Avaya Identity Engines Ignition Guest Manager Configuration

Avaya Identity Engines Ignition Server
Release 8.0

Document Status: **Standard**
Document Number: **NN47280-501**
Document Version: **03.02**
Date: **April 2012**

© 2012 Avaya Inc.
All Rights Reserved.

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

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

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

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

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

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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

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

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

Contents

Purpose of this document

New in this release

Features 11
Exporting and Importing Guest Manager Configurations 11

Customer Service

Getting technical documentation 13
Getting product training 13
Getting help from a distributor or reseller 13
Getting technical support from the Avaya Web site 13

Preface

Using This Guide 15
Other Ignition Documents 15
Symbols and Typefaces 16

Introduction

Guest Manager Application in Context 17
Types of Accounts in Your Ignition Server Installation 17
The Guest Manager Administrator's Role 19
Provisioner's Role 19
Guest Users 20
Example Guest User 21
Example Device 21

Installing Guest Manager

System Requirements 23
Application Server Hardware 23
Browser Compatibility 23
Ignition Server Compatibility 23
Before You Install 23
Installation Instructions 24
Run the Installer 24
Set Up Tomcat to Require HTTPS Connections 25

Configuring Guest Manager

About Usernames and Passwords 29
Launch Tomcat 30
Launch Guest Manager 31
Create a Provisioner Access Policy 33
Create an Advanced Provisioner Access Policy 36
Install the SOAP Certificate 39
Make SOAP Settings on the Ignition Server 40
Make SOAP Settings in Guest Manager 42
Make RADIUS Settings on the Ignition Server 44
Make RADIUS Settings in Guest Manager 45
Test Guest Manager's RADIUS Connection Settings 45
Set Up E-Mail Notification Parameters 46
Set Up SMS Notification Parameters 47
Exporting and Importing Guest Manager Configurations 48
Exporting a Guest Manager Configuration 48
Importing a Guest Manager Configuration 49
Next Step 50

Managing Guest Manager

Running the Guest Manager Administrator Application 51
If You Act as Both Administrator and Provisioner 52
Restarting Guest Manager 52
Connecting Guest Manager to the Ignition Server Appliance 53
Disconnecting Guest Manager from the Ignition Server Appliance 53
Setting the Administrator Username and Password 54
Editing E-Mail Notification Settings 54
Editing SMS Notification Settings 55
Creating SMS Gateways 55
Deleting SMS Gateways 55
Configuring Timeout Settings 55
Provisioner Idle Timeout Threshold 55
Administrator Session Timeout Threshold 55
SOAP Client Timeout Threshold 56
Log Files 56
Viewing the Log Files 56
Default Location of the Log File 57
Changing the Default Location of the Log File 57

Setting Guest Authorization Policies

Contents 59
Dashboard Configuration Checklist 59

Setting Authorization Policies for Guest Users 60
Access Constraint Check Boxes on the Create Guest User Page 60
Authorization Policies 63
Mapping Internal User Groups to Virtual Groups 63
Sample Authorization Policies to be Used in This Chapter 63
Step-by-Step Configuration in Ignition Dashboard 65
Next Steps 83
Creating a Minimal Authorization Policy 83

Setting Up Self-Provisioning

Contents 85
Creating a Self-Provisioning Service 85
Deploying a Self-Provisioning Service 89
Managing Self-Provisioned Users 90
Deleting a Self-Provisioning Portal 91

Administrator Application: Managing Provisioners, Guests, and Devices

Contents of This Chapter 93
Setting Up Provisioners 95
Creating a Provisioning Group 95
Creating a Provisioner in the Internal Store 99
Creating a Provisioner From an Account in an LDAP or AD Store 102
Bulk Importing Provisioner Accounts from a File 102
Checklist: Before Your Provisioners Start Working 104
Writing SMS and E-mail Templates for Account Notifications 104
Administrator Access to the Provisioner Application 105
Managing Provisioners 105
Viewing the Internal Provisioners List 106
Modifying a Provisioner Account 107
Assigning a Provisioner to a Provisioning Group 108
Deleting a Provisioner Account 108
Changing a Provisioner's Password 109
Setting the Provisioner Timeout Period 109
Monitoring Provisioner and Guest Logins 109
Managing Provisioning Groups 110
Creating a Provisioning Group 110
Managing Provisioning Groups 110
Modifying a Provisioning Group 112
Setting Provisioner Groups for Provisioners Stored in LDAP and AD 112
Managing Group Memberships 112
Reassigning a Provisioner's Guest User Accounts and Devices to Another Provisioner 112
Moving Provisioners, Guests, or Devices to a New Provisioning Group 112
Assigning Unmanaged Guests or Devices to a Provisioner 113

Bulk Operations on Guest Users 114
Retrieving the Guest Users Owned by a Provisioner 114
Retrieving the Guest Users That Belong to a Provisioning Group 115
Deleting the Guest Users of a Provisioner or Provisioning Group 115
Deleting Expired Guest Users 115
Exporting Guest User Records to a File 116
Bulk Operations on Devices 116
Retrieving the Devices Owned by a Provisioner 116
Retrieving the Devices Owned by a Provisioning Group 116
Exporting Device Records to a File 117

Provisioner Application: Managing Guests and Devices

Contents of this Chapter 119
Introduction to Guest User Accounts 120
What Limits You Can Set on a Guest User Account 120
Guest User Account Attributes 120
Guest User Account Validity Period 122
How a Guest User Logs In 123
Launching the Provisioner Application 123
Failed Connection 124
Application Timeout 124
Main Page of the Provisioner Application 124
Managing Guests 124
Creating Guest User Accounts 125
Bulk Importing Guest User Accounts from a File 126
Sending Guest Account Notifications 129
Viewing Guest User Accounts 129
Finding Guest User Accounts 131
Modifying Guest User Accounts 131
Checking the Validity of Guest User Accounts 133
Printing Guest User Account Details 133
Renewing a Guest User Account 134
Deleting Guest User Accounts 134
Managing Devices 134
Creating a Device Record 134
Bulk Importing Device Records from a File 135
Assigning a Device to a Guest User 137

Troubleshooting and FAQs

Contents of this Chapter 139
Problem: Provisioner Can’t Log In 139
Problem: Connection to Appliance Fails 139
Problem: Installer Gives Errors and Warnings 140

Problem: Not Sure Whether Tomcat is Running 140
Problem: Errors Reported During Bulk Saves and Deletes 141
Problem: No Log File Displayed 141
Launching Ignition Dashboard 142

Index 143

Purpose of this document

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
- Set up 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

New in this release

The following section details what is new in *Avaya Identity Engines Ignition Guest Manager Configuration* (NN47280-501).

Features

Exporting and Importing Guest Manager Configurations

Release 8.0.0 introduces a new Guest Manager enhancement that allows you to export and import Guest Manager Configurations. This feature enables you to port Guest Manager configurations between multiple Guest Manager deployments.

The configurations you can export and import include:

- Appliance configurations
- RADIUS configurations
- User certificates
- Tomcat configurations (HTTP, SSL etc.)
- User preferences

For more information about exporting and importing Guest Manager configurations, see "Exporting and Importing Guest Manager Configurations" on page 48.

Customer Service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Preface

Avaya Identity Engines Ignition Guest Manager is a guest user provisioning application that makes it easy for front desk personnel to create and manage network logins for temporary users, such as contractors, visiting colleagues, partners, vendors, and customers. You may create as many different classes of guest users as required by your organization's network security policy, with each class of user receiving the degree of access specified by their specific policy. For example, you may specify that non-employee guests receive only Internet access while visiting employees from your branch offices are assigned to their proper VLAN on the internal network.

Using This Guide

Use this guide as an aid to perform these tasks:

- Install Guest Manager
- Set up 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.

Other Ignition Documents

The following Avaya Identity Engines Ignition Server documents also ship with your Ignition Server and are available from the Ignition Server support online, at **http://www.avaya.com/support**

- The *Avaya Identity Engines Ignition Server Administration* guide provides comprehensive documentation of the Avaya Identity Engines Ignition Server appliance and the Ignition Dashboard management application.
- The *Avaya Identity Engines Ignition Server Getting Started* guide shows you how to get Ignition running and how to connect Ignition to your switches, access points, and user data stores.
- The *Avaya Identity Engines Ignition CASE Administration* guide explains how to install, configure, and deploy Avaya Identity Engines Ignition Client for Accessing Secure Enterprise (CASE).

- The *Avaya Identity Engines Ignition Access Portal Administration* guide explains how to install and configure the Avaya Identity Engines Ignition Access Portal.

