redirect to the self-service registration page

Deploying a self-provisioning service

When you create a self-provisioning service, Guest Manager deploys it automatically on the server where Guest Manager is running.

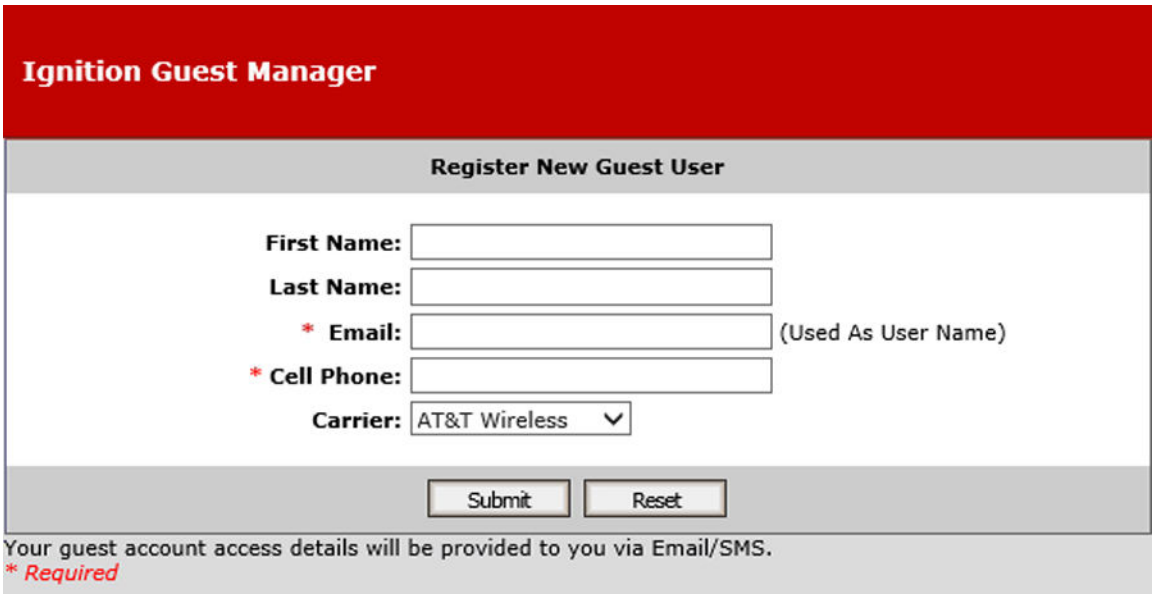
Procedure

1. Find the URL of the self-provisioning service:
   - Log in to the Administrator Application.
   - Click **Self-Service** from the main toolbar.
   - Find your portal in the **Self-Provisioning Service** list. The **URL** column shows the URL for the service.
2. On the computer that guests will use to create their accounts, set up a browser window that points to the portal URL. For example, the Guest User example in the previous section uses the following URL: https://<server_name>/GuestManager/portal/Orinthology_Conference/input.jsp

   Note that the URLs for Device portals are different than the URLs for Guest User portals. For example, the Device portal example in the previous section uses the following URL:

   https://<server_name>/GuestManager/device/Orinthology_Conference/input.jsp

   With an Internet Explorer 8.0 browser, you may see the URL truncated especially if you are viewing with larger fonts. In this case, do the following:
   - Decrease the font size so you can see the complete URL.
   - Use an older version of the browser (6.0) or other browsers that do not have this problem.
3. Test the page. The Register New Guest User page should appear as follows.



When a new user clicks **Submit**, his or her account is created, and the account details are sent to the specified email address or mobile telephone number. After a few seconds, the page refreshes, displaying a new Register New Guest User page for the next guest.

The Register New Device page should appear as follows:

4. For security, Avaya strongly recommends that you disable unneeded features in the web browser that displays your self-provisioning portal. Disable all menus, tool bars, and the URL address bar.
5. Guest Manager must be connected to the Avaya Identity Engines Ignition Server appliance at all times for the self-provisioning portal to operate. To connect, see Connecting Guest Manager to the Ignition Server Appliance on page 67.

Managing self-provisioned users

To manage self-provisioned users, you must be the portal provisioner who manages the portal where the guests created their accounts.

Procedure

1. Run the Provisioner Application. For instructions, see Launching the provisioner application on page 138.
2. Log in using the portal provisioner user name and password you received from your Guest Manager administrator.

   If you do not have this user name and password, ask your administrator.

   The administrator can get your portal provisioner name and reset your password by running the Guest Manager Administrator Application, clicking the **Self-Service** button, clicking the name of your portal, and making changes there.
3. Click the **Guest Users** button. See Viewing guest user accounts on page 143 for further information.

Deleting a self-provisioning portal

The steps below explain how to delete a self-provisioning portal. When you delete a portal, Guest Manager deletes the portal application and its portal provisioner account.

Procedure

1. Run the Administrator Application.
2. Click the **Provisioners** button.
3. In the Provisioners table, tick the check box of the portal you wish to delete.
4. Click the **Action** button and select **Delete Provisioners** button. In the confirmation dialog, click **OK**.

   The portal application is deleted and the portal provisioner is deleted.

   Guest user accounts and device accounts that were created by the deleted provisioning portal remain in the provisioning group of the provisioning portal. For information on retrieving these user accounts, see Retrieving the guest users owned by a provisioner on page 131.

Chapter 9: Administrator application: managing provisioners, guests, and devices

The Avaya Identity Engines Ignition Guest Manager *administrator* manages provisioner accounts, manages the Guest Manager application settings and, in most organizations, manages the guest authorization policies. The Guest Manager *administrator* can also delete, export, and reassign guest and device accounts, but not create them.

Guest Manager *provisioners*, in contrast to the Guest Manager *administrator*, exist only to create and manage guest user accounts. Provisioners do not manage other provisioners, nor do they change Guest Manager settings or policies. For a comparison of user types, see Types of accounts in your Ignition Server installation on page 18.

This chapter shows the Guest Manager administrator how to create and manage provisioners, as well as how to perform bulk operations on guest and device accounts, such as deleting expired guest accounts.

If you are a provisioner, you may skip this chapter and proceed to Provisioner application: Managing guests and devices on page 134.

Important:

When using Guest Manager, *do not* use your browser's Refresh command to update a page. Instead, click the appropriate command button on the left side of the window to reload the page. *Do not* open a link in a new tab at any time.

Setting up provisioners

A *provisioner* is a person who creates and manages guest user accounts and device records in Guest Manager.

As the Guest Manager administrator, you use the application to create or map provisioner accounts. Each provisioner account is stored either in the Avaya Identity Engines Ignition Server internal store or in your LDAP or Active Directory store. Your installation may store provisioners in both places at once.

In turn, each provisioner that you create will use the Guest Manager application to create, modify, and delete guest users. The provisioner owns the guest user accounts that he or she creates. If the provisioner's account is deleted, then the guest user accounts it owns are either transferred to other provisioners or deleted.

Creating a provisioning group

A provisioning group is a container for provisioners, guest users, and device records. Typically, the provisioning group collects a number of provisioners (or self-provisioners) who work together to manage a set of guest accounts. The provisioning group establishes the administrative rights and account settings of the provisioners that belong to it.

You create a provisioning group for each set of provisioners that requires a unique set of rules for creating guest users. Every provisioner must belong to at least one provisioning group.

Procedure

1. Run the Administrator Application:
   - Open a browser and navigate to the Administrator Application URL.
   - Type your Guest Manager administrator `username` and `password`.
   - Guest Manager must be connected with the Ignition Server appliance. If it is not connected now, see Connecting Guest Manager to the Ignition Server Appliance on page 67.
2. Click the **Provisioning Groups** section in the main toolbar. The Provisioning Groups screen appears.
3. Click **Actions** > **New Provisioning Group**.
4. Configure the provisioning group name and common details for this provisioning group. See Configuring the common details on page 106.
5. Configure the guest user account details. See Configuring the guest user account details on page 107.
6. If self-service guest users must be approved by a sponsor before they are granted access, configure sponsor approval. See Configuring sponsor approval on page 110.
7. Configure the device records for this provisioning group. See Configuring the device record details on page 111.

   Important:

   If you configured sponsor approval, you cannot allow provisioners in this provisioning group to manage devices.
8. Configure the contents of the account notification messages sent to guest users. See Configuring the account notification templates on page 114.
9. If required, configure the advanced details for this provisioning group. See Configuring advanced details on page 116.

10. Check your entries and click **Submit**. Guest Manager creates the provisioning group.

Configuring the common details

Use the **Common** tab to configure some common details for this provisioning group.

Procedure

1. Enter a Group Name for the group.
2. If the provisioners in this group will collaborate to manage guest users, check the **Provisioners in this group can view and edit each other's records** check box. If you wish to limit each provisioner so that he or she can see only the guest accounts that he or she has created, do not check this check box.
3. Set the maximum account life span the group's provisioners can grant to a guest. In the **Temporary accounts may be valid for up to** section, set the maximum life span by selecting the radio button to specify the units (minutes, hours or days) and then entering the number of minutes, hours or days in the preceding field.
4. Set the provisioners' scope of authority. For this, use the check boxes in the lower part of the Create Provisioning Group screen labelled, **Areas to which guest users/devices can be granted access**.

   Check the check box for each access type, network right, and access zone that this group's provisioners may grant to guests. For information on these check boxes, see Access constraint check boxes on the Create Guest User page on page 73.

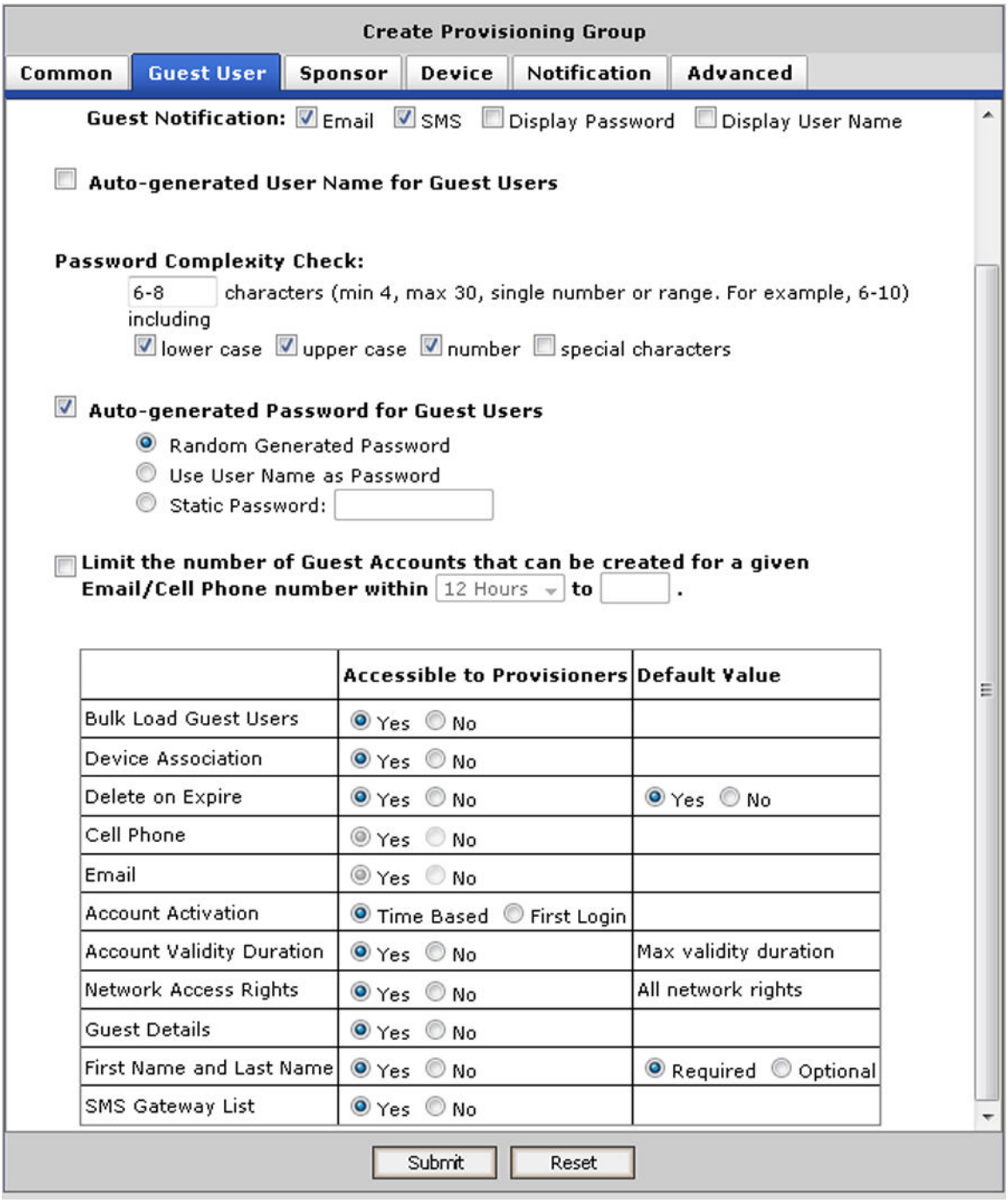
   For example, if you wish to create a provisioner who can grant guests intranet access over secure 802.1X connections in any of your building locations, check the check boxes as follows:

Next steps

Go to Configuring the guest user account details on page 107.

Configuring the guest user account details

Use the **Guest User** tab to configure the guest user account details for this provisioning group.



Procedure

1. In the **Guest Notification** section, select the ways that this group's provisioners will notify guests of their new guest accounts. Select all that apply.
   - **Email** Check this box to notify guest users of their new guest user accounts by way of email.

- **SMS** Check this box to notify guest users of their new guest user accounts by way of SMS.
- **Display Password** Check this box to include the password in the message that is displayed when a guest user account is successfully created (self-service or by provisioner).
- **Display User Name** Check this box to include the username in the message that is displayed when a guest user account is successfully created (self-service or by provisioner).

2. Check the **Auto-generated User Name for Guest Users** check box to pre-populate a guest user name and increase the likelihood that it will be unique. Select one of the following:
   - **Generate User Name with** Use the radio buttons below the check box to define the format of the guest user name. The default auto-generated guest user name format is: FirstnameandLastname (for example, John Smith -> JohnSmith) with three random numbers as a suffix. For example, if a provisioner creates a user with first and last name “Tom” and “Jones,” Guest Manager will default his user name to “TomJonesXYZ” where “XYZ” is a three digit random number.
   - **Use Email as User Name**
   - **Use Cell Phone Number as User Name**
3. In the **Password Complexity Check** section, select the requirements for passwords.
4. Check the **Auto-generated Password for Guest Users** field if you want the provisioner to be able to auto-generate passwords for the guest users that he or she owns. In this case, the user does not have to enter a password to login. Select the type of auto-generated password.
   - **Random Generated Password**
   - **Use User Name as Password**
   - **Static Password** Enter the static password.