Symbols and Typefaces

This book uses the following visual cues to alert you when the text covers an important or easily overlooked issue:

Symbol	Meaning
‡	A selection or step within a menu, such as **File → Open** or **Edit → Paste**.
← ↑ → ↓ ✓ ✕	The buttons on the front panel of the Ignition Server.
Italic type	Italics signify new or important terminology and variable input for commands.
Bold type	Boldface signifies a command you click or an option you select.
	**Tip.** Indicates a shortcut or a resolution to a common problem.
	**Note.** Indicates background information or a reference to other sources of information.
	**Warning.** Indicates a situation where an error could cause data loss or a security breach.
	**Danger.** Indicates a situation where an error could cause bodily injury or equipment damage. Follow instructions carefully.
	**Danger.** Hazardous voltages are present. To reduce the risk of electric shock, follow the instructions.
	**Danger.** Hot surface. Avoid contact.

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 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 AutoConnect, client-side software to help users configure their laptops to connect via 802.1X.
- *optionally*: Avaya Identity Engines Ignition Server Portal, web-based authentication 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. In other words, 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. We will talk about the following types of users in this manual:

- 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 will act 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 54.

- The *Tomcat Administrator* runs the Apache Tomcat server that hosts the Guest Manager application. Make sure this administrator has a secure password, as noted in the “Run the Installer” on page 24.
- The *SOAP API user credentials* allow Guest Manager to connect to the Ignition Server. See “Make SOAP Settings on the Ignition Server” on page 40.
- 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. Provisioners are frequently called *sponsors* because they sponsor, or take responsibility for, the guest whose account they create. For example, if you want to give your company’s receptionist the ability to hand out temporary passwords for wireless access, you will 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 may store provisioners in both places at once.

  - To create provisioner accounts in the Ignition Server internal store, see “Creating a Provisioner in the Internal Store” on page 99. 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 102.
- 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 thereafter owned by the portal provisioner who owns the portal where the guest account was created. See “Creating a Self-Provisioning Service” on page 85.
- 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 119.

- A *user* is any user that Ignition Server can authenticate. The account for such a user may 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 laptop 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 134.

When you log into Guest Manager, you must log in either as the Guest Manager administrator or as a provisioner. The set of 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.



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

The Guest Manager Administrator’s Role

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

The Guest Manager administrator account:

- 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 may delete expired guest user accounts and may export guest user accounts to file.

Provisioner’s Role

Provisioner users manage guest users. Each provisioner employs the Guest Manager application to create/modify/delete guest users. The provisioner owns the guest users that he or she creates.

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



Provisioner accounts should be managed and deleted 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 will be 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.

Example Guest User

Figure 1 Example Guest User Provisioning Form

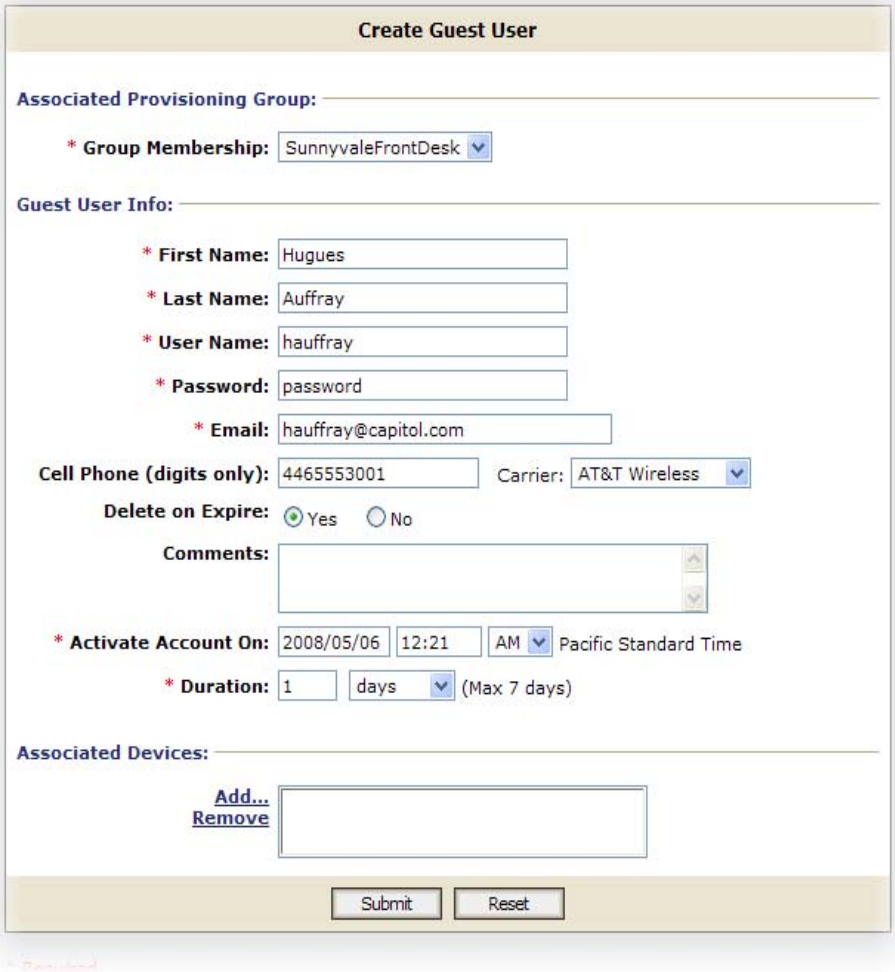


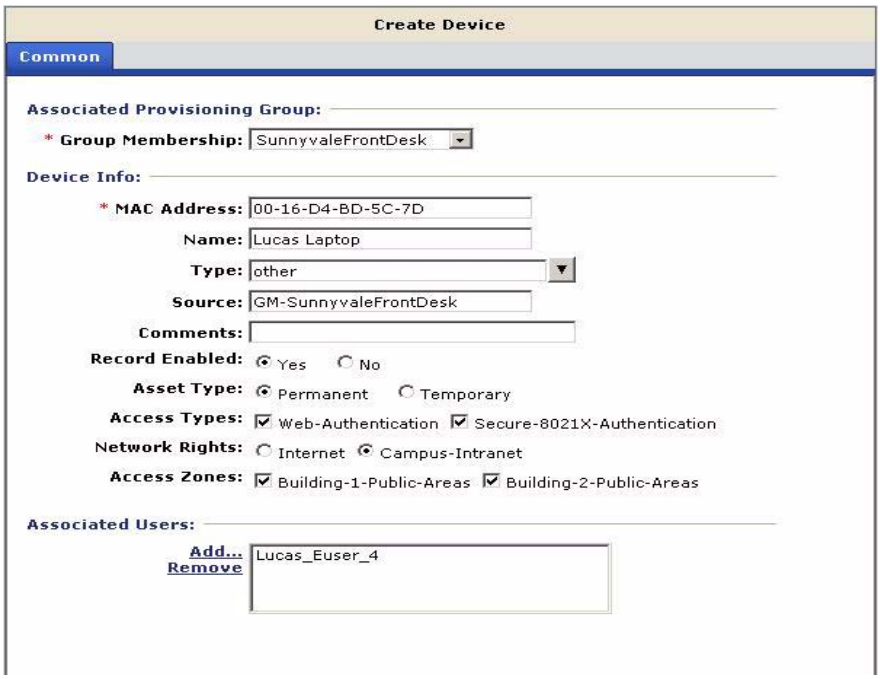
Figure 1 shows an example of a guest user provisioning form that is ready to be submitted in order to provide guest access for Hugues Auffray. His account is valid for 1 day starting on the **Activate Account On** date, and his provisioner has selected to turn on **Delete on Expire**. Both the guest and the provisioner for the guest account will receive electronic confirmation of the creation of this account.

Example Device

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 device creation window looks like this:

Figure 2 Example: Creating a device record



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 set them up in Ignition Dashboard. For instructions, read the section “Requiring the User to Connect Using His or Her Assigned Device” in the Asset Correlation chapter of the *Avaya Identity Engines Ignition Server Administration Guide*.

You can create device records individually (see “Creating a Device Record” on page 134) or in bulk (see “Bulk Importing Device Records from a File” on page 135).

Installing Guest Manager

This chapter shows you how to install Avaya Identity Engines Ignition Guest Manager, (and if needed) its required components, Apache Tomcat, and the Sun Java Runtime Environment (JRE). Guest Manager will be installed in your Apache Tomcat installation, in the `webapps` directory.

System Requirements

Application Server Hardware

The application server machine that hosts Guest Manager must meet these minimum hardware requirements:

- Pentium 4, 2.4 GHz or equivalent
- a minimum of 2 GB of RAM

Browser Compatibility

Guest Manager is compatible with the following web browsers:

- Microsoft Internet Explorer, version 6.0 or later, running on Windows.
- Firefox 1.5 or later, running on Windows.

Ignition Server Compatibility

Guest Manager 8.0.0 is compatible with version 8.0.0 of the Ignition Server appliance.