   If you select to use the user name as the password or enter a static password, the guest user can log in with only a user name. The Access Portal login page must be modified to accept a user name without a password. You must be able to set the password as a fixed string so that a single password can be used for multiple accounts.
5. If required, check the box to **Limit the number of Guest Accounts that can be created for a given Email/Phone number**. Select the number of hours and enter the number of guest accounts.
6. Select the options that are accessible to provisioners and the default value, if appropriate.
   - Bulk Load Guest Users
   - Device Association
   - Delete on Expire
   - Cell Phone
   - Email

- Account Activation
- Account Validity Duration
- Network Access Rights
- Guest Details
- First Name and Last Name
- SMS Gateway List. If you select **No**, the SMS Gateway List is not accessible to Provisioner/Self-service guest user registration and SMS messages are sent using the configured default gateway for each service provider.

  Important:

  If a guest user's cell phone service provider does not support the configured default gateway, the SMS messages are not sent.

Next steps

Do one of the following:

- If sponsor approval is required for the self-service guest users in this provisioning group, go to Configuring sponsor approval on page 110.
- If this provisioning group manages devices, go to Configuring the device record details on page 111.
- Otherwise go to Configuring the account notification templates on page 114.

Configuring sponsor approval

Configure sponsor approval if self-service guest users must be approved by a sponsor before they are granted access.

If sponsor approval is required, provisioners in this provisioning group cannot manage devices.

Procedure

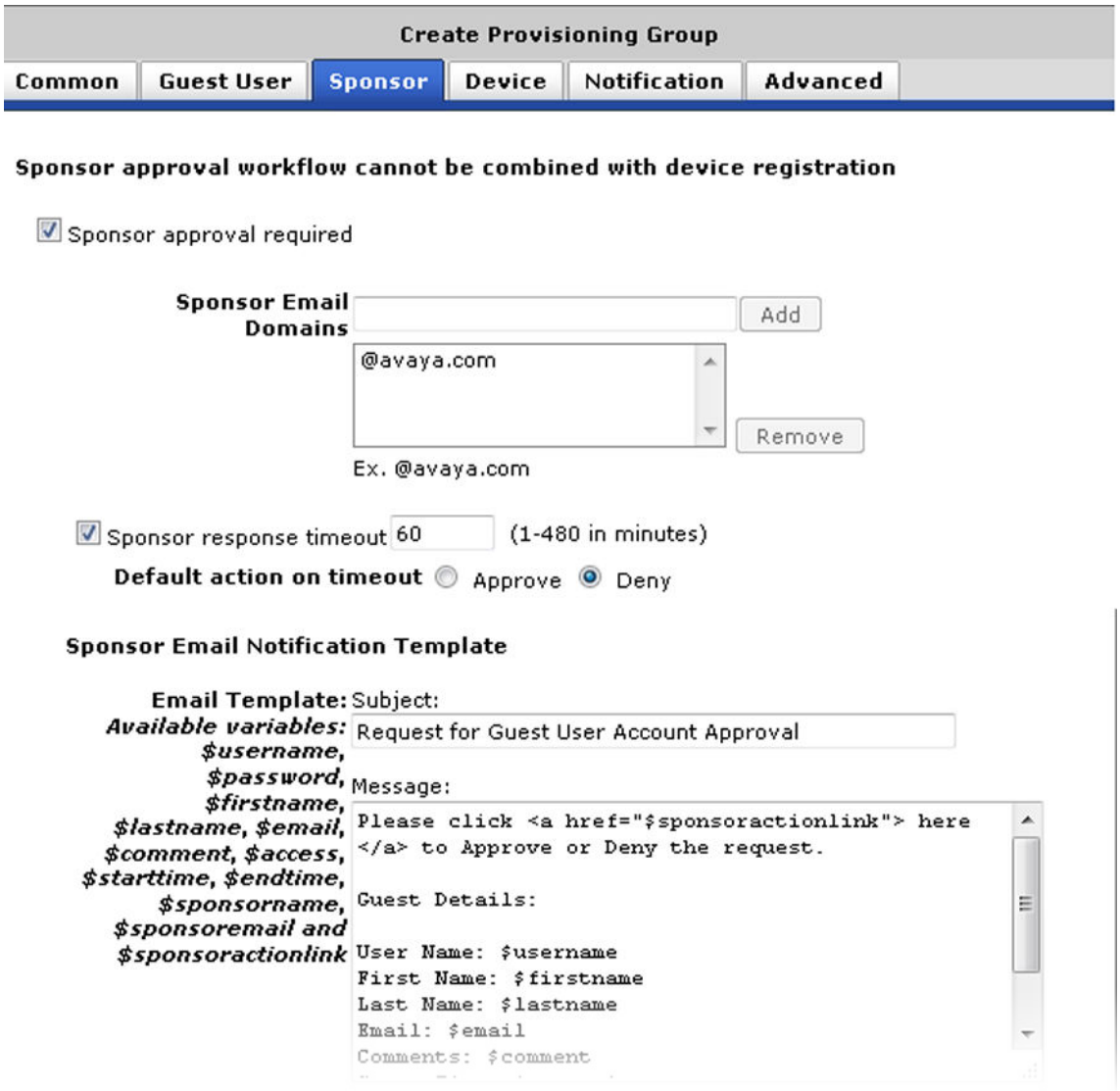
1. On the **Sponsor** tab, check the **Sponsor approval required** check box.
2. To force a guest user to have a sponsor in a particular domain, enter the allowed domain in the **Sponsor Emails Domain** field and click **Add**. For example, enter @avaya.com to force the guest to enter an email address with @avaya.com.

   Repeat to add additional domains.
3. If required, configure a time limit for the sponsor approval and the default action when the time limit passes.
   a. Check the **Sponsor response timeout** check box and enter a time in minutes.
   b. In the **Default action on timeout** field, select **Approve** or **Deny**.
4. In the **Sponsor Email Notification Template** section, enter the contents of the email message to send to the sponsor to approve or deny the request for a guest user account.

Important:

The notification email message is HTML-enabled. As a result, you can add an HTML tag that is rendered in HTML format.

Example



Next steps

Go to Configuring the account notification templates on page 114.

Configuring the device record details

Use the **Device** tab to configure the device record details for this provisioning group.

If sponsor approval is required, provisioners in this provisioning group cannot manage devices.

Procedure

1. If provisioners in this group can create and edit *device records*, select **Allow** under the heading **Allow or deny provisioners in this provisioning group the right to manage (create, edit, associate) devices**.

   If sponsor approval is required for this provisioning group, select **Deny**.

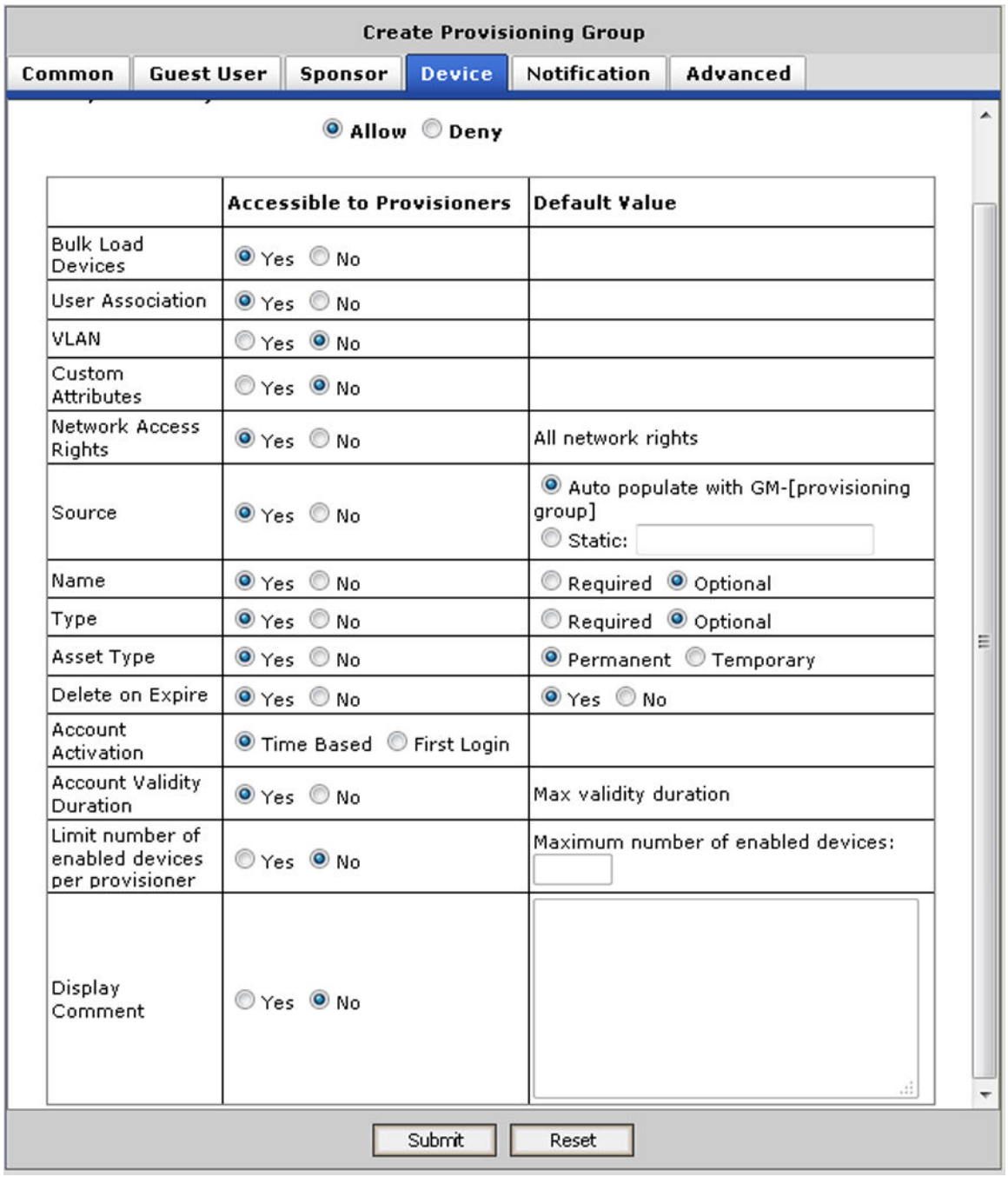
2. Select the following device record settings accessible to provisioners in this provisioning group and, if applicable, select a default value.

   - Bull Load Devices
   - User Association
   - VLAN
   - Custom Attributes
   - Network Access Rights
   - Source
   - Name
   - Type
   - Asset Type
   - Delete on Expire
   - Account Activation
   - Account Validity Duration
   - Limit number of enabled devices per provisioner

     If **Yes**, enter the maximum number of enabled devices allowed for a provisioner.
   - Display Comment

     If **Yes**, enter the comment to be displayed on the provisioner's Create Device page.

Example



Next steps

Go to Configuring the account notification templates on page 114.

Configuring the account notification templates

Use the **Notification** tab to configure the contents of the account notification messages sent to guest users.

Procedure

1. On the **General** tab, use the **SMS Template** to enter the text message to be sent to the guest user's cell phone when a provisioner saves the guest user's account. For instructions on writing the SMS template, see Writing SMS and Email templates for account notifications on page 121.

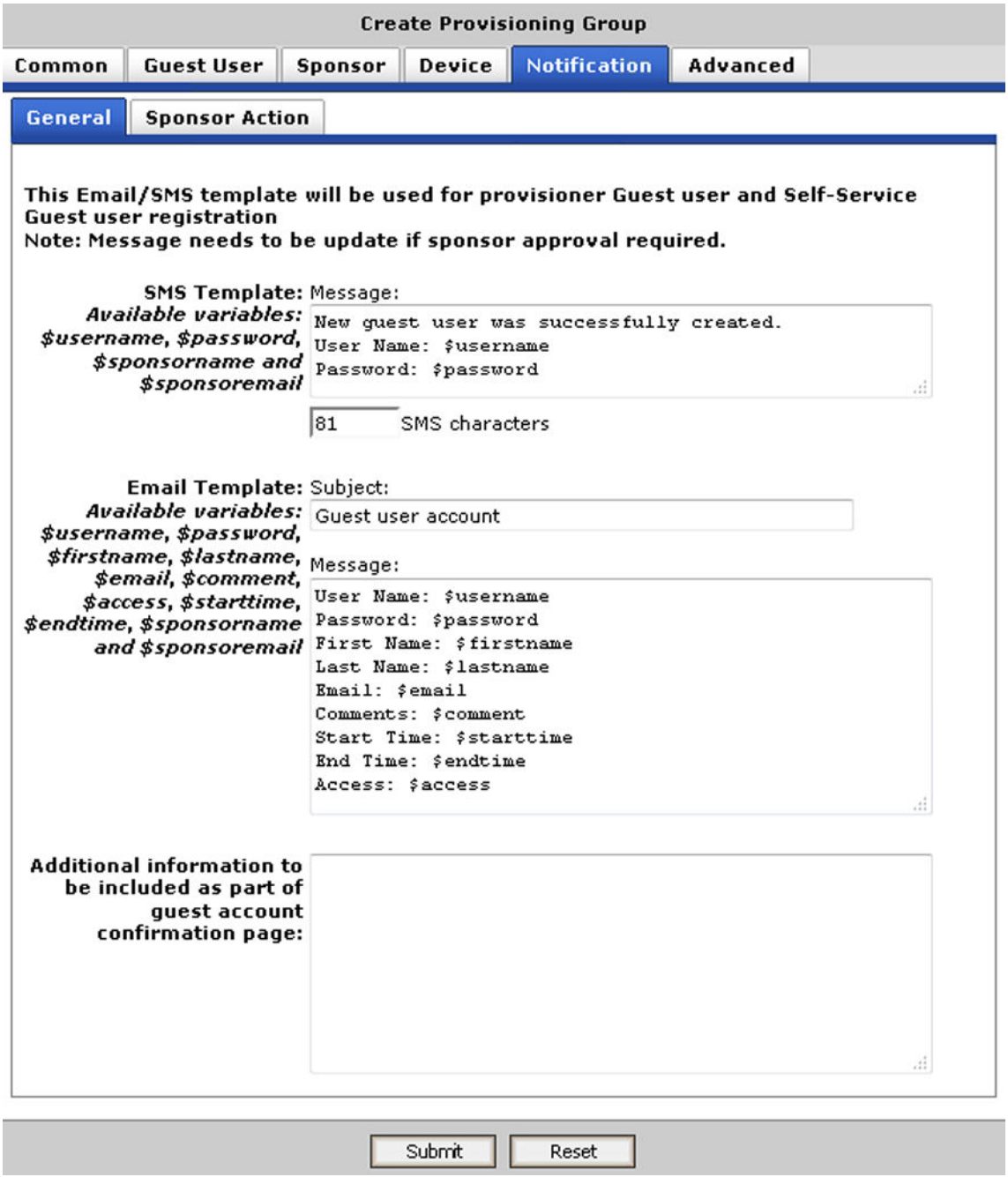
   If sponsor approval is required, change the default message and variables to indicate that the request is pending the approval of the sponsor.

2. On the **General** tab, use the **Email Template** to enter the contents of the confirmation email to be sent to the guest user when a provisioner saves the guest user's account. For instructions on writing the email template, see Writing SMS and Email templates for account notifications on page 121.

   If sponsor approval is required, change the default message and variables to indicate that the request is pending the approval of the sponsor.

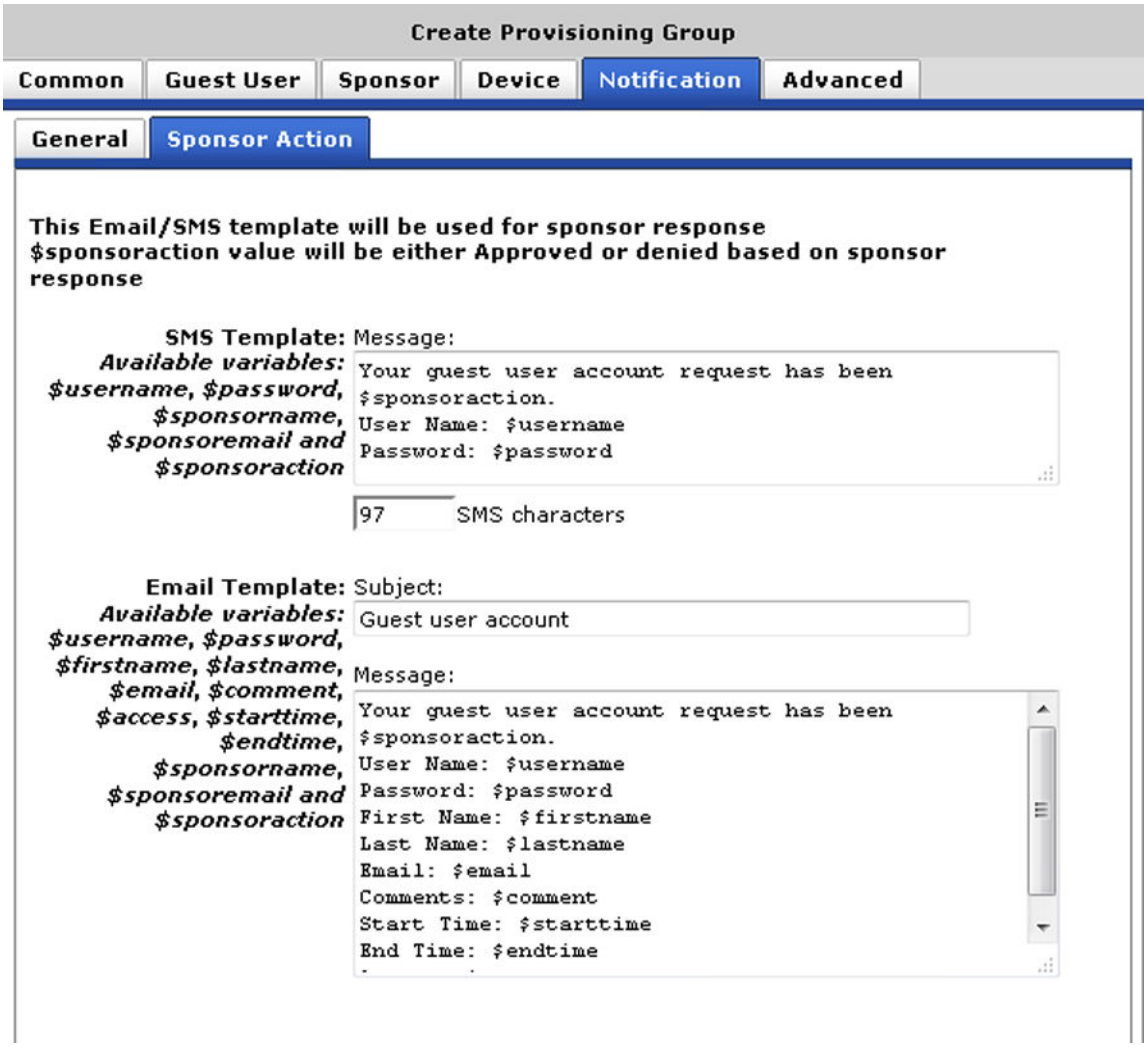
3. If required, enter a message in the **Additional information to be included as part of guest account confirmation page** field to be displayed on the guest account confirmation page when an account is created. The provisioner can print this confirmation and hand it to the guest user.

   Text that you type in the **Additional information** field does not appear on the email confirmation sent to the user. To include a message in the confirmation email to the guest, add the *$comment* variable to the **Email Template** (see Creating a provisioning group on page 105) and have your provisioners type the message in the **Comment** field when creating the guest user.



4. On the **Sponsor Action** tab, use the **SMS Template** to enter the text message to be sent to the guest user's cell phone when a sponsor approves or denies the guest user's account. For instructions on writing the SMS template, see Writing SMS and Email templates for account notifications on page 121.
5. On the **Sponsor Action** tab, use the **Email Template** to enter the email message to be sent to the guest user when a sponsor approves or denies the guest user's account. For

instructions on writing the email template, see Writing SMS and Email templates for account notifications on page 121.



Next steps

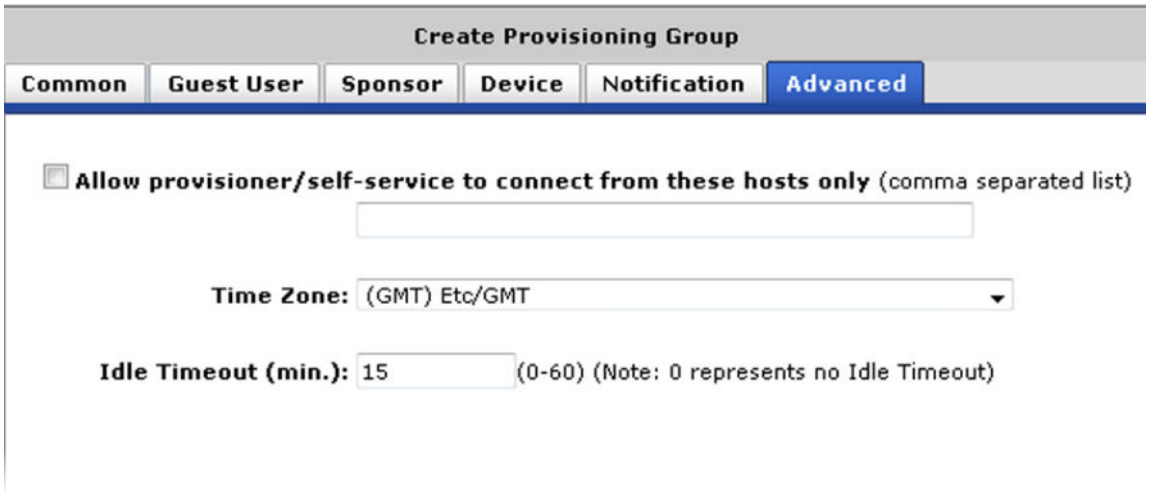
If advanced details are required for this provisioning group, go to Configuring advanced details on page 116. Otherwise, go to Creating a provisioning group on page 105.

Configuring advanced details

Use the **Advanced** tab to

- Limit the locations from which provisioners can log into the Provisioner Application and manage users.
- Select a time zone.

- Configure the period of inactivity after which a provisioner's session in the Provisioner Application automatically disconnects. After the session disconnects, the provisioner must log in again.



Procedure

1. Check the **Allow provisioner/self-service to connect from these hosts only** check box. Enter the fully qualified machine name or IP address in the field just below.

   For example, if the provisioners in this group will be required to log in from a computer with the host name “birne” and the domain of your network is “idengines.com”, enter `birne.idengines.com`.

2. In the **Time Zone** drop-down box, select a time zone.
3. In the **Idle Timeout** field, set the set the time in minutes.

   If a provisioner belongs to multiple provisioning groups, Guest Manager applies the lowest idle timeout number configured among the provisioning groups.

   Idle Timeout does not set an idle timeout for *guest user* accounts — only for *provisioners*.

Next steps

Go to Creating a provisioning group on page 105.

Creating a provisioner in the internal store

A provisioner is a member of your organization who will create and manage guest users and devices. Each provisioner account is stored either in the Ignition Server internal store or in your LDAP or Active Directory store. This section explains how to create a provisioner account *in the internal store*. We refer to these internally stored provisioners as *internal provisioners*.

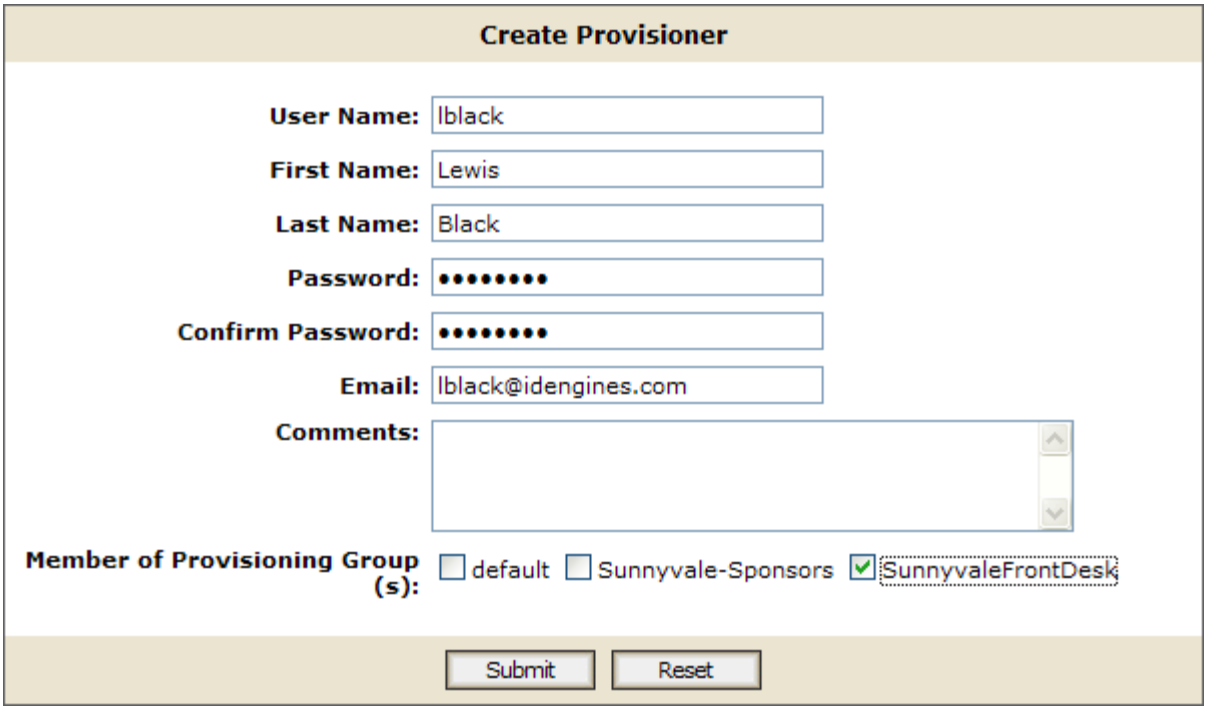
To authenticate provisioners against LDAP or AD, see Creating a provisioner from an account in an LDAP or AD store on page 119. To bulk-import provisioners, see Bulk importing provisioner accounts from a file on page 119.

Before you begin

Before you create a provisioner account, make sure you have created the provisioning group to which the new provisioner will belong. If you do not have an appropriate provisioning group, see Creating a provisioning group on page 105.

Procedure

1. Run the Administrator Application (note that you cannot use Ignition Dashboard for this):
   - Open a browser and navigate to the Administrator Application URL.
   - Type your Guest Manager administrator `username` and `password`.
   - Guest Manager must be connected with the Ignition Server appliance. If it is not connected now, see Connecting Guest Manager to the Ignition Server Appliance on page 67.
2. Select **Provisioner** in the main toolbar. The Internal Provisioners screen appears.
3. Select **Actions** > **New Internal Provisioner**. The Create Provisioner screen appears.



4. Set the provisioner's account details:
   - **Username**, **First Name**, and **Last Name**: Fill in the appropriate information for the provisioner. Only numbers and characters are allowed in the name. No spaces or periods may be used. The length of the name must be 30 characters or less.
   - **Password** and **Confirm Password**: Set the provisioner's password in these two fields. Since Guest Manager encrypts the password, note your entry now for future reference.

Important:

Do not type single or double quotation marks in the password field. Doing so can cause the entered password to be clipped at the location of the first quotation mark.

- **Email**: Enter the email address of the provisioner.
- In **Comments**, enter any notes you wish to make. These comments are not sent to the provisioner.

5. In the **Member of Provisioning Group** check boxes, check the provisioning group(s) that this user belongs to.
6. Check your entries and click **Submit**. Guest Manager creates the provisioner.

   If at any time you wish to reset all fields to the state they were in when you opened the window, click the **Reset** button.
7. Notify the provisioner of his or her new provisioner username and password, and provide the URL of the provisioner application, which is

   `http://<Guest Manager machine>/GuestManager/provisioner/`

   OR

   `https://<Guest Manager machine>/GuestManager/provisioner/`

   If you want to view the provisioner account you saved, select **Provisioners**.

Creating a provisioner from an account in an LDAP or AD store

You have the option of allowing existing users in your LDAP or Active Directory store to act as provisioners. See Creating a Provisioner access policy on page 47 or Creating an Advanced Provisioner access policy on page 51 for instructions.

Bulk importing provisioner accounts from a file

Use these steps to create provisioner accounts for all the users listed in a file. Provisioners you create via this procedure are stored in the Ignition Server internal store.

If your provisioners exist in an LDAP or AD store, then you might not have to import them at all. Instead, you can set Guest Manager to authenticate these provisioners directly against LDAP or AD as shown in Creating a provisioner from an account in an LDAP or AD store on page 119.

Use these steps to bulk-import provisioner accounts:

Procedure

1. Save your provisioner data to a text file in comma-separated value (CSV) format.

   The format consists of one user per line:

   - *If you wish to import passwords*, then format each line as follows:

```
Username,FirstName,LastName,Email,Password
```

- *If you do not wish to import passwords*, then Guest Manager will generate a password for each user. Format each line as follows:

```
Username,FirstName,LastName,Email
```

Separate fields with a comma, and end each user line with a line break. Fields may not contain spaces. No space or tab character is permitted after the comma.