Before You Install

To install Guest Manager, you need:

- A PC running Microsoft Windows XP Service Pack 3 (32 bit) or Windows Server 2003™ (32 bit and 64 bit) or Windows Server 2008™ (32 bit and 64 bit). You will install Guest Manager and its supporting Apache Tomcat server on this PC.
- A running Ignition Server appliance, reachable on the network from the PC where you will run Guest Manager. The SOAP interface must be enabled on the Ignition Server.
- Administration rights with Windows Vista and Windows 7 UAC enabled. The Guest Manager must be installed by Administrator of the machine.

- An installation of the Ignition Dashboard management application on a PC. Make sure you also have a copy of the *Ignition Administration Guide*.
- The Guest Manager product CD, which contains installers for:
  - Java™ 2 Platform Standard Edition Runtime Environment (JRE) 6,
  - Apache Tomcat 6.0
  - Ignition Guest Manager
- Note that Guest Manager 8.0.0 also installs/upgrades the Apache Tomcat Web server 6.0.29 as well as the JRE release 6 update 27.
- If you are installing the 8.0.0 Guest Manager over an existing Guest Manager version or installing on a system where another instance of Tomcat web server is running, note that the GM 8.0.0 would install a new instance of Tomcat web server 6.0.29
  - To avoid any conflicts while running multiple instances of web server on the same system, select a different port number when installing the Tomcat web server.

Installation Instructions

This section explains how to install Guest Manager.

Run the Installer

Follow these steps to install Guest Manager:

1. On the Windows PC that will host Guest Manager, insert the Guest Manager product CD and run the file named **GuestManagerInstaller-8.0.0<Build Number>.exe**.
2. The License Agreement screen appears. Scroll down to review the entire license agreement. Select the radio button indicating you accept the license agreement, and click **Next**.
3. In the Choose Install Folder screen, specify the directory in which Guest Manager will be installed, and click **Next**.
4. Review the information on the Pre-Installation Summary screen and click **Install**. A Pre install confirmation window appears stating “Confirm Installation. The following tools are necessary for Avaya Guest Manager 8.0 Java JRE 1.6.0_27 and Apache Tomcat 6.0. These will be selected for installation.”
5. In the Pre install confirmation window, click **OK** to confirm the installation of Java JRE and Apache Tomcat.
6. The **Installing** window appears. If you have the correct version of JRE, a notification appears indicating that JRE is already installed and that the installer will skip the JRE installation. Click **OK** to continue.

7. *If Apache Tomcat is not found on your computer*, the installer displays the **Tomcat Installation** window. If this window appears:
   - Click **OK** to install Tomcat.
   - The installer may ask whether you wish to overwrite the file "GuestManager_config.txt". If you wish to retain this computer's old installation of Guest Manager, click **No** and abort your Guest Manager installation now. To continue the installation, click **Yes**.
   - In the **Choose Components** window, accept the defaults.
   - In the **Choose Install Location** window, use the default or choose your own location.
   - In the **Configuration** window, specify your Tomcat port number, specify a Tomcat administrator account name, and *specify a password that is unlikely to be guessed*. Make a note of your account name and password.
   - In the **Java Virtual Machine** window, accept the default JRE path.
   - In the **Completing the Apache Tomcat Setup Wizard** window, tick **Run Apache Tomcat** and untick **Show Readme**, and click **Next**.
8. *If your computer contained an earlier version of Guest Manager*, a notification window appears stating, "The installer has found existing configuration files. Do you wish to keep the existing configuration files?" Do one of the following:
   - If you use *your own certificate* to secure communication between Guest Manager and the Ignition Server, click **Yes**. Make sure that you have bound the corresponding certificates as the SOAP certificate on your Ignition Server. See "Install the SOAP Certificate" on page 39 for more information about certificates.
   - If you use the Identity Engines *default certificate*, click **No** to replace it.
9. The Install Complete screen appears with a "Congratulations" message and states that the Guest Manager installer has increased Tomcat's memory allocation limit. Click **Done** to quit the installer. The installation of Tomcat, Java, and Guest Manager is now complete.

Next Step: Set Up Tomcat to Require HTTPS Connections as explained below.

Set Up Tomcat to Require HTTPS Connections

Avaya recommends that you set your Tomcat server to require HTTPS browser connections for all users of the Guest Manager Administrator Application and Provisioner Application. This section explains how to do this.

To set Tomcat to require HTTPS connections, perform the steps below. (For more detailed instructions, see the “SSL Configuration HOWTO” in the Tomcat 5 documentation bundle.)

1. Open Tomcat’s `server.xml` file in a text editor. By default, it should reside in the install directory for Tomcat (`<tomcat_install>\conf\server.xml`).
2. Locate the block of settings associated with port 8443. This is the https configuration block — the second connector entry in the `server.xml` file, which starts with the text `Connector port="8443"`. The block of code looks like this:

```
<!--
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
           maxThreads="150" scheme="https" secure="true"
           clientAuth="false" sslProtocol="TLS" />
-->
```

3. Remove the HTML comment tags around the https configuration block in the `server.xml` file. (i.e. Remove the **<!--** at the beginning and remove the **-->** at the end.) When you remove the comment tags you have the following block:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
           maxThreads="150" scheme="https" secure="true"
           clientAuth="false" sslProtocol="TLS" />
```

4. In the “Connector” block, add the “keystoreFile” parameter to specify the location of your keystore. You may use the default keystore shipped with Guest Manager or you may use your own keystore. In a typical Guest Manager installation on Windows, the default keystore is saved as `C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\GuestManager\WEB-INF\ksTomcat`. To use the default keystore, add the following line to the Connector block:

   ```
   keystoreFile="webapps/GuestManager/WEB-INF/ksTomcat"
   ```

   (**Note!** Do not confuse the HTTPS keystore with the keystore that secures the Guest Manager-to-Ignition Server connection.)

After you make the addition, the https configuration block in `server.xml` reads:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
           maxThreads="150" scheme="https" secure="true"
           keystoreFile="webapps/GuestManager/WEB-INF/ksTomcat"
           clientAuth="false" sslProtocol="TLS" />
```

5. Comment out the “Connector” block for port 8080. This prevents users from loading Guest Manager over a cleartext connection.
6. Close and save the `server.xml` file, and restart Tomcat.

Now that you have set up your Tomcat server to require SSL, the default URL for Guest Manager will take the form (assuming an example host name of *pluto*): **https://pluto:8443/GuestManager/admin** instead of the non-SSL URL (**http://pluto:8080/GuestManager/admin**).

Next Step: Next, connect Guest Manager to the Ignition appliance as explained in Chapter , “Configuring Guest Manager”.

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.

This chapter contains the following sections:

- "About Usernames and Passwords", below.
- "Launch Tomcat" on page 30
- "Launch Guest Manager" on page 31
- "Create a Provisioner Access Policy" on page 33 (or "Create an Advanced Provisioner Access Policy" on page 36)
- "Install the SOAP Certificate" on page 39
- "Make SOAP Settings on the Ignition Server" on page 40
- "Make SOAP Settings in Guest Manager" on page 42
- "Make RADIUS Settings on the Ignition Server" on page 44
- "Make RADIUS Settings in Guest Manager" on page 45
- "Test Guest Manager's RADIUS Connection Settings" on page 45
- "Set Up E-Mail Notification Parameters" on page 46
- "Set Up SMS Notification Parameters" on page 47
- "Exporting and Importing Guest Manager Configurations" on page 48
- "Next Step" on page 50

About Usernames and Passwords



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

- **Guest Manager administrator:** This is the principal administrator of the Guest Manager application. Only the Guest Manager administrator can set up 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 page 54.

- **Tomcat administrator**: This person runs the Tomcat server that hosts the Guest Manager application. Make sure this administrator has a secure password, as noted in the "Run the Installer" on page 24.
- **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, "Make SOAP Settings on the Ignition Server" on page 40.
- **Ignition Server administrator:** This is the administrator who runs Ignition Dashboard and manages the Ignition Server appliance. You need these credentials in order to set up the Ignition Server appliance and in order 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 may be stored locally in Ignition, or they may be accounts in your LDAP or AD user store.

For additional details on the various accounts used to configure and run Guest Manager, see "Types of Accounts in Your Ignition Server Installation" on page 17.

Launch Tomcat

To run Guest Manager:

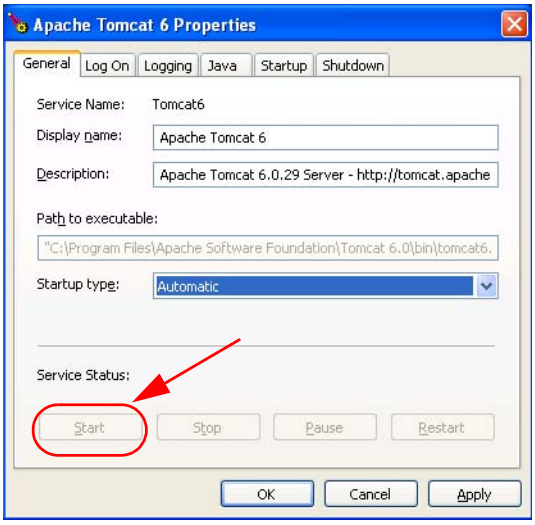
1. Open the Apache Tomcat Properties window on your PC that hosts Guest Manager. In Windows, click **Start**: **Programs**: **Apache Tomcat 6.0**: **Configure Tomcat**.