For example, a file containing the following lines would create three provisioners:

```
vdavis,Vernon,Davis,vdavis@niners.com
mrobinson,Michael,Robinson,mrobinson@niners.com
pharalson,Parys,Haralson,pharalson@niners.com
```

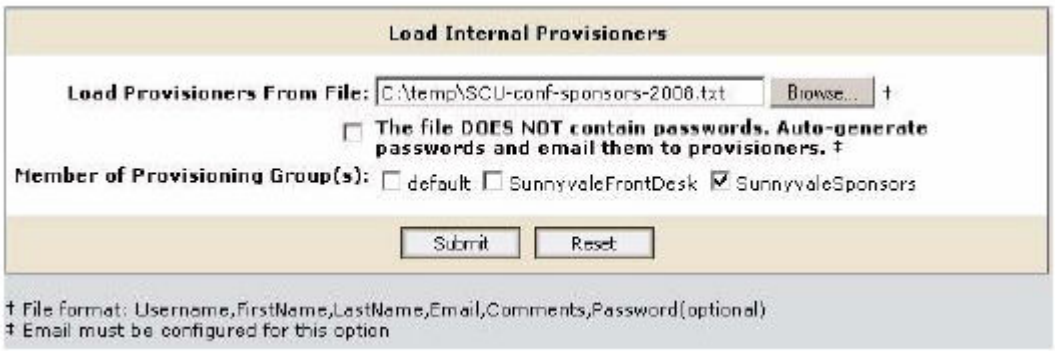
Important:

The maximum number of provisioners you can import from a file is 1000.

Important:

If possible, choose an off-peak time to bulk load provisioners. Bulk loading users during times of heavy authorization traffic can result in the failure to save some users from the CSV file.

2. Run the Guest Manager Administrator Application.
3. In the toolbar on the left, click **Provisioners**. The Internal Provisioners screen appears. Select **Actions** > **Load Internal Provisioners**. The Load Internal Provisioners screen appears.



4. To the right of the **Load Provisioners From File** field, click the **Browse** button and browse to find your CSV file. Click **Open**.
5. If you wish to import passwords from the file, clear the **File DOES NOT contain passwords** check box. With this check box selected, Guest Manager automatically chooses a password for each provisioner you import.
6. In the **Member of Provisioning Group(s)** section, select the check box(es) of the groups to which the imported provisioners will belong. Membership in a provisioning group establishes the provisioners' rights and settings.

7. Click **Submit**. Guest Manager displays a progress bar while it imports the users. Under some conditions, the bulk loading may take several minutes to complete.

   Once the provisioner accounts have been created, you may view them by clicking **Provisioners** in the command bar on the left of the window. To see a record of the success or failure of each account creation attempt, check your Guest Manager logs as explained in Viewing the log files on page 71.

Checklist: Before your provisioners start working

Before your provisioners can start working, you (as Guest Manager administrator) must ensure the following:

- **Provisioner accounts**: Each provisioner must have a *provisioner account* stored in Ignition Server or mapped via Ignition Server to your LDAP or AD store.
- **Access to the Guest Manager Provisioner Application**: Each provisioner must be able to connect to the Guest Manager Provisioner Application via his or her browser.
- **Connection to an Ignition Server appliance**: The Guest Manager application must remain connected to the Ignition Server in order to save and retrieve guest data.
- **Required configurations**: The Ignition Server must have the access type, access zone, and network rights configurations that form the set of assignable access constraints for guest users.
- **Notification settings**: Make sure you have configured Guest Manager to send email notifications to new guest users. See Setting up Email notification parameters on page 59. If desired, make sure you have configured Guest Manager to send SMS messages. See Setting up SMS notification parameters on page 61.

If you have created your guest authorization policies and set up your provisioner accounts, you should now train the provisioners to use the Guest Manager Provisioner Application. As the basis for this training, use Provisioner application: Managing guests and devices on page 134.

Writing SMS and Email templates for account notifications

Guest Manager allows you to edit the information sent in account notifications to new users. When a guest user is granted a temporary network account, he or she is notified by means of an email, an SMS message, or both. Usually, these messages contain the guest's account username and password. If you wish to edit the information that is sent in account notifications, you must do so through the SMS and email templates.

Use the **Notification** > **General** tab for messages sent to the guest user when a provisioner saves the guest user's account, or, if sponsor approval is required, when that request is pending sponsor approval.

Use the **Notification** > **Sponsor Action** tab for messages sent to the guest user when the sponsor approves or denies the user account request.

Before you begin

Make sure you have set up your email and/or SMS gateways as shown in Setting up Email notification parameters on page 59 and Setting up SMS notification parameters on page 61.

Procedure

1. Run the Administrator Application, and click on the **Provisioning Groups** section in the main toolbar.
2. From the **Provisioning Groups** list, click on the group whose template(s) you wish to edit.
3. Click the **Notification** > **General** or **Notification** > **Sponsor Action** tab in the Edit Provisioning Group screen. You will see the **SMS Template** and the **Email Template**. The text boxes to the right of these fields display the current account notification messages being sent to new users.
4. Edit the **SMS** and/or **Email Template**.
   - Note that in the SMS character field, the length of your message is counted in characters. The field counts the character length of the variables *$username* and *$password* literally, and cannot estimate how long their actual replacement values will be. So when editing this field, keep in mind that most carriers enforce a limit of 160 characters on SMS messages.
   - For emails, you can place and edit variables in both the **Subject** and the **Message**.
   - The comments (or variable, *$comment*) sent in this message reflect any information that the provisioner or the self-provisioning guest typed into the Comments field of the Create Guest User form. The variable *$access* is a summary of the Access Types, Network Rights, and Access Zones that have been granted to the user.
5. Click **Submit** to save your changes to the template(s). A message confirms your action.

Administrator access to the provisioner application

In order for you as the Guest Manager administrator to access the Provisioner Application (for example, if you want to create guest user accounts to test your policies), you must have a provisioner account for your own use.

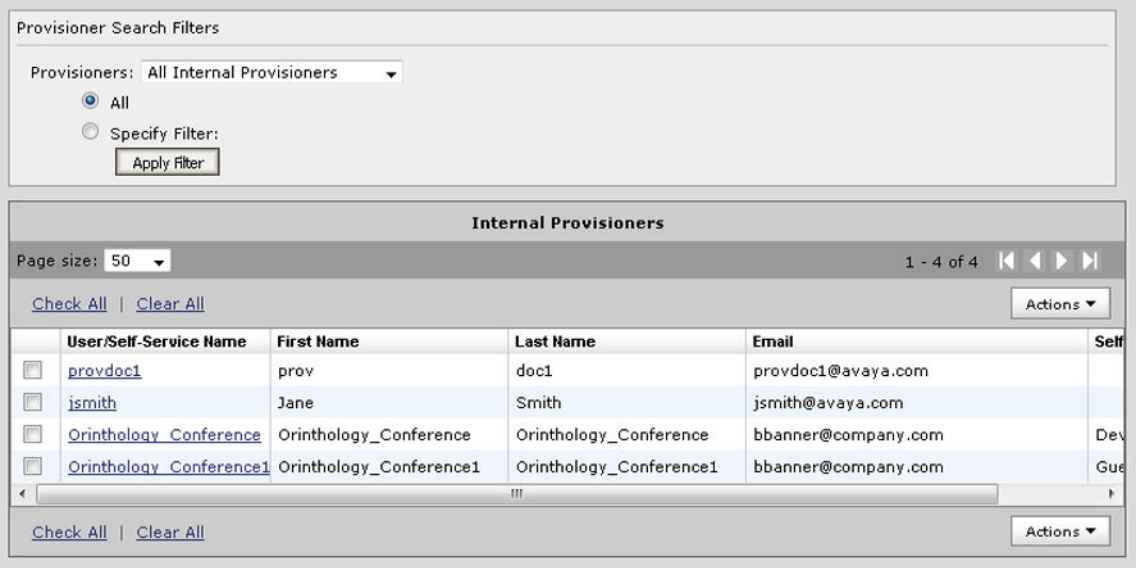
Managing provisioners

As the Guest Manager administrator, you can perform operations on provisioner accounts that are stored in the Ignition Server internal store.

Your site may also use provisioner accounts that are stored externally in your corporate LDAP or Active Directory store. You cannot edit these users in Guest Manager, but you can set up rules that place them in the appropriate provisioning groups. See Creating a Provisioner access policy on page 47.

Viewing the internal provisioners list

As the Guest Manager administrator, you manage internal provisioners using the **Provisioners** section in the main toolbar of the Administrator Application. Note that you can only edit *internal provisioners*. Provisioner accounts stored in LDAP or AD cannot be edited using Ignition Server tools.



The **Internal Provisioners** list contains the following:

- a check box to select the row containing the provisioner account data
- the **User/Self-Service Name**, which is the active link to the details of the provisioner's account
- the **First Name**, **Last Name**, and **Email** address of each provisioner. If the provisioner is a *self-provisioner*, the **Self-Service** column shows the Self-Service Type.

Use the **Check All** and **Clear All** command links to select or clear all the provisioners in the list.

The **Actions** drop-down menu allows you to carry out bulk actions that apply to all the provisioners whose check boxes you have selected:

- **Delete Provisioners** deletes the selected provisioner(s). See Deleting a provisioner account on page 125.
- **Delete Expired Guest Users** deletes all the expired guest accounts owned by the provisioner(s) you have selected. See Deleting expired guest users on page 132.
- **Export Guest Users** exports to a CSV-formatted file the account details of all the guest accounts owned by the provisioner(s) you have selected. See Exporting guest user records to a file on page 132.
- **Export Devices** exports to a CSV-formatted file the account details of the device accounts owned by the provisioner(s) you have selected. See Exporting device records to a file on page 133.

Modifying a provisioner account

Procedure

1. Click **Provisioners** in the main toolbar of the Administrator Application. The Internal Provisioners screen appears displaying the list of provisioners currently authorized to set up guest access (as shown in the previous section).
2. Locate the row containing the provisioner whose account you wish to modify.
3. Click on the entry in the **User/Self-Service Name** column.

   The Edit Provisioner screen appears. This screen contains the same fields as the Create Provisioner screen. See Creating a provisioner in the internal store on page 117 for an explanation of each field.
4. Edit the fields as desired. If you wish to change the provisioner's password, click the "change" link in the **Password** field.

   If at any time you wish to reset all fields to the state they were in when you opened the provisioner record, click the **Reset** button.
5. Click **Submit**.

   Guest Manager updates the provisioner account and displays a confirmation message.

Assigning a provisioner to a provisioning group

Follow this procedure to put a provisioner in one or more provisioning groups.

This procedure works only for *internal provisioners* stored in Ignition. If your provisioners are stored in LDAP or AD, turn instead to Creating a Provisioner access policy on page 47.

Procedure

1. Click **Provisioners** in the main toolbar of the Administrator Application. The Internal Provisioners screen appears displaying the list of provisioners.
2. Locate the provisioner account you wish to modify and click on its name in the **User/Self-Service Name** column.

   The Edit Provisioner screen appears
3. In the **Member of Provisioning Groups** section, select the check boxes of all the groups to which this provisioner belongs.
4. Click **Submit**.

Deleting a provisioner account

You can delete internal provisioner accounts. Each provisioner owns the guest users that he or she has created. Before you delete a provisioner, consider reassigning ownership of his or her guest users to another provisioner.

After you delete a provisioner, the system may still contain some guest users and device accounts that were owned by the deleted provisioner. Provisioners who are in the same provisioning group as the deleted provisioner can retrieve the deleted provisioner's users and accounts, provided that the provisioning group allows sharing.

Procedure

1. Click **Provisioners** in the main toolbar of the Administrator Application. The Internal Provisioners screen appears displaying the list of provisioners.
2. If the provisioner you plan to delete owns guest and device accounts and you wish to keep those accounts, then reassign them as explained in Reassigning a provisioner's guest user accounts and devices to another provisioner on page 128.
3. From the Internal Provisioners list, select the check box of the provisioner account(s) you wish to delete.
4. In the **Actions** menu, choose the **Delete Provisioners** command. In the confirmation dialog, click **OK**.

   Warning:

   When a provisioner is deleted, that provisioner's guests and devices may be assigned to a different provisioning group. When a guest user is reassigned to a different provisioning group and/or provisioner, the guest's group memberships are not forced to conform to the group membership limitations of the new provisioning group. In other words, if a guest user is created and has access, for example, to the Internet and the *HQ-corporate network*, and that guest is reassigned to a provisioning group whose power is limited to granting access to the Internet only, that guest will retain his rights to both the Internet and the *HQ-corporate network*, despite the new group's limitations. If a provisioner from the new group edits the guest user, then the new group's limits apply.

Changing a provisioner's password

You can change the password of an internal provisioner using the following steps:

Procedure

1. Click **Provisioners** in the main toolbar of the Administrator Application. The Internal Provisioners screen appears displaying the list of provisioners.
2. Click the **User/Self-Service Name** of the provisioner whose password you wish to change. The Edit Provisioner window appears.

3. In the **Password** field, select the **Change** link.
4. Type the new `password` in the **New Password** field.
5. Retype the `password` in the **Confirm Password** field.
6. Click **Submit**.

Setting the provisioner time-out period

See Provisioner Idle Timeout Threshold on page 70.

Monitoring provisioner and guest logins

The logs in Ignition Dashboard maintain a record of each provisioner login attempt and guest login attempt. These records are visible in the Ignition Server *access log*, which you can load as follows.

Procedure

1. Run Ignition Dashboard (see Launching Ignition Dashboard on page 154) and click **Monitor** to show the system monitoring view.
2. Click the IP address or name of your Ignition Server in the tree.
3. Click the **Log Viewer** tab.
4. Click the **Access** tab and scroll or use a filter to find the desired record. In the **Type** column, provisioners' login attempts bear the labels *GM Provisioner: Accepted or GM Provisioner: Rejected*. Guest user login attempts bear the labels *RADIUS Request Accepted and RADIUS Request Rejected*.
5. Click a record to inspect it. You can view a more detailed description of each access request by opening its **Access Record Details**. Click the **Access Record Details**... at the bottom of the window, or click a cell in the Log Message column. See *Avaya Identity Engines Ignition Server Administration*, NN47280-600 for more information.

   You can filter the set of records. See *Avaya Identity Engines Ignition Server Administration*, NN47280-600.