Hint: If the Start menu fails to launch the window, look in the system tray for an icon that looks like the one shown below. Double-click it to open the Properties window.



Tomcat icon in the Windows system tray

Windows displays the Apache Tomcat Properties screen. The **Service Status** field indicates whether the Tomcat Server is running.



2. Click **Start** to start Tomcat.
3. Click **OK** to close the Apache Tomcat Properties window.

Next Step: Launch Guest Manager as explained below.

Launch Guest Manager

In this section you will launch Guest Manager to check that it has been installed correctly. (At this point in the set-up 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:** This is the application the Guest Manager administrator will use to configure Guest Manager and to create provisioner accounts. Only the Guest Manager administrator can use it.
- **Provisioner Application:** This is the application provisioners use to create guest users.

Connect to the **Administrator Application** as follows:

1. Open a web browser and point it at the **GuestManager/admin/** application on your Tomcat server. If you have a default installation of Tomcat running on machine *pluto*, the URL is typically:

https://pluto:8443/GuestManager/admin/ (If the browser reports certificate errors, see “Set Up Tomcat to Require HTTPS Connections” on page 25.)

Note that the URL may instead be **http://pluto:8080/GuestManager/admin/** if you are not using a secure port to host Guest Manager. Avaya strongly recommends that you set up your Tomcat Server to require SSL connections. See “Set Up Tomcat to Require HTTPS Connections” on page 25.

2. Enter the login credentials of the Guest Manager administrator. By default, these are:
   - Username: **admin**
   - Password: **admin**

   A note on password retention: 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 will choose the option, “Never for this site.” Allowing the browser to retain passwords for the Guest Manager application is not secure, and it may cause your browser to display misleading “password update” messages when you edit users.
3. Click **Submit**. The Guest Manager administrator window appears. 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 again your new password in the C**onfirm Password** field. You may 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.

Next Step: 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 policy sections below and turn immediately to “Install the SOAP Certificate” on page 39.
- If any of your provisioner accounts are stored *in LDAP or AD*, turn to the next section, “Create a Provisioner Access Policy”.

Create a Provisioner Access Policy

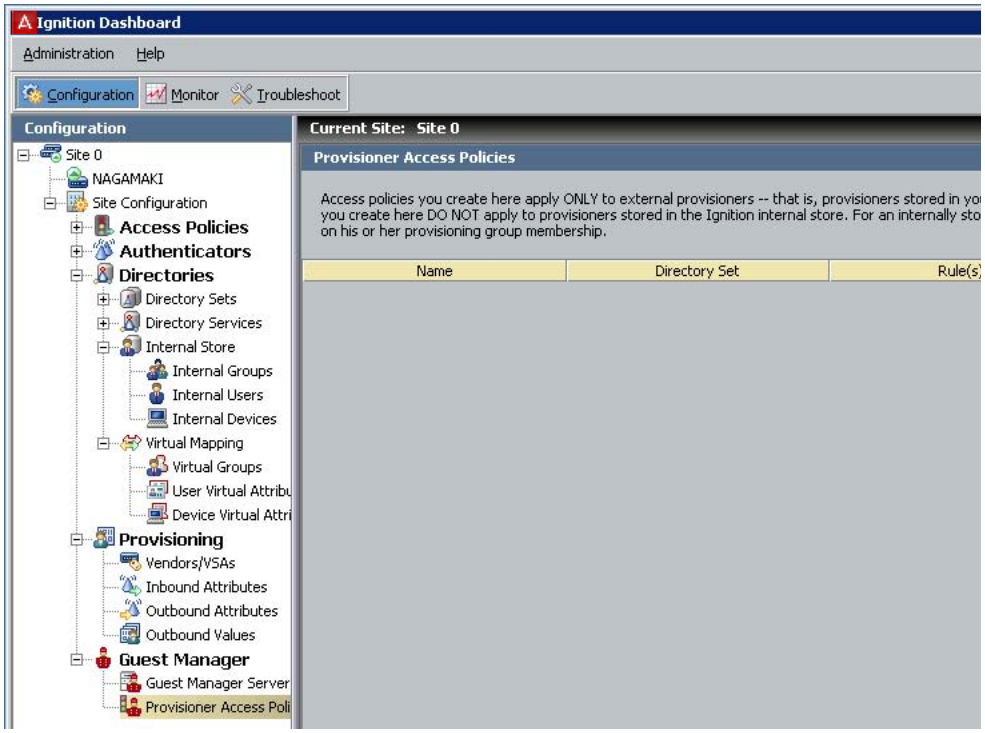
This section explains how to create a policy that gives certain users in your LDAP or Active Directory (AD) store the right to act as provisioners in Guest Manager. We call this policy a “provisioner access policy” or a “Guest Manager access policy.” Your provisioner access policy determines how Ignition Server looks up provisioner accounts in LDAP or AD and what type of provisioner access it grants to each provisioner.

Note! 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 proceed immediately to “Make RADIUS Settings on the Ignition Server” on page 44.

Follow these steps to set up LDAP or AD authorization of your provisioners:

1. Create the directory services, directory sets, and virtual groups that will 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 the *Avaya Identity Engines Ignition Server Administration Guide*.
   - 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 the *Avaya Identity Engines Ignition Server Administration Guide*.
   - 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 the *Avaya Identity Engines Ignition Server Administration Guide*.

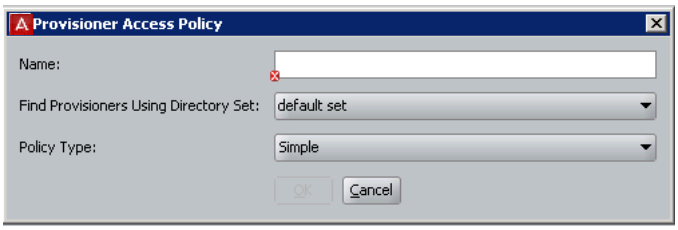
2. Create the provisioner access policy in Ignition Dashboard:



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

  Note that 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 shown "Managing Provisioning Groups" on page 110.)

- In the Provisioner Access Policy window, type a **Name** for this policy.



- In the **Find Provisioners Using Directory Set** dropdown list, choose the directory set you created or found in Step 1, above.

- In the **Policy Type** dropdown, choose *Simple* or *Advanced*.

  A *Simple* policy lets you map each virtual group to one or more provisioning groups; and *Advanced* policy lets you consider more criteria. If you choose *Simple*, continue to follow the steps below. If

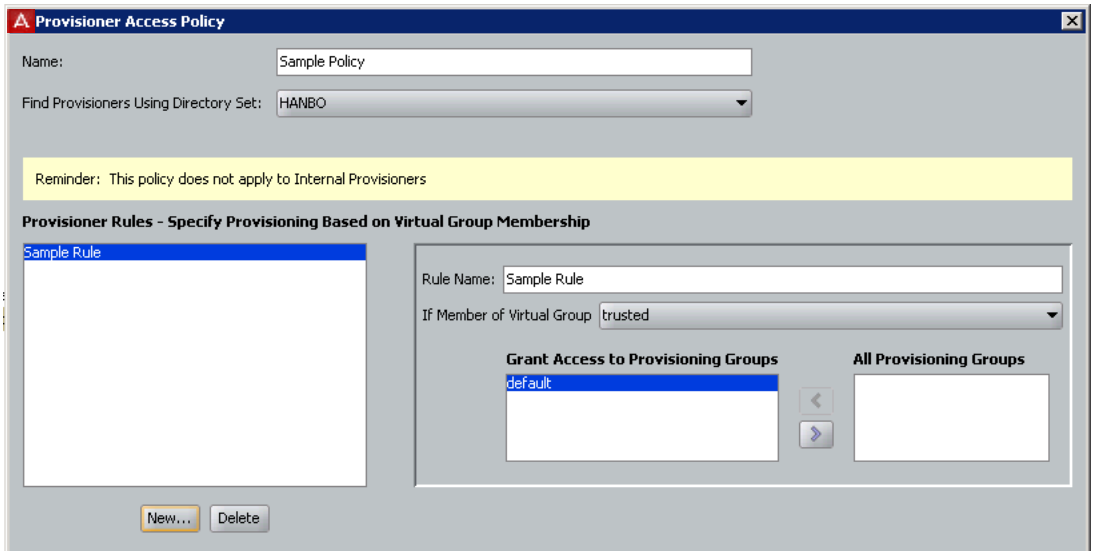
you choose *Advanced*, turn to "Create an Advanced Provisioner Access Policy" on page 36.