Managing provisioning groups

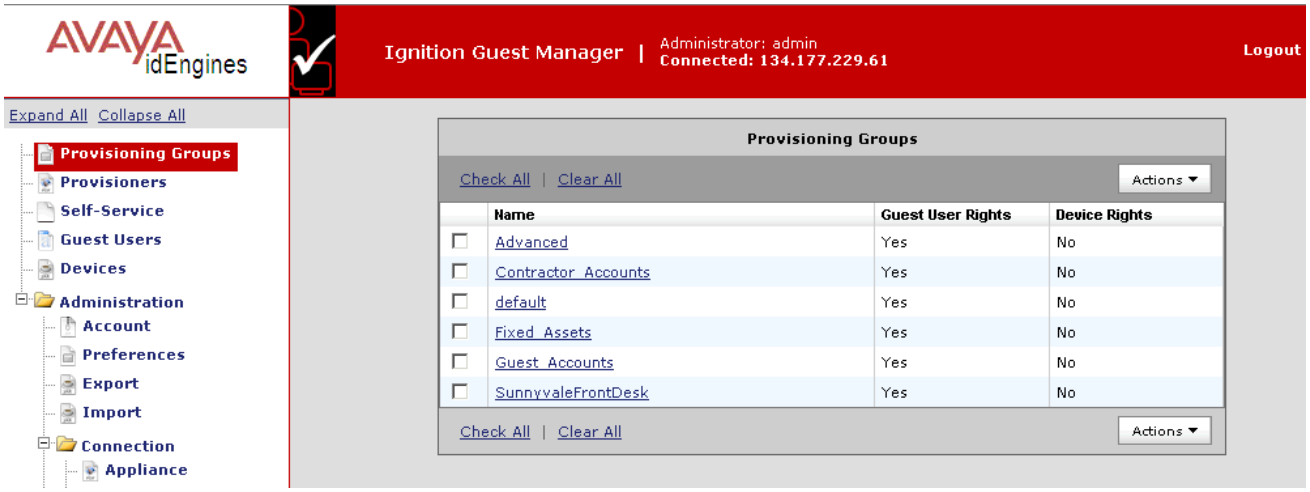
Provisioning groups are containers that collect internal users, guest users, and devices and allow these items to be managed by one or more provisioners in the provisioning group. In addition, each provisioner belongs to a provisioning group. The provisioner's membership in the provisioning group determines his or her provisioner rights and Guest Manager application settings.

The most common tasks are described in the following sections:

- Modifying a provisioning group on page 128
- Setting provisioner groups for provisioners stored in LDAP and AD on page 128

Managing provisioning groups

Provisioning groups determine the rights and application settings for your provisioners. To see the list of groups, click **Provisioning Groups** in the main toolbar of the Administrator Application.



Use the **Check All** and **Clear All** command links to select or de-select all the provisioners in the list.

Below the table, the **Actions** menu allows you to carry out bulk actions that apply to all the groups whose check boxes you have selected:

- **New Provisioning Group** creates a new provisioning group.
- **Reassign Provisioning Group Membership** invokes the Reassignment window to let you move the selected group's internal provisioners, users, and/or devices to a different provisioning group.
- **Delete Provisioning Group Members** lets you delete all the internal provisioners, guest users, and/or devices in the group you have selected. When you choose this command, Guest

Manager displays a dialogue window that allows you to choose which types of records to delete.

- **Delete Expired Guest Users** deletes all the expired guest accounts owned by the provisioner(s) you have selected. See Deleting expired guest users on page 132.
- **Delete Provisioning Groups** deletes the selected group(s).
- **Export Guest Users** exports to a CSV-formatted file the account details of all the guest accounts owned by the provisioning group(s) you have selected. See Exporting guest user records to a file on page 132.
- **Export Devices** exports to a CSV-formatted file the account details of all the devices owned by the provisioning group(s) you have selected.

Modifying a provisioning group

Procedure

1. Click **Provisioning Groups** in the main toolbar of the Administrator Application.
2. In the table, click the name of the provisioning group that you wish to modify.
3. In the Edit Provisioning Group window, make your edits and click **Submit**.

Setting provisioner groups for provisioners stored in LDAP and AD

If your provisioner accounts are stored in LDAP or Active Directory, you must set up rules to associate each provisioner account with a provisioning group. The provisioning group provides the provisioner's rules of operation. See this setup as shown in Creating a Provisioner access policy on page 47 or Creating an Advanced Provisioner access policy on page 51.

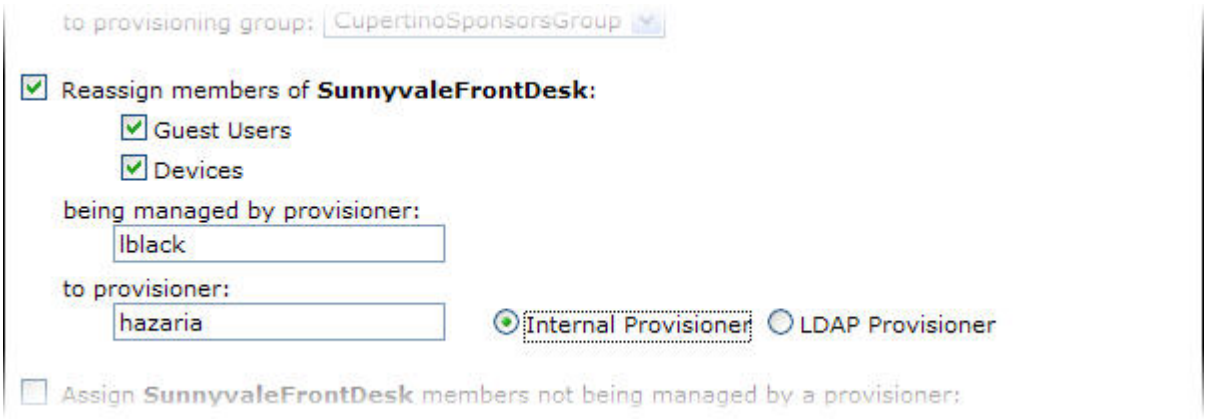
Managing group memberships

Reassigning a provisioner's guest user accounts and devices to another provisioner

Procedure

1. From the Guest Manager Administrator Application, click **Provisioning Groups** from the main toolbar.
2. Select the check box of the name of the provisioning group of the provisioner whose guests and/or devices you wish to reassign.

3. Click **Actions** > **Reassign Provisioning Group Membership**.
4. In the *middle part* of the window, check **Reassign members of**.
5. Check the **Guest Users** and/or **Devices** check boxes, as applicable.
6. In the **being managed by provisioner** field, type the name of the provisioner who currently owns the users or device records.

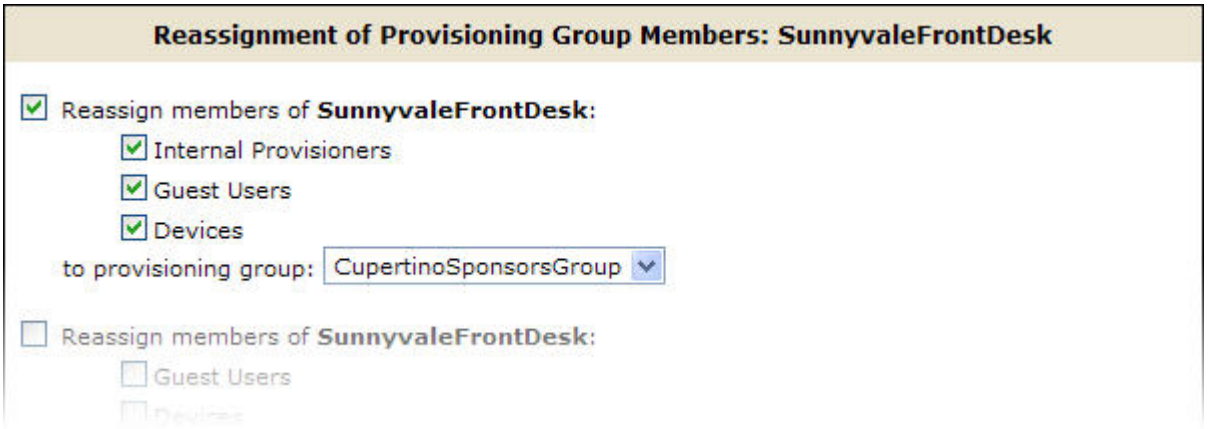


7. In the **to provisioner** field, type the name of the provisioner to whom you will assign the users or device records.
8. Click **Submit**.

Moving provisioners, guests, or devices to a new provisioning group

Procedure

1. From the Guest Manager Administrator Application, click **Provisioning Groups** on the main toolbar.
2. Select the check box of the name of the provisioning group whose provisioners, guests, or devices you wish to reassign.
3. Click **Actions** > **Reassign Provisioning Group Membership**.
4. In the *top part* of the window, check the check box, **Reassign members of**.

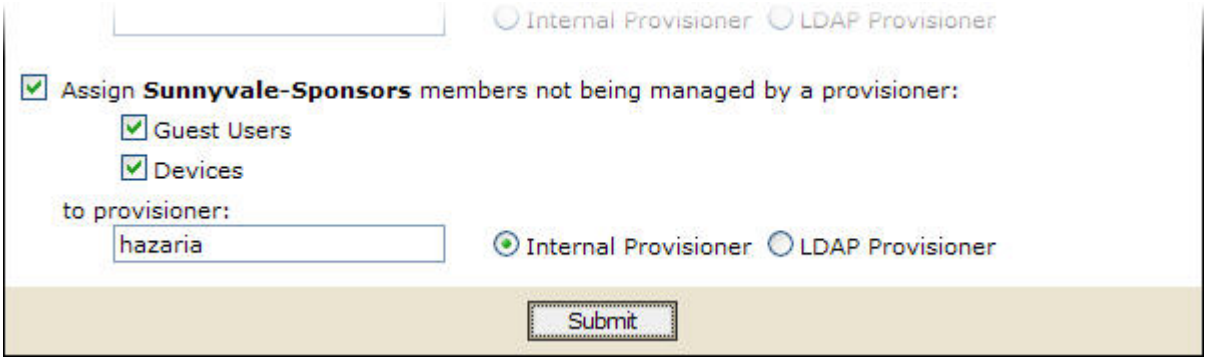


5. Check the **Internal Provisioners**, **Guest Users**, and/or **Devices** check boxes, as applicable.
6. In the **to provisioning group** drop-down list, choose the name of the provisioning group to which you will assign the provisioners, users, or device records.
7. Click **Submit**.

Assigning unmanaged guests or devices to a provisioner

Procedure

1. From the Guest Manager Administrator Application, click **Provisioning Groups** on the main toolbar.
2. Select the check box for the name of the provisioning group whose unmanaged guests or devices you wish to reassign. This is typically the provisioning group of a recently deleted provisioner who owned the guest accounts or device records.
3. Click **Actions** > **Reassign Provisioning Group Membership**.
4. In the *bottom part* of the window, check the check box, "**Assign <GROUP> members not being managed by a provisioner**" (where "<GROUP>" is the provisioning group name).
5. Check the **Guest Users** and/or **Devices** check boxes, as applicable.



6. In the **to provisioner** field, type the name of the provisioner to whom you will assign the guest users or device records.
7. Click **Submit**.

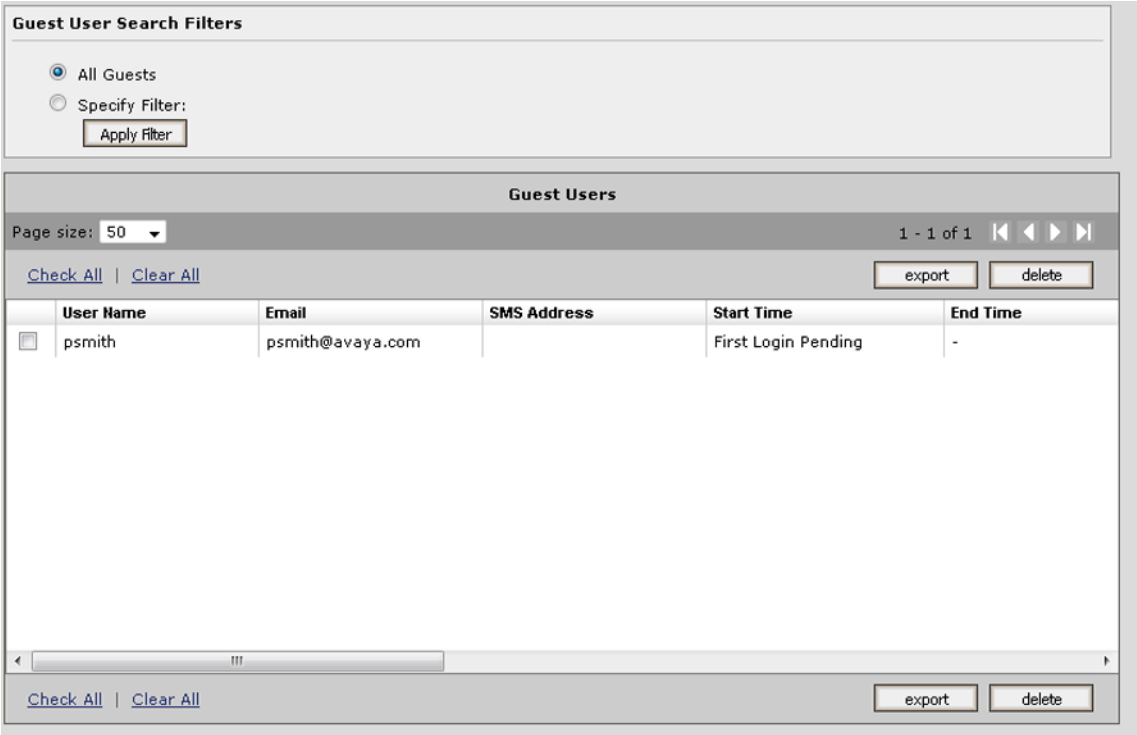
Bulk operations on guest users

Generally, provisioners are the people responsible for managing your guest users, but in some cases you (the administrator) may wish to carry out bulk operations on guest user accounts.

Retrieving the guest users owned by a provisioner

Procedure

1. From the Guest Manager Administrator Application, click **Guest Users** on the main toolbar. This shows all guest users provisioned in the system.



2. Select **Specify Filter** and select **Provisioner** from the drop-down menu.
3. Enter the operation (Start with, Equal, Not Equal, Contains, Ends With) and the name of the provisioner.
4. Click **Apply Filter**. A list of guest users provisioned by the selected Provisioner appears.

Retrieving the guest users that belong to a provisioning group

Procedure

1. From the Guest Manager Administrator Application, click **Guest Users** on the main toolbar. This shows all Guest users provisioned in the system.
2. Select **Specify Filter** and select **Provisioning Group** from the drop-down menu.
3. Select the provisioning group from the drop-down menu of provisioning groups.
4. Click **Apply Filter**. A list of guest users that belong to the selected provisioning group appears.

Deleting the guest users of a provisioner or provisioning group

Procedure

1. Load the users as explained in Retrieving the guest users owned by a provisioner on page 131 or as explained in Retrieving the guest users that belong to a provisioning group on page 132.
2. Select the check box of each user you want to delete.
3. Click **Delete**.

   The Guest Manager Log lists the users who were deleted.

Deleting expired guest users

Procedure

1. From the Guest Manager Administrator Application, click **Provisioners** on the main toolbar.
2. On the Internal Provisioners screen, select the check box(es) of the provisioner(s) whose expired guest users you wish to delete.
3. In the **Actions** menu, click **Delete Expired Guest Users**.

   The Guest Manager Log contains a list of the users who were deleted.

Exporting guest user records to a file

Procedure

1. From the Guest Manager Administrator Application, click **Provisioners** on the main toolbar.
2. On the Internal Provisioners screen, select **Export Guest Users** from the **Action** button.
3. Use your browser's **Save** interface to save the file.

Bulk operations on devices

Generally, device records are managed by provisioners, but in some cases you (the administrator) may wish to carry out bulk operations on these records. This section explains the most common bulk operations.

Retrieving the devices owned by a provisioner

Procedure

1. From the Guest Manager Administrator Application, click **Devices** from the main toolbar. This shows all devices provisioned in the system.
2. Select **Specify Filter** and select **Provisioner** from the drop-down menu.
3. Enter the operation (Start with, Equal, Not Equal, Contains, Ends With) and the name of the provisioner.
4. Click **Apply Filter**. A list of devices provisioned by the selected provisioner appears.

Retrieving the devices owned by a provisioning group

Procedure

1. From the Guest Manager Administrator Application, click **Devices** from the main toolbar. This shows all devices provisioned in the system.
2. Select **Specify Filter** and select **Provisioning Group** from the drop-down menu.
3. Select the provisioning group from the drop-down menu of provisioning groups.
4. Click **Apply Filter**. A list of devices owned by the selected provisioning group appears.

Exporting device records to a file

Procedure

1. From the Guest Manager Administrator Application, click **Provisioners** from the main toolbar.
2. On the Internal Provisioners screen, click the check box(es) of the provisioner(s) whose devices you wish to export.
3. Select **Export Devices** from **Action** button.
4. Use your browser's **Save** interface to save the file.

Chapter 10: Provisioner application: Managing guests and devices

As an Avaya Identity Engines Ignition Guest Manager provisioner, you create and manage guest user accounts. Your provisioner account is part of one or more provisioner groups that establish your rights, such as the maximum lifetime of accounts you create, and what network rights you can give those accounts.

This chapter shows provisioners how to create and manage guest user accounts and device records. You use the Guest Manager Provisioner Application to perform these actions.

Introduction to guest user accounts

A guest user is a visitor, or other temporary user, to whom you grant specific, limited rights to use your network. Guest user accounts expire automatically after a specified period of time. Creation of guest user accounts is done in the Guest Manager application by a provisioner. For a comparison of user types, see Types of accounts in your Ignition Server installation on page 18.

What limits you can set on a guest user account

Guest users are individuals needing network access at your facility. In Ignition, we refer to the creation of guest users as “guest user provisioning.” When you create a guest user account, you are determining how and when the user can use your network.

- You set the *duration of access* for the guest user. The account can be valid for only a few minutes or for a number of weeks. Later, if the account expires, you can renew it if needed.
- You establish the set of *allowed connection mechanisms* a guest can use: 802.1X-secured wired connection, 802.1X-secured wireless connection, web-authenticated wireless connection, and so on. These are called “access types” in Ignition.
- You determine *which network ports or access points* the user can connect to. That is, you specify which access points or conference room network jacks will allow the user to connect. These are called “access zones” in Ignition.
- You specify *which segments of your network the user* can reach once connected. For example, you might give a user Internet access only, or you might give him or her access to the corporate intranet. These are called “network rights” in Ignition.

Guest user account attributes

A guest user account is a temporary, automatically expiring network account with specific, limited rights to use the network. Create new accounts in the Create Guest User page of Guest Manager. The table below explains the attributes that define a guest user account. Note that the available access types, network rights, and access zones are customized for your site; your Ignition Server Administrator will have set up these fields in Ignition Dashboard.

Field	Description
Group Membership	The provisioning group of which this user is a member. You must choose the provisioning group before you begin creating a user, because the provisioning group limits what rights can be granted to the user.
First Name	First or given name of the guest user
Last Name	Family name of the guest user
User Name	Login name of the guest. Cannot contain spaces. User name entered should be unique. If the provisioning group is configured to auto-generate the user name, the User Name field is auto-filled after the provisioner enters the first and last names.
Password	The password for the guest user account. If the provisioning group is configured to auto-generate the password, the Password field does not appear.
Email	Email address of the guest user. When this account is created, you can instruct Guest Manager to send a notification to this or another address. (See **Send Notification** below.)
Cell Phone (digits only)	The cell phone number (digits only) of the guest user. This is the number to which Guest Manager will send account notification via SMS messaging. To the right of this field, select the user's wireless **Carrier**.
Delete on Expire	If **Yes** is selected, Guest Manager automatically deletes the guest account one week after it expires. If you wish to manually delete this guest account after it expires, select **No** here.
Comments	Use this section to add any notes or specific log-in instructions for the guest user. Important: The Guest Manager administrator must add the "$comment" variable to the Email Template of the provisioning group in order to allow this value to be sent to the guest user. See Writing SMS and Email templates for account notifications on page 121.
Guest Details	Use this section to add details about the guest user, such as company name.
Activate Account on	The date and time at which the guest user account becomes active. The value in these fields defaults to the current date and time on the Ignition Server appliance. **Date**: Enter the start date for activating guest user account. The date should be in yyyy/mm/dd format.

Table continues…

Field	Description
	Time: Enter the time in hours and minutes based on a 12-hour setting. The time should be in hh:mm format. **AM/PM**: Select AM for morning; PM for afternoon.
Activate on First Login	This displays as “Yes” when the Guest has been assigned the activate on first login. The Activate account information on an non-assigned guest is replaced by this information.
Duration	The duration of validity of this guest account. The account validity period starts at the Activate Account On time and lasts for the specified Duration. By default, the Guest Manager application sets the entry to 8 hours. Type the period as an integer and set the units by selecting minutes, hours, or days from the drop-down list. See Guest user account validity period on page 137 for more details.
Access Types	Each check box here represents a mechanism by which the guest user may connect to the network. Select the check box for each access type you wish to allow. For example, you might tick two check boxes, one to allow the user to connect over a secure wireless and one to allow her to connect over secure wired connections. The Guest Manager Administrator determines which Access Type check boxes are available to you. These check boxes are present only if your site uses Access Type constraints. The Ignition Server Administrator defines the access type constraints in Ignition Dashboard by creating internal groups of type “accessType.”
Network Rights	Each check box here represents a network realm to which this guest user has access, such as, for example, the Internet only or the southeast regional sales department VLAN. Select the radio button for the appropriate realm. You may choose only one. The Guest Manager Administrator determines which Network Rights check boxes are available to you. These check boxes are present only if your site uses Network Right constraints. The Ignition Server Administrator defines the network right constraints in Ignition Dashboard by creating internal groups of type “networkRight.”
Access Zones	Each check box here represents a physical location from which the guest user is permitted connect to the network. Each is typically the location of a switch or access point. Select the check box(es) for the appropriate access zone(s). You may tick more than one check box. The Guest Manager Administrator determines which Access Zones check boxes are available to you. These check boxes are present only if your site uses Access Zone constraints. The Ignition Server Administrator defines the access zone constraints in Ignition Dashboard by creating internal groups of type “accessZone.”

Table continues…

Field	Description
Associated Devices	To assign a laptop or other device to a user, so that the user can only log in using his own device, use the **Associated Devices: Add** button and assign the device to the user you are editing. This is possible only if the provisioning group allows device provisioning.
Send Notification	In this section, tick a check box for each address or number to which you wish to send an account notification. Guest Manager sends notifications via email or via SMS messaging. See Sending guest account notifications on page 142 for details.

Guest user account validity period

A user account you create in Guest Manager has an account start time and account end time that define its period of validity (times marked in red indicate an expired guest account). At the conclusion of the validity period, the account will remain on the system as an expired account that can be renewed or deleted.

If you wish for an expired guest account to be deleted automatically from the system, select Yes under the Delete on Expire option from the Create Guest User or Edit Guest User pages.

☐	afargnoli	sqjATkX0	afargnoli@idengines.com	2007/02/23 02:33 PM	2007/02/23 10:33 PM
☐	mhingis	Dccr0YW0	a@a.com	2007/03/07 12:07 PM	2007/03/15 01:07 PM
☐	mmcbride	q74k3x24	b@b.com	2007/03/07 12:08 PM	2007/03/07 08:08 PM

As the provisioner who owns the user account, you may edit the start and expiry dates at any time, such as, for example, when a user's account has expired and you wish to renew its validity. For information on managing account expiries see:

- Checking validity of guest user account on page 146
- Renewing a guest user account on page 147

How a guest user logs in

When guests have their temporary user name and password, they can connect in one of two ways:

1. **Standard login**: In most networks, the guest user plugs his or her laptop into the wired network or connects to an open wireless access point. The networking client (known as the "supplicant") on the user's laptop brings up a login dialog. The user types his or her credentials, clicks a button, and, in the typical configuration, is given a session on the appropriate VLAN or secure SSID/VLAN.
2. **Captive portal**: If you use a captive portal tool, the user plugs his laptop into the wired network, or connects to an open wireless access point and launches his browser. The captive portal intercepts the user's web traffic and displays a login page in the browser. The

user types his or her credentials, clicks a button, and, in the typical configuration, is given a session on the appropriate VLAN or secure SSID/VLAN.

Launching the provisioner application

Procedure

1. Open your web browser and type the URL of the Provisioner Application:

   http://<Guest Manager machine>/GuestManager/provisioner/

   OR

   https://<Guest Manager machine>/GuestManager/provisioner/

   where “Guest Manager machine” is the name of your Guest Manager server.

2. In the Login screen, enter your provisioner **Username** and **Password**. If you do not have a provisioner account, contact your Guest Manager Administrator.

3. Click **Logn**. If your login attempt succeeds, the following message appears:

   You have successfully signed in as <UserName>.

   Important:

   When using Guest Manager, *do not* use your browser’s Refresh command to update a page. Instead, click the appropriate command button on the left side of the window to reload the page. *Do not* open a link in a new tab at any time.

   If your login attempt fails see Problem: Provisioner cannot login on page 152.

Failed connection

If Guest Manager has not been connected to the Ignition Server, your login attempt will fail with the following message:

Application time-out

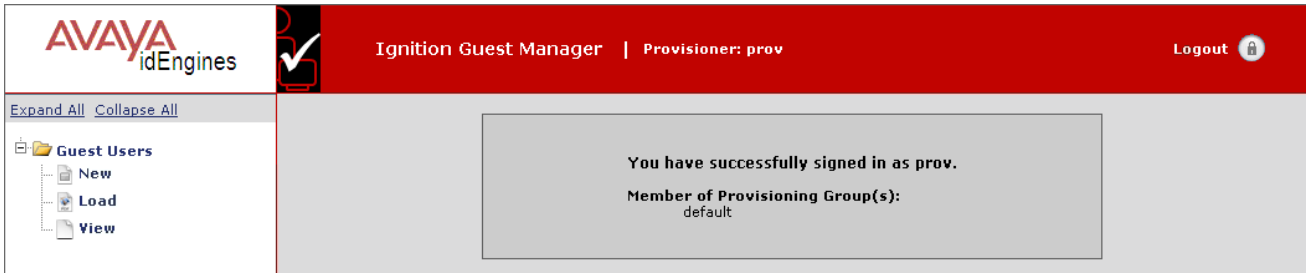
Your Provisioner Application session will disconnect if you leave it inactive for a period of time. The Guest Manager Administrator sets this timeout threshold. When you attempt to use the Provisioner Application after it has disconnected, it prompts you to log in again. Re-enter your username and password.

Warning:

Never allow the browser to remember your password.

Main page of the provisioner application

When you successfully log in to the Provisioner Application, Guest Manager displays the following page:



Managing guests

Creating guest user accounts

To create many accounts at once, use the **Load Guest Users** command, instead, as explained on Bulk importing guest user accounts from a file on page 141.

Use the steps below to create a guest user account.

Procedure

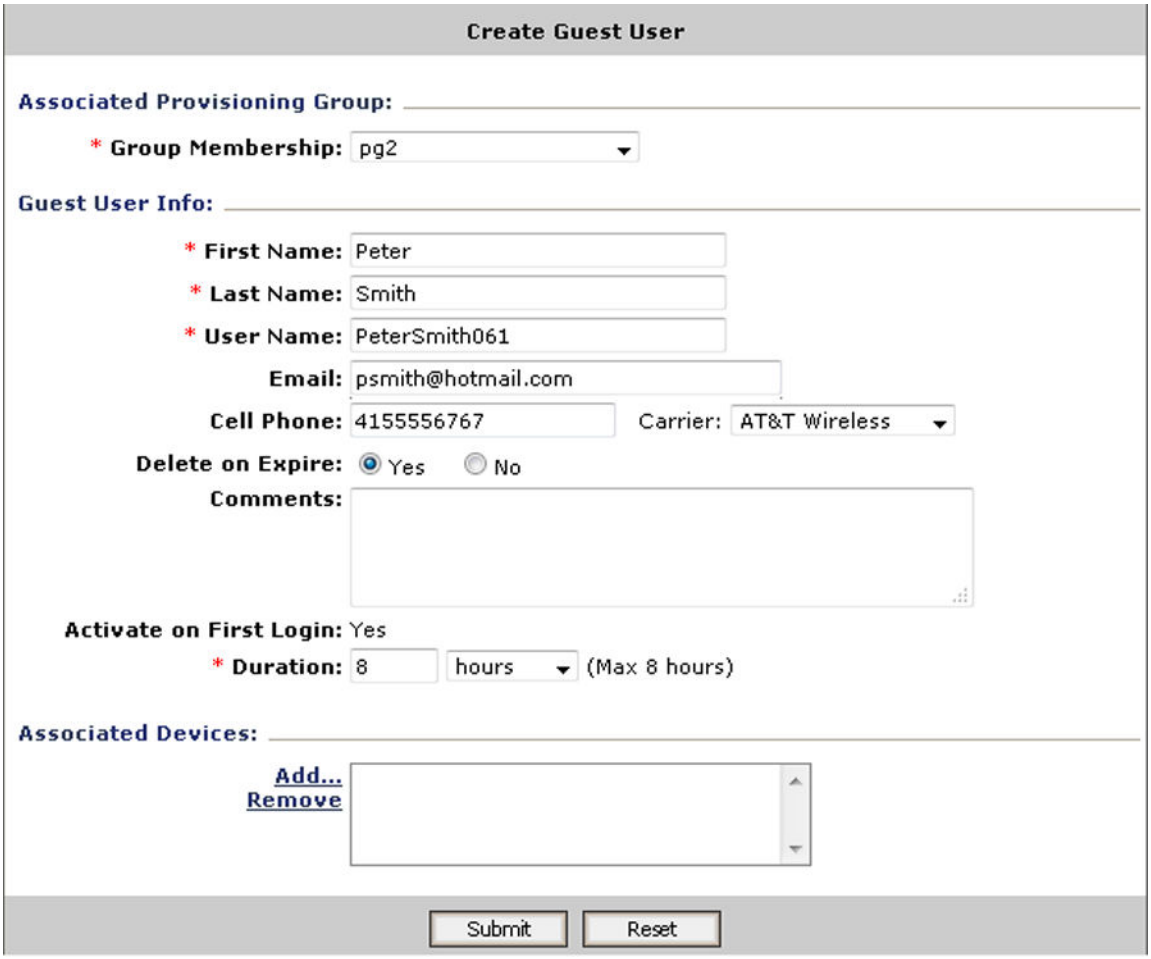
1. Log in to the Provisioner Application. See Launching the provisioner application on page 138.
2. Click **Guest Users** > **New** in the toolbar on the main page of the Provisioner Application.
3. In the Create Guest User screen, provide the account details. Do the following:
   a. In the **Group Membership** drop-down list, choose the provisioning group this guest will belong to.