- Click **OK**.

The Provisioner Access Policy window appears. 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 the **New** button.
   - 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 Step 1 on page 33).
   - 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 Step: Turn to "Install the SOAP Certificate" on page 39.

Create 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, "Create a Provisioner Access Policy" on page 33, before you begin creating your advanced policy.

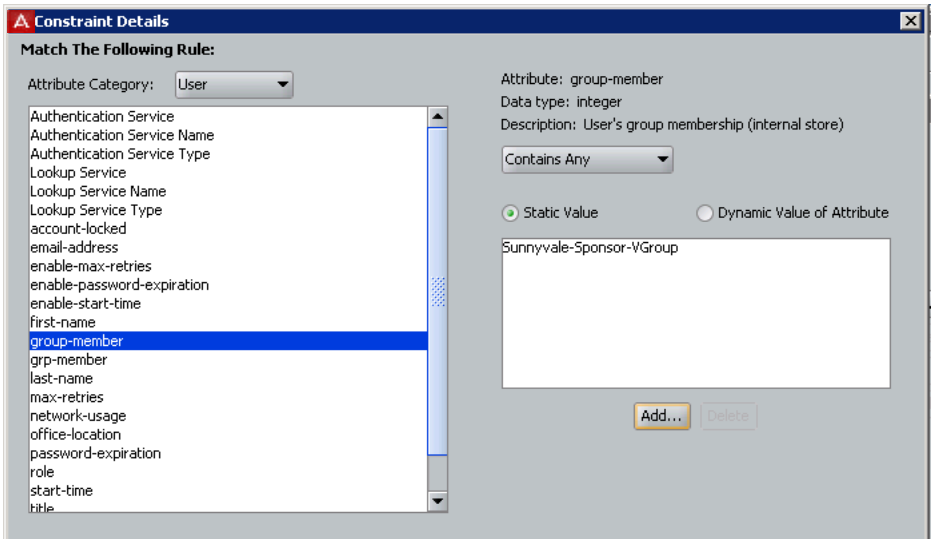
Follow these steps to set up advanced, rule-based authorization for you LDAP or AD-stored provisioners:

1. Create the directory services, directory sets, and virtual groups that contain your provisioner accounts. (See the "Create a Provisioner Access Policy" on page 33 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, type a **Name** for this policy. In the **Find Provisioners Using Directory Set** dropdown list, choose the directory set that contains your provisioners.
5. In the **Policy Type** dropdown, choose *Advanced*.
6. Click **OK**.
7. The Edit Provisioner Access Policy window appears. This window lets you write rules that assign each provisioner to one or more provisioner groups. 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.

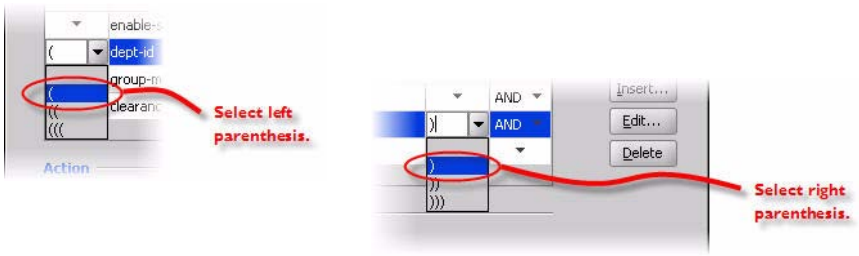
8. Below the **Rules** list, click **Add**.
9. In the New Rule window, give the rule a **Name** and click **OK**.
10. To add decision logic to your rule, add one or more constraints in the **Constraint** table. Each constraint tests the value of an attribute. If there are multiple constraints, join them into a single logical statement using the AND and OR conjunctions and, if needed, parentheses. Follow the steps below to do this:
    - 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** dropdown list, choose the type of attribute you want to test. (For explanations of the types, see “Attributes Used in Rule Constraints” in the *Avaya Identity Engines Ignition Server Administration Guide*.)
    - 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 dropdown 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 one of:
  - 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 Guide*.)
- If this is an **Allow** rule, add group provisioning to the rule. In the **All Provisioning Groups** list, click on the provisioning group you want to assign to the provisioner. Click the left-pointing arrow button to add that group to the **Grant Access to Provisioning Groups** list. *Optionally*, you can choose more groups from the **All Provisioning**

Groups list and click the left-pointing arrow button to add each one to the list. A provisioner can be a member of more than one provisioning group.

- Add additional rules to your user authorization policy as needed. To do this, go to the bottom left of the Edit Authorization Policy window, click **Add** to create a new rule, name the rule, and repeat the steps above.

11. Click **OK**. Your policy is complete.
12. *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 Step: Turn to "Install the SOAP Certificate" on page 39.

Install 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. You 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 "Make SOAP Settings in Guest Manager" on page 42.

Procedure: Use the steps below to install a new SOAP service certificate in Ignition Server and Guest Manager. *Remember, 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!*

1. Run Ignition Dashboard (see page 142) and create and import your new certificate as explained in the section, "Getting a New Certificate" in the "Managing Certificates" chapter of the Avaya *Identity Engines Ignition Server Administration Guide*.
2. Designate your new certificate as the *SOAP service certificate* as explained in the section, "Assigning the SOAP Service Certificate" in the "Managing Certificates" chapter of the *Avaya Identity Engines Ignition Server Administration Guide*.
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 the Guest Manager Administrator Application by pointing your web browser to **GuestManager/admin/** on your Tom cat server. For example, if you have a default installation of Tomcat running on a machine called *pluto*, the URL would be **https://pluto:8443/GuestManager/admin/** (or, if your are not using a secure port to host Guest Manager, the URL may be **http://pluto:8080/GuestManager/admin/**). Enter your Guest Manager administrator login credentials and click **Submit**. Do not allow the browser to remember your password.
5. Click **Administration > Connection > Certificate** button in the toolbar of the Administrator Application.
6. Click the **Add Certificate** button.
7. In the Add Certificates window, click **Browse** to load the certificate file. In the browser window, select the file name and click **Open**.
8. 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.
9. Click **Submit**. Ignition Server adds the selected entry to Guest Manager's **Trusted Certificates** list. The installed certificate resides in the Guest Manager keystore.



Tip. 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 "Set Up Tomcat to Require HTTPS Connections" on page 25.

Next Step: Make SOAP Settings on the Ignition Server as explained below.

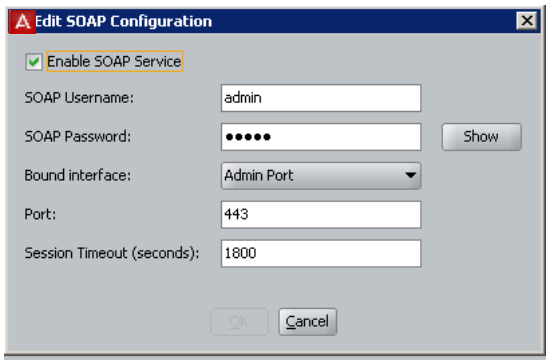
Make SOAP Settings on the Ignition Server

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 Guide*. Always check that document for the latest information on the SOAP service.

1. Launch Ignition Dashboard (see page 142) 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 the section, "Managing Ignition Server Licenses" in the *Avaya Identity Engines Ignition Server Administration Guide*.
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.

Figure 3 Example Settings for SOAP Service



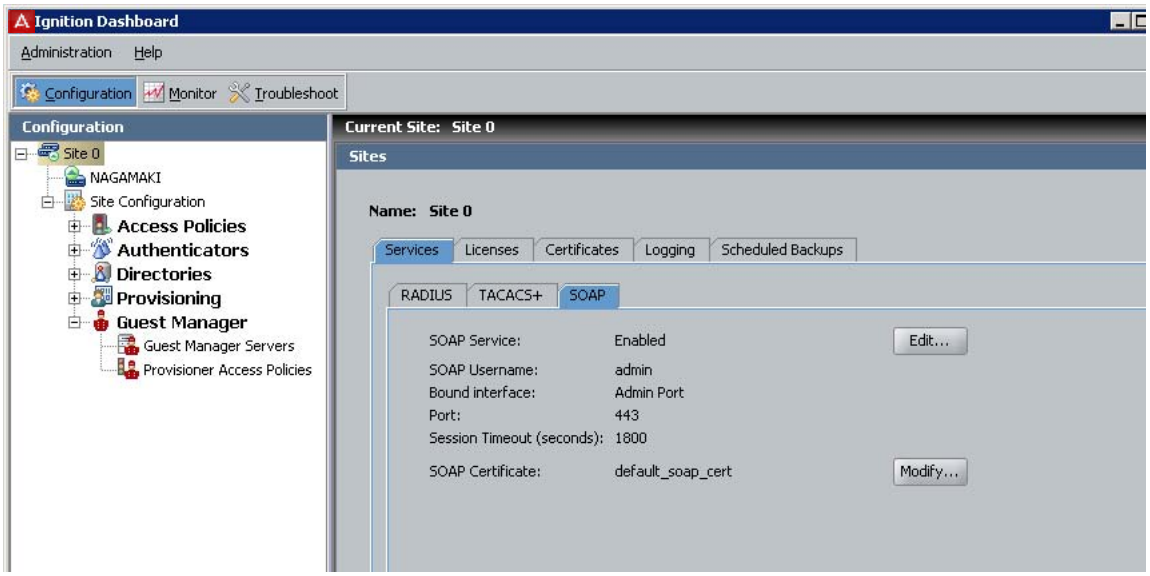
6. Edit the entries as follows, and make a note of these entries. (You will use them to connect Guest Manager to the appliance in Step 4 on page 43.)
7. Set the SOAP connection parameters:
   - **Enable SOAP Service**: Tick this check box to make the SOAP API service available.
   - **SOAP Username**: 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 dropdown 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 dropdown list. For further information on using VIPs, consult the section “High Availability Configuration” in the *Avaya Identity Engines Ignition Server Administration Guide*.

- **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 56 for details.

  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.

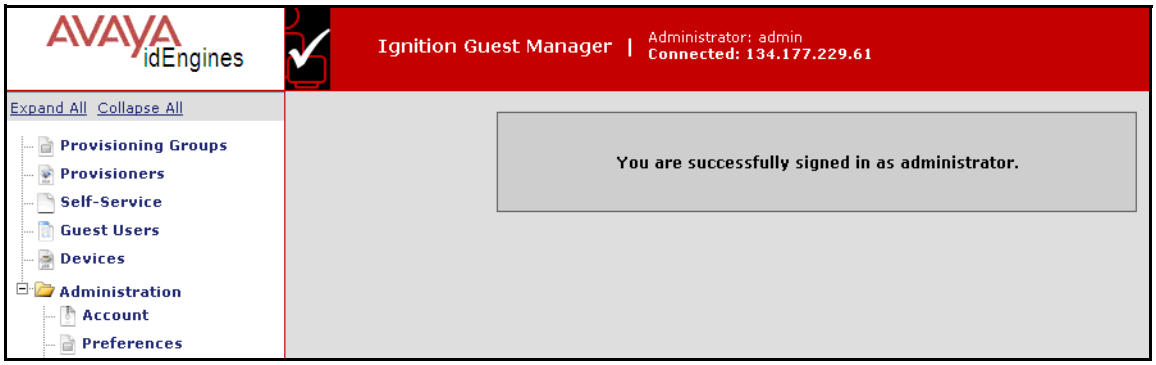
Next Step: Make SOAP Settings in Guest Manager as explained below.

Make SOAP Settings in Guest Manager

Specify your SOAP settings in Guest Manager:

1. Open the Guest Manager Administrator Application by pointing your web browser to **https://pluto:8443/GuestManager/admin/** or **http://pluto:8080/GuestManager/admin/** on your Tomcat server. Enter your Guest Manager administrator login credentials (*admin/admin* is the default) and click **Submit**. Do not allow the browser to remember your password.
2. Click on **Administration > Connection > Appliance** in the toolbar of the Administrator
3. 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 Step 6.
   - **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 (see page 142) 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 Step 6.
5. Click **Connect**.
6. The **Connected to Appliance** screen appears confirming the appliance connection. Guest Manager displays the name of the appliance to which you are connected.

Figure 4 Successfully connected to the Ignition Server



Note that the connection will disconnect after the timeout interval specified in Step 6.

Next Step: Make RADIUS Settings on the Ignition Server as explained below.

Make RADIUS Settings on the Ignition Server

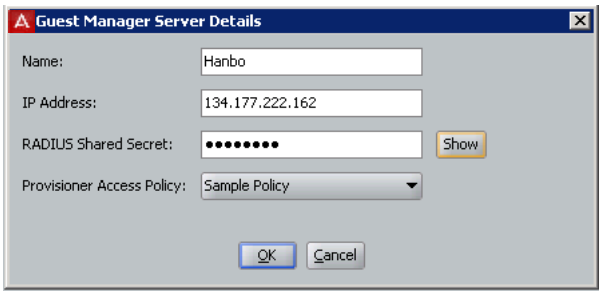


Next, you must create a *Guest Manager Server entry* in Ignition. This entry allows Ignition Server to recognize Guest Manager as a RADIUS authenticator that will be sending authentication requests.

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:

1. Launch Ignition Dashboard if it is not running already (see page 142).
2. In the main Dashboard window, click the **Configuration** button.
3. In the **Configuration** hierarchy tree, expand the **Guest Manager** node and click on **Guest Manager Server**s. 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 any 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 on page 45.
7. In the **Provisioner Access Policy** field, choose the policy you created in Step 2.
8. Click **OK**.

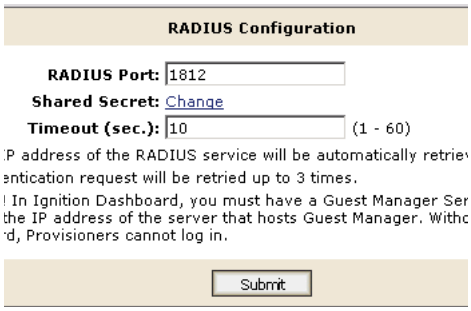
9. Make sure your firewall settings permit RADIUS traffic between Guest Manager and Ignition. Guest Manager uses RADIUS to authenticate provisioners. Your network must allow RADIUS (UDP) traffic to travel between the Guest Manager machine and the Ignition Server.

Note: 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 The Guest Manager configuration in the Dashboard Configuration tree.

Next Step: Make RADIUS Settings in Guest Manager as explained below.

Make RADIUS Settings in Guest Manager

Ignition Server uses RADIUS to authenticate provisioners. Set this up as follows:



1. In the Guest Manager Administrator Application (**https://pluto:8443/GuestManager/admin/** or **http://pluto:8080/GuestManager/admin/**) click on **RADIUS Configuration** in the toolbar of the Administrator Application.
2. Click **Administration > Connection > RADIUS**. In the RADIUS configuration screen, type the **RADIUS port number** where the Ignition Server RADIUS service is running. By default, this is 1812.
3. Enter shared secret in **Shared secret** field. If shared secret was previously set, click **change**. This is the secret you used in Step 5.
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**.

Next Step: Test Guest Manager's RADIUS Connection Settings as explained below.

Test Guest Manager's RADIUS Connection Settings

Follow these steps to test your RADIUS setup:

1. Create a provisioner account for yourself as explained in "Creating a Provisioner in the Internal Store" on page 99.
2. Click **Administration > Notification > Email**.

3. In the Login screen, enter your provisioner **Username** and **Password**.
4. Click **Sign In**. If your login attempt fails, see “Problem: Provisioner Can’t Log In” on page 139.

Next Step: Set Up E-Mail Notification Parameters as explained below.

Set Up E-Mail Notification Parameters

When provisioners create guest user accounts, the usual way to give the guest his or her new username and password is by e-mail. Alternatively, you may e-mail the credentials to your front desk receptionist, for example, who prints them and passes them to the guest. To enable the sending of e-mail notifications, do the following:

1. Log in to the Administrator Application.
2. In the Administrator Application, click **Manage Configuration**.
3. Tick the **Enable Sending of Email Notification** check box. With this feature turned on, Guest Manager sends guest users, provisioners, and/or others an e-mail notification when guest user accounts are created and/or updated.
4. In the **SMTP Server** field, type the fully-qualified domain name or the IP address assigned to the server that will transmit e-mail notifications from Guest Manager.
5. In the **From Address** field, type the e-mail address that will appear in the “From” line of the messages that Ignition Server sends. For example, user provisioning notifications might contain a **From Address** such as “guest-reception@idengines.com”. This address appears in all types of e-mails that Guest Manager sends.
6. If your SMTP server requires authentication, then tick the **User Authentication** check box and, in the **SMTP Server User Name** and **Password** fields, type the login credentials of the SMTP server user. (Click **Change** to expose the password fields.)
7. Click **Submit**.