      Each provisioning group imposes certain account guidelines (for example, auto-generation of the user name, auto-generation of the password, max. validity period, allowable access zones, and so on), according to how the administrator configured the guest user account details for this provisioning group. As a result, the fields and defaults of the window can change after you choose a provisioning group.

b. Enter the account details. See Guest user account attributes on page 135 for an explanation of the rest of the fields.

c. If you have login instructions for the user, type them in the **Comments** field. Later when you send the user a notification email, or print the user's login information sheet, the comments are included.

d. To reset the fields to their default values, click **Reset**.



4. Click **Submit**. The Guest Manager application creates the guest user account and sends email notifications to the people you specified in the Send Notifications section. See Sending guest account notifications on page 142 for details. Guest Manager displays the **Successful Guest Creation** page to confirm the account was saved.

5. You can print the user's account details. In the Successful Guest Creation page, click the Printer Friendly Version button. In the Guest User Account page that appears, click the **Print** button. To find out how the user will log in to your network, see How a guest user logs in on page 137.

   To view the guest user you created, click **Guest Users** > **View** from the main toolbar of the Provisioner Application.

Guest users you create belong to your provisioner account. Other provisioners cannot view or edit your guest users. The Guest Manager Administrator can view and delete your guest user accounts, but cannot edit them.

Bulk importing guest user accounts from a file

Use these steps to create guest accounts for all the users listed in a file.

Procedure

1. Save your user data to a text file in comma-separated value (CSV) format. The format consists of one user per line.
   - *If you wish to import passwords*, then format the file as follows:

     `Username,FirstName,LastName,Email,Comments,GuestDetails,Password`
   - *If you do not wish to import password*s, then Guest Manager will generate a password for each user. Format the file as follows:

     `Username,FirstName,LastName,Email,Comments,GuestDetails`

     Separate fields with a comma, and end each user line with a line break. Fields may not contain spaces. No space or tab character is permitted after the comma.

     For example, a file containing the following lines would create three guest users.

     `vdavis,Vernon,Davis,vdavis@niners.com,Welcome,Niners`

     `mrobinson,Michael,Robinson,mrobinson@niners.com,Welcome,Niners`

     `pharalson,Parys,Haralson,pharalson@niners.com,Welcome,Niners`

     Important:

     Observe the following guidelines when bulk loading guest users:

     - The maximum number of guest users you can import from a file is 1000.
     - Avaya recommends that each Provisioner own no more than 1000 guests and devices.
     - If possible, choose an off-peak time to bulk load guest users. Bulk loading users during times of heavy authorization traffic can result in the failure to save some users from the CSV file.
2. Run the Provisioner Application.
   - With the Guest Manager application running, open a web browser and navigate to the Provisioner Application URL.
   - Type your provisioner `Username` and `Password`.
3. In the toolbar on the left, click **Guest Users > Load**. The Load Guest Users screen appears.
4. In the **Group Membership** drop-down list, choose the provisioning group that will own the accounts.

5. To the right of the **Load Guest Users From File** field, click the **Browse** button and browse to find your CSV file. Click **Open** to select it.
6. To import passwords from the file, select the **Use Passwords Included in the Uploaded File** check box. *This check box is only visible if your provisioner account has the right to edit guest user passwords. Contact your Guest Manager Administrator if you need this right*.
7. In the **Activate Account On** field, enter the time when the accounts will become usable. Enter the date in the form, YYYY/MM/DD, and enter the time in the form, HH:MM:SS, and select AM for morning and PM for afternoon time.
8. In the **Duration** field, enter the length of time the accounts will remain valid. Use the drop-down list to set the units to minutes, hours, or days. The accounts' validity period starts at the **Activate Account On** time and lasts for the specified **Duration**. At the conclusion of the validity period, accounts remain on the system as expired accounts if the **Auto Expiry Deletion** option has not been selected. If the **Activate on First Login** has been assigned, the Activate Account is replaced by Activate on First Login "Yes" information.
9. Tick the appropriate **Send Notification** check boxes to send email with the new user names and passwords to your desired recipients:
   - Select **Guest User Email** to send each user his or her username and password. One email will be sent per guest user, and it will be sent to the guest's email address provided in the CSV file.
   - If you wish to send a notification email to an additional address, select the **Other Email** check box and provide an email address or a comma-separated list of email addresses. Send notifications only to people who you trust with the guest user password. One email will be sent to each address.
10. Click **Submit**. Guest Manager displays a progress bar while it imports the users. Under some conditions, the bulk loading of guest users may take several minutes to complete.

    Once the users have been created, click **Guest Users > View** to view the users. To see a record of the success or failure of each user creation attempt, check your Guest Manager logs as explained in Viewing the log files on page 71.

Sending guest account notifications

The check boxes in the **Send Notification** section of the Guest User pages allow you to instruct Guest Manager to send notification messages to the guest, the provisioner, and/or others to provide them with the new guest account details. Guest Manager sends the message automatically when you create or update a guest user account.

A notification email has the format of the email template configured in the provisioning group of which the guest user is a member. A notification SMS message has the format of the SMS Template configured in the provisioning group of which the guest user is a member.

These check boxes are present only if the Guest Manager Administrator has configured the application to send messages. For set-up instructions, see Setting up Email notification parameters on page 59 and Setting up SMS notification parameters on page 61.

Procedure

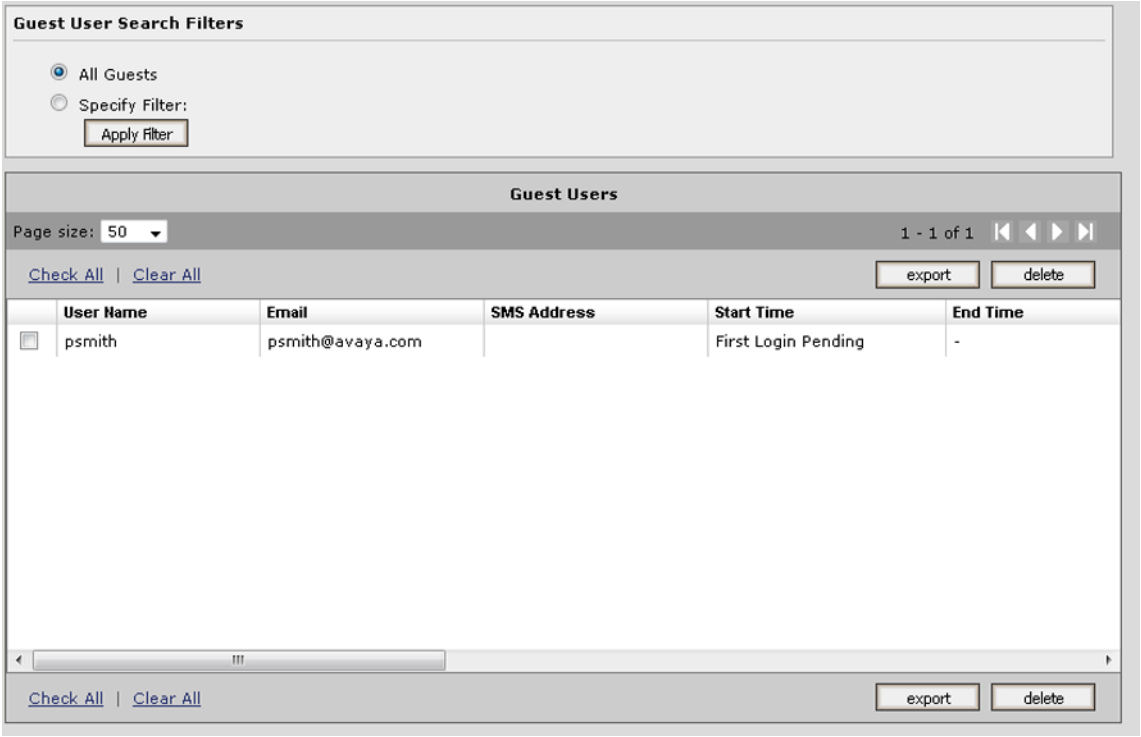
1. In the Edit Guest User or Create Guest User window, tick the appropriate check boxes in the **Send Notification** section of the page:
   - **Guest User Email** sends the guest an email with his account details. Only the fields specified in the guest's provisioning group's **Email template** are sent.
   - **Other Email** sends the guest's account details to the address you specify. Only the fields specified in the guest's provisioning group's **Email template** are sent.
   - **Password to guest user mobile phone** sends the guest an SMS message with his account details. Only the fields specified in the guest's provisioning group's **SMS template** are sent.
2. Click **Submit**. Guest Manager sends a notification to each person whose check box you selected.

   To set up your templates see, Writing SMS and Email templates for account notifications on page 121.

Viewing guest user accounts

As a provisioner of guest user access to your company's network, you manage the guest user accounts that you create using the **Guest Users > New/Load/View** buttons in the main toolbar of the Provisioner Application.

Each provisioner owns the guest user accounts that he or she creates; however, the Guest Manager Administrator can use the Administrator Application to view all guest users.



The **Guest Users** screen contains the following:

- a check box to select the row containing the guest user account data.
- the **Username** which you can click to edit the guest user account.
- the guest user's **Password**. The password is visible only if the Guest Manager Administrator has given you permission to view it.
- the guest user's **Email** and **SMS Address**
- the **Start Time** at which the account becomes usable. This text will be red if the account is not yet usable. Edit the guest account if you need to activate it sooner.
- the **End Time** at which the account becomes unusable. This text will be red if the account has expired. Edit the guest account if you need to reactivate it.
- the **Provisioning Group** and **Provisioner**
- the **Sponsor Name**, **Sponsor Email**, and **Sponsor Response**
- the **Guest Details**

To select or deselect all the user rows, use the **Check All** and **Clear All** links at the bottom of the list.

The **Delete** button deletes all guest user account(s) whose check box(es) are selected.

The **Export** button exports a csv file of the Guest User records that match the filter.

If your provisioner account manages a large number of guest user accounts, you may wish to adjust the viewing options of the Guest Users page. You can view your guest accounts in groups of 50,

100, 200, or 500. To do so, select the page size from the drop-down box, located at the top of the **Guest Users** list. The new page size takes effect as soon as you load a page of users. Click the buttons on the right of the box to navigate through multiple pages of guest accounts.

You may also click on any of the column headings (Username, Email, and so on) to choose how you wish to sort the list of guest accounts. For example, clicking on the **End Time** column can sort the guest accounts by either oldest end time or most recent end time.

Finding guest user account

Procedure

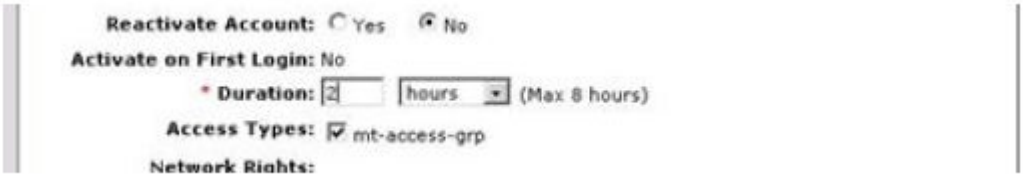
1. Click the **Guest Users > View** button in the main toolbar of the Provisioner Application. The Guest Users screen appears, displaying the list of guest user accounts currently authorized to gain guest access.
2. In the **Guest User Search Filters** section, in the **Provisioned By**, click the name of the provisioner or provisioning group that owns the guest account.
3. To add more filtering, click the **Specify Filter** radio button, choose a criterion type, a matching logic, and type a search criterion. Click **Apply Filter**.

   Matching records are loaded into the table. If you wish to restore the view to show all users, click **All Guests** and click **Apply Filter**.

Modifying guest user accounts

Procedure

1. Click **Guest Users > View** in the main toolbar of the Provisioner Application. The Guest Users screen appears, displaying the list of guest user accounts currently authorized to gain guest access.
2. Locate the row containing the guest user whose account you wish to modify.
3. Click on the entry in the **Username** column. The Edit Guest User screen appears.
4. Edit the fields as desired.
5. If you had previously configured a First Login account and it has expired you will find a **Reactivate Account** option appearing in this screen. Click **Yes** to reactivate the account.

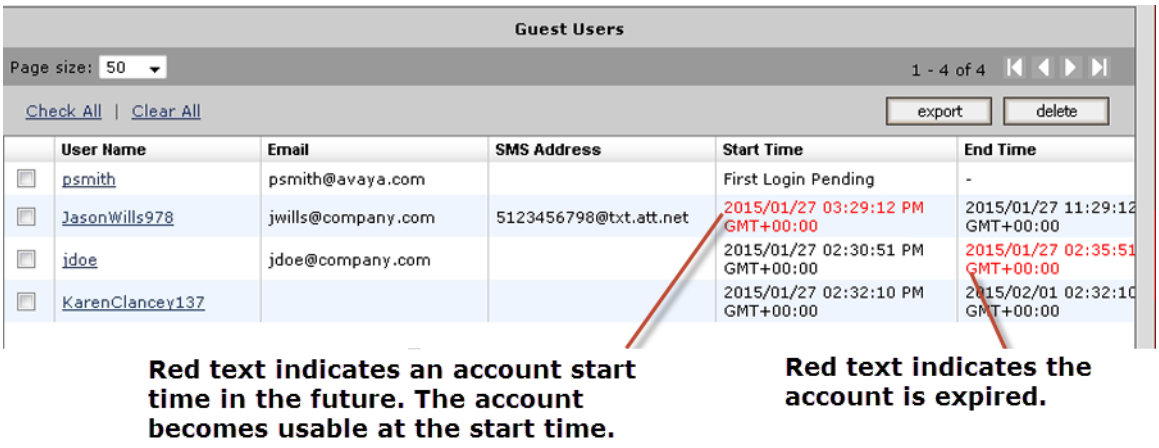


6. Click **Submit**. Guest Manager updates the guest user account and sends email notifications to the people that you specified in the **Send Notifications** section. See Sending guest account notifications on page 142 for details. Guest Manager displays the updated guest user account information in the Successful Guest Update page to confirm the account changes were saved.
7. You can print the user's account details. In the **Successful Guest Update** page, click the **Printer Friendly Version** button. In the **Guest User Account** page that appears, click the **Print** button.

Checking validity of guest user account

Procedure

1. Run the Provisioner Application.
2. Click **Guest Users > View** in the main toolbar on the left.
3. Find the user record you wish to check, and look at the **Start Time** and **End Time** columns. Red text indicates a not-yet-valid or expired account, as shown here:



4. If an account is currently not usable because its period of validity is in the future or past, you can make the account usable.
   - To make a not-yet-valid account usable now, open the user record and change the **Activate Account On** field to a time at or before the current time.
   - To renew an expired account, see Renewing a guest user account on page 147.

Printing guest user account details

To print an account summary of a guest user account, do the following:

Procedure

1. Click the **Guest Users > View** button in the main toolbar of the Provisioners Application.
2. In the Guest Users screen, locate the row containing the guest user whose account details you wish to print.
3. Click on the user's entry under the **Username** column. The Edit Guest User screen appears.
4. Click **Submit**. Guest Manager re-saves the account.
5. In the **Successful Guest Update** page, click the **Printer Friendly Version** button.
6. In the **Guest User Account** page, click the **Print** button.

Renewing a guest user account

Unless the Auto Expiry Deletion option has been set to Yes, expired accounts remain on the system after they have expired.

Procedure

1. Run the Provisioner Application.
2. Click **Guest Users > View** in the command bar on the left.
3. Open the user record you wish to renew.
4. Edit the **Duration** field, extending the period of validity, or edit the **Activate Account On** field to restart the period of validity at a desired time.
5. Click **Submit**.

Deleting guest user accounts

You can also delete the guest user accounts that you own.

Procedure

1. Click the **Guest Users > View** button in the main toolbar of the Provisioner Application. The Guest Users screen appears, displaying the list of guest user accounts currently authorized to gain guest access.
2. Locate the row or rows containing the guest user(s) whose account(s) you wish to delete, and select the check box for each user to be deleted.
3. Click the **Delete** button.

   Guest Manager deletes the selected guest user accounts.

Managing devices

Device management is only permitted if your provisioning group allows it.

Creating a device record

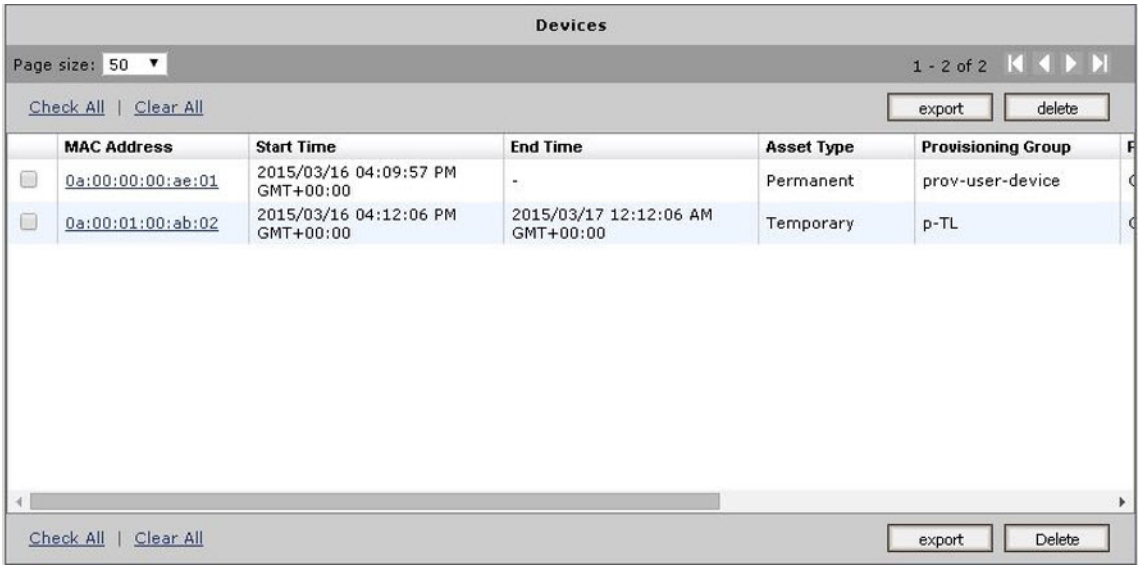
Ignition Server can enforce rules that allow a guest to connect only using his or her own device. See Device example on page 22 for details.

To create many device records at once, use the “Load Devices” command.

Procedure

1. Log in to the Provisioner Application.
2. Click the **Devices > New** button in the toolbar on the main page of the Provisioner Application.
3. In the **MAC Address** field, specify the MAC address of the device. Enter the address as a string of six octets. You may write the twelve characters without separators, or you may separate the octets with period, colon, or hyphen characters. Do not mix separator characters.
4. In the **Name** field, type a name for the device. This name identifies the device in logs and when you associate it with a group or user.
5. In the **Type** drop-down list, you may optionally designate what sort of device this is, such as a laptop, printer, or handheld device. You may choose one of the preset values or type your own value.
6. If you wish to disallow this device from connecting to the network, select the **Record Enabled: No** check box.
7. Specify whether this is a temporary device. Do one of the following:
   - To create a permanent record for the device, click **Permanent**.
   - To create a temporary record for the device, click **Temporary** and **specify the Activate Account On** date and the **Duration** of validity. If the Guest has been assigned to **Activate on First Login**, the Activate Account is replaced with a Yes for the first login. If the device record should be deleted when it expires, click the **Delete on Expire: Yes** button.
8. Specify where and how the device can be used by clicking the appropriate **Access Type**, **Network Rights**, and **Access Zone** check boxes.
9. To assign the device to a user, click the **Add** button in the Associated Users section.
10. Click **Submit**.

    The Guest Manager application creates the device record. To view the device record you created, click **Devices > View** from the main toolbar of the Provisioner Application.



Bulk importing device records from a file

Use these steps to create device records for all the devices listed in a file.

1. Save your device data to a text file in comma-separated value (CSV) format. The format consists of one device per line with the following field order:

   ```
   MAC Address,Name,Type,Attribute 1,Attribute 2,
   Attribute 3,Attribute 4,Attribute 5,Comments,
   VLAN Label,VLAN ID,Account Disabled
   ```

   where Account Disabled is either “yes” or “no”. (Default is “no”.)

   Separate fields with a comma, and end each record with a line break. Fields may not contain spaces. No space or tab character is permitted after the comma.

   Important:

   Observe the following guidelines when bulk loading:

   - The maximum number of device records you can import from a file is 1000.
   - Avaya recommends that each Provisioner own no more than 1000 guest and device records.
   - If possible, choose an off-peak time to perform the bulk loading. Bulk loading during times of heavy authorization traffic can result in the failure to save some records from the CSV file.

2. Run the Provisioner Application.
   - With the Guest Manager application running, open a web browser and navigate to the Provisioner Application URL.
   - Type your provisioners `Username` and `Password`.

3. In the toolbar on the left, click **Devices > Load**. The Load Devices screen appears.
4. In the **Group Membership** drop-down list, choose the provisioning group that will own the records.
5. To the right of the **Load Devices From File** field, click the **Browse** button and browse to find your CSV file. Click **Open** to select it.
6. In the **Source** field, you may type a name as a reminder of the information source you used for this bulk import.
7. If your file has a heading row, select the **Skip the first line** check box to instruct Guest Manager to ignore the first row.
8. Specify whether the device records will be temporary or permanent. Do one of the following:
   - To create permanent records for the devices, click **Permanent**.
   - To create temporary records for the devices, click **Temporary** and specify the **Activate Account On** date and the **Duration** of validity. If the Guest has been assigned to **Activate on First Login**, the Activate Account is replaced with a Yes for the first login. If the device record should be deleted when it expires, select **Yes** for the **Delete on Expire** field.
9. Specify where and how the device can be used by clicking the appropriate **Access Type**, **Network Rights**, and **Access Zone** check boxes.
10. Click **Submit**. Guest Manager displays a progress bar while it imports the records. Under some conditions, bulk loading may take several minutes.

Once the devices have been created, you may view them by clicking **Devices > View** in the main toolbar on the left of the window. To see a record of the success or failure of each record creation attempt, check your Guest Manager logs as explained in Viewing the log files on page 71.

Assigning a device to a guest user

Ignition Server can enforce rules that allow a guest to connect only using his or her own device. See Device example on page 22.

Procedure

1. Click the **Guest Users > View** button in the main toolbar of the Provisioner Application. The Guest Users screen appears, displaying the list of guest user accounts currently authorized to gain guest access.
2. Locate the row containing the guest user whose account you wish to modify, and click on the entry in the **User Name** column. The Edit Guest User screen appears.
3. In the Associated Devices section of the window, click **Add**. A list of devices appears.
4. Locate the user's laptop or device record in the list. If it is not there, see Creating a device record on page 148. Click the check box of the desired device and click **Add Devices to User**.

5. In the Edit Guest User screen, click **Submit**.

Chapter 11: Troubleshooting and FAQs

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

Trouble Ticket

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

Creating a trouble ticket

Procedure

1. From the Administrator Application, select **TroubleTicket** in the main toolbar.
2. On the Create Trouble Ticket screen, click **Create Ticket**.
3. Save the Guest Manager trouble ticket file to an appropriate location.
4. Contact technical support for instructions on how to upload the file to Avaya.

Problem: Provisioner cannot login

Possible cause: **Changed IP address**. If you are testing Guest Manager on a machine without a static IP address, then this problem crops up frequently.

To fix this: Check the Guest Manager entry in Ignition Dashboard to make sure it has the correct IP address and RADIUS shared secret of your Guest Manager host machine. Follow the steps in Making RADIUS Settings on the Ignition Server on page 58 and follow the steps in Making RADIUS settings in Guest Manager on page 59.

Possible cause: Wrong account type. Make sure the account you are using to log in is a *provisioner account*. You cannot connect to the Guest Manager Provisioner Application with a *Guest Manager administrator account*.

Problem: Connection to appliance fails

Connection to Appliance Fails When you restart the Guest Manager application, unless you have activated the Persist Connection to Appliance feature, you must reconnect Guest Manager to your Avaya Identity Engines Ignition Server appliance using the **Administration > Connection > Appliance** button of the Guest Manager Administrator Application. If your connection attempt fails, check the following and attempt to reconnect:

- Check that the Ignition Server is running correctly from Dashboard to verify that the appliance is running.
- Check Guest Manager's appliance connection settings: Click the **Administration > Connection > Appliance** button and check the settings for the desired appliance in the **Login to Appliance** screen.
- Check Ignition Dashboard's connection to the appliance: check whether the machine that hosts the Guest Manager appliance can ping the IP address of the SOAP port of the Avaya Identity Engines Ignition Server. If it cannot, check your network settings.
- Check to make sure the SOAP service is enabled on the appliance. Run Ignition Dashboard (see Launching Ignition Dashboard on page 154), connect to the appliance, click on **Configuration** tab, select the site, click on Services tab, click your node, and click the **SOAP** tab. See Making SOAP settings on the Ignition Server on page 55 for details.
- Check that the correct admin root certificate has been installed in Guest Manager. See Installing the SOAP certificate on page 53.

Problem: Errors reported during bulk saves and deletes

When using any bulk save, update, or delete command in (for example, the Load Guest Users command or the Delete Guest Users check box in the Administrator Application), the Guest Manager application may report the error: `java.net.SocketTimeoutException: Read timed out`. You may safely ignore this error.

This error is reported because Ignition Server's SOAP-MTL server time-out interval expired before the Ignition Server finished the save or delete operation. The Ignition Server saves or deletes the users as instructed. Wait until the Ignition Server finishes the operation, and reload your Guest User list to verify that the users were saved or deleted.

Problem: Virtual machine issues

Guest Manager URL is not accessible

1. Log in to the Guest Manager VM as admin.
2. From the CLI, enter `httpd restart`.

Guest Manager HTTPS is not using the custom certificate

If the Guest Manger HTTPS connection is not using the associated certificate and key after you uploaded the custom certificate and associated it with httpd, do the following:

1. Log in to the Guest Manager VM as admin.
2. From the CLI, enter `httpd restart`.

Guest Manager CLI

If you are not able to ping the Guest Manager VM after you assign the IP address and configure the route, do the following:

1. From the CLI, enter `reboot`.

Problem: Guest Manager Email Sending Failed

1. Make sure that the email notification is properly configured.

   Log in to the Guest Manager Administrator interface and go to **Notification>Email** and click **Submit**.

2. Log in to the Guest Manager virtual machine as admin.
   a. Enter `show dns` to check if the dns is configured. If dns is not configured, configure dns.
   b. Enter `reboot`.

Launching Ignition Dashboard

Some Ignition Guest Manager settings must be made in Ignition Dashboard, the standalone user interface application that manages your Ignition Server. Dashboard is a desktop application, not a web-based application.

Procedure

1. On the Windows PC where Ignition Dashboard is installed, double-click the Ignition Dashboard icon on the desktop or select the command **Start:Programs: Ignition Dashboard: Ignition Dashboard**. The login window appears.

2. Type the Ignition Server administrator **User Name** and **Password**. The default user name and password are `admin` and `admin`.
3. In the **Connect To** field, do one of the following:
   - To connect to an individual Ignition Server site, type the hostname or IP address of your Ignition Server.
   - To connect to a group of Ignition Server sites that you manage, choose the Site Group Name in the **Connect To** drop-down list.
4. Click **OK**. If you are unable to log in, see the section, “Problem: Cannot Connect to Ignition Dashboard” in the Avaya Identity Engines Ignition Server Administration Guide.

   If the administrator’s View Log Files fails to display log messages, make sure the path in log4j.properties is an absolute path. See the section, “Problem:Cannot connect to Ignition Dashboard” in the *Avaya Identity Engines Ignition Server Administration*, NN47280-600.