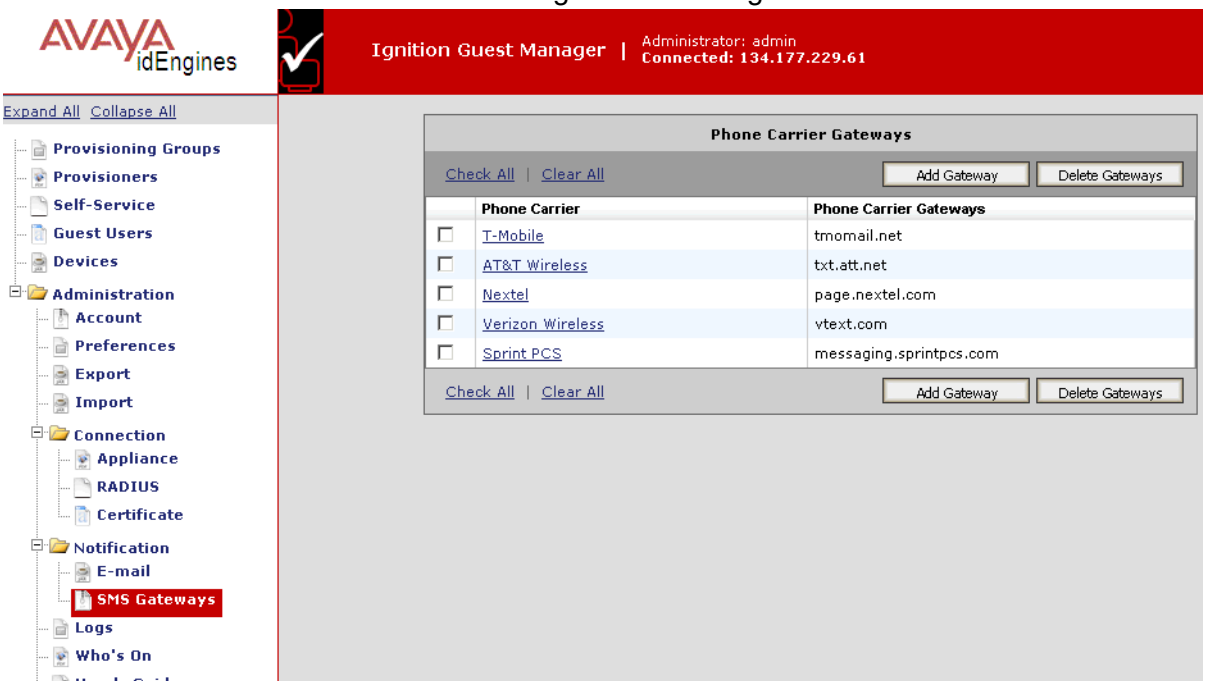
Hint: Make sure you set up an appropriate e-mail notification template as shown in “Writing SMS and E-mail Templates for Account Notifications” on page 104.

Next Step: Set Up SMS Notification Parameters as explained below.

Set 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. To set this up:

1. Run the Guest Manager Administrator Application.
2. Click **Administration > Notification > SMS Gateways**.
3. 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.



4. Set up gateways in one of the following ways:
   - To edit an existing gateway, click its name. In the Edit window, type the SMS gateway address in the **Carrier Gateway** field and click **Submit**.
   - To add a gateway, click **Add Gateway**. In the Add Carrier Gateway window, type the **Carrier Name** and the **Carrier Gateway** address, and click **Submit**.

Hint: Make sure you set up an appropriate e-mail notification template as shown in "Writing SMS and E-mail Templates for Account Notifications" on page 104.

Exporting and Importing Guest Manager Configurations

Release 8.0.0 introduces a new Guest Manager enhancement that allows you to export and import Guest Manager Configurations. This feature enables you to port Guest Manager configurations between multiple Guest Manager deployments.

The configurations you can export and import include:

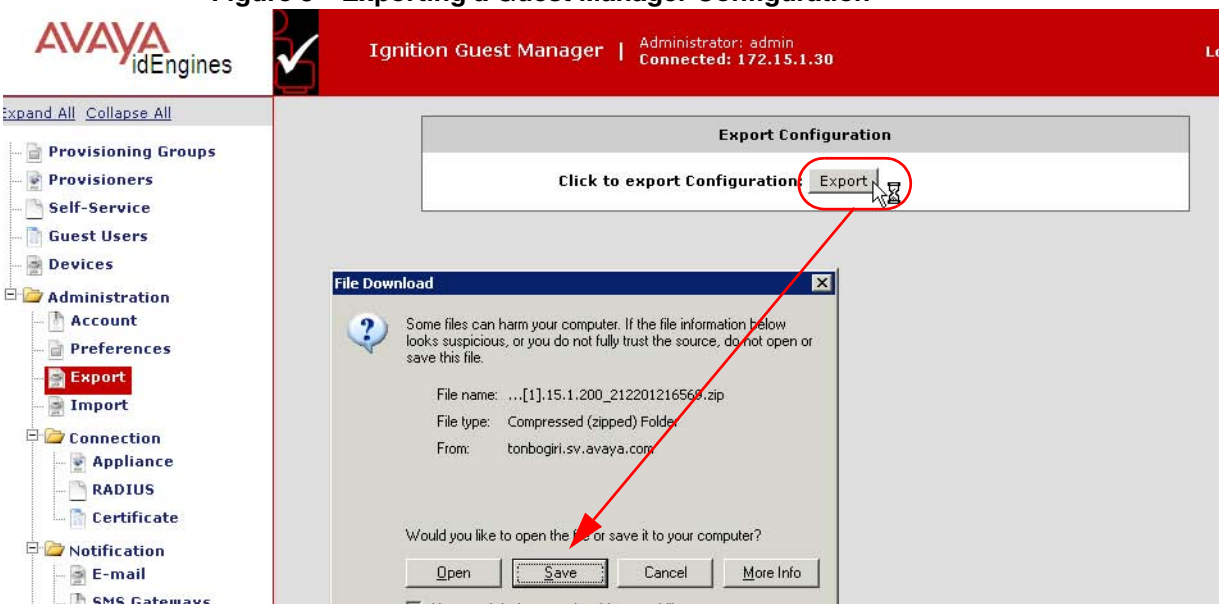
- Appliance configurations
- RADIUS configurations
- User certificates
- Tomcat configurations (HTTP, SSL etc.)
- User preferences

Exporting a Guest Manager Configuration

To export a Guest Manager configuration:

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**.

Figure 5 Exporting a Guest Manager Configuration



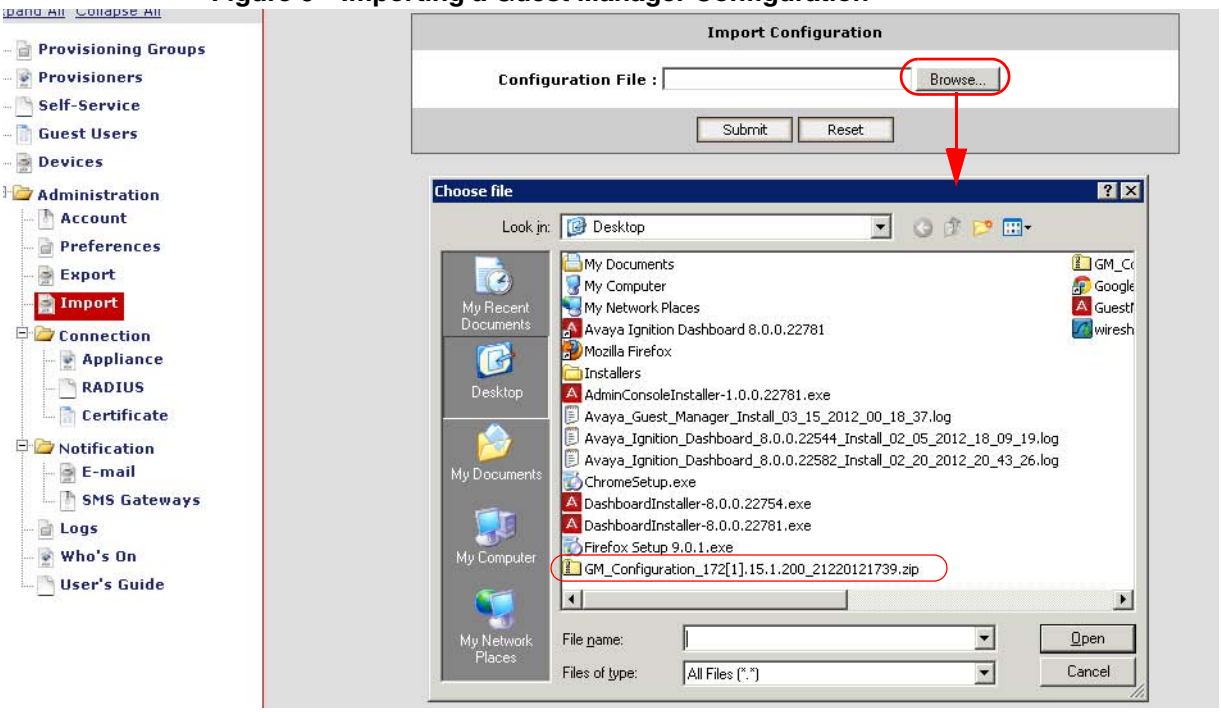
4. In the **Save as** window, browse to where you want to save the configuration zip file and click **Save**.
5. In the **Download complete** window, click **Close**.

Importing a Guest Manager Configuration

To import a Guest Manager configuration:

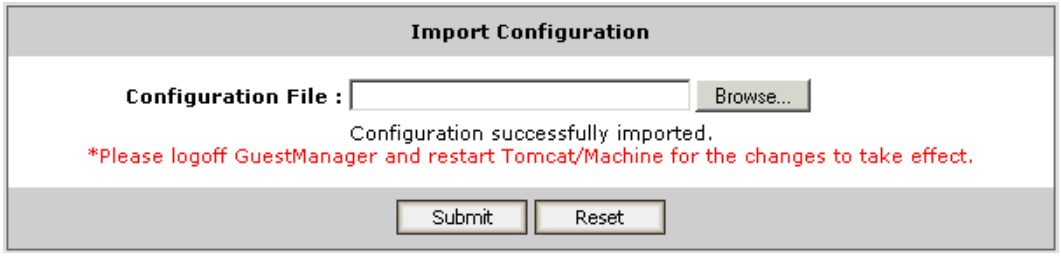
1. From the Guest Manager Administrator Application, click **Administration > Import**.
2. On the **Import Configuration** page, click **Browse**.
3. In the **Choose file** window, select your configuration zip file, and click **Open**.

Figure 6 Importing a Guest Manager Configuration



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

Figure 7 Successful Import



5. Log off of Guest Manager and restart Tomcat/Machine for the changes to take effect.

Next Step

Set up your guest authorization policies as explained in Chapter , “Setting Guest Authorization Policies”.

Managing Guest Manager

This chapter is intended for the Avaya Identity Engines Ignition Guest Manager Administrator; it 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 119.



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.

The contents of this chapter are:

- “Running the Guest Manager Administrator Application” on page 51
- “If You Act as Both Administrator and Provisioner” on page 52
- “Restarting Guest Manager” on page 52
- “Connecting Guest Manager to the Ignition Server Appliance” on page 53
- “Disconnecting Guest Manager from the Ignition Server Appliance” on page 53
- “Setting the Administrator Username and Password” on page 54
- “Editing E-Mail Notification Settings” on page 54
- “Configuring Timeout Settings” on page 55
- “Log Files” on page 56

Running the Guest Manager Administrator Application

To log in to the **Guest Manager Administrator Application**:

1. Point your web browser to **GuestManager/admin/** on your Tomcat server. By default, the location is (assuming an example host name of *pluto*) **http://pluto:8080/GuestManager/admin** or **https://pluto:8443/GuestManager/admin**.

   The login screen appears. If the window does not load, see “Launch Tomcat” on page 30. If the browser reports certificate errors, see “Set Up Tomcat to Require HTTPS Connections” on page 25.

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 as a provisioner. Please follow the guidelines below to do this.

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 17.

To Switch Between the Administrator and Provisioner Applications

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.

1. Log out of the current application.
2. Point your browser to the desired Guest Manager application (replace “pluto” here with the name of the server that hosts your Guest Manager).
   - To switch to the Administrator Application, go to: **http://pluto:8080/GuestManager/admin** or **https://pluto:8443/GuestManager/admin**
   - To switch to the Provisioner Application, go to: **http://pluto:8080/GuestManager/provisioner** or **https://pluto:8443/GuestManager/provisioner**
3. Type your user name and password, and do *not* allow the browser to remember your password.

Restarting Guest Manager

To restart Guest Manager:

1. On your Guest Manager PC, click **Start: Programs: Apache Tomcat 6.0: Configure Tomcat**, and then click **Stop** in the Apache Tomcat Properties screen. Click **Start**. Click **OK** to close the window.
2. Reconnect to the Avaya Identity Engines Ignition Server as explained below in “Connecting Guest Manager to the Ignition Server Appliance”.

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.

Figure 8 Guest Manager’s connection indicator showing no connection



Connect Guest Manager to the Ignition Server as follows:

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 > 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 “Make SOAP Settings on the Ignition Server” on page 40.
5. Click **Connect**.

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

Figure 9 Guest Manager’s connection indicator showing a connection



Disconnecting Guest Manager from the Ignition Server Appliance

In order to log out of the Ignition Server appliance to which Guest Manager is currently connected, do the following:

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 Click on **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 17 for details.)

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.** The Administrator Account screen appears.
4. If desired, edit the **User Name**.
5. If you wish to edit the **Password**, click the **Change** link in the Password field, type the **Current Password**, type the **New Password**, and type the new password again in the **Confirm Password** field.



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 “Set Up E-Mail Notification Parameters” on page 46.

Editing SMS Notification Settings

Creating SMS Gateways

You may set up the e-mail notification settings as explained in “Set Up SMS Notification Parameters” on page 47.

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.

To delete an SMS gateway:

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
- Administrator Session Timeout Threshold.
- SOAP Client 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 95.

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.

To set the administrator HTTP session timeout period:

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 in order 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 "Make SOAP Settings on the Ignition Server" on page 40.

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 53.

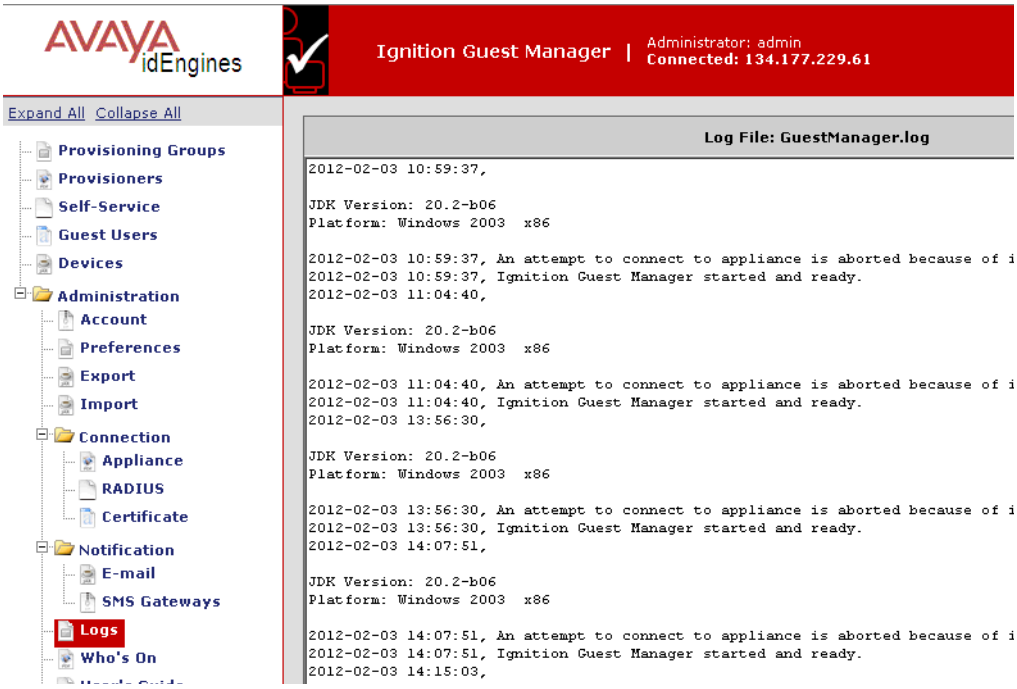
Log Files

The default name for the log files of Guest Manager takes the form, **GuestManager.log**, **GuestManager.log.1**, **GuestManager.log.2**, and so on. You can change the name and default location for this log file, as explained in the sections that follow.

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 10 Contents of the GuestManager.log File



Default Location of the Log File

By default, the **GuestManager.log** file is located in the **logs** sub-directory under the location where you have installed the Tomcat application. If you have chosen the default settings for the installation of the Tomcat application, you will find the **GuestManager.log** file at the location: `C:\Program Files\Apache Software Foundation\Tomcat 6.0\logs`.

Changing the Default Location of the Log File

The default location for the **GuestManager.log** file is specified in the configuration file **log4j.properties** which is located under the **webapps** sub-directory associated with the Tomcat application. In a typical installation, you will find the **log4j.properties** file at the location:

`C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\GuestManager\WEB-INF\classes`.

Required Steps

In order to specify a different location for the log file,

1. Instruct all provisioners to log out of Guest Manager. Make sure no guests are using the self-provisioning portals (if any).
2. If Tomcat is running, stop the Tomcat application.
3. Locate the **log4j.properties** file.
4. Open the **log4j.properties** file in a text editor.

5. Locate the entry "`log4j.appender.ROLLFILE.File`" in this file. The default assignment is `C:/Program Files/Apache Software Foundation/Tomcat 6.0/logs/GuestManager.log`
6. Edit the assignment for this variable. Specify the desired path for the **GuestManager.log** file. If you need to, you can specify another name for the log file.
7. Save your changes to the **log4j.properties** file.
8. Restart the Tomcat application.
9. Connect Guest Manager to the Ignition Server (see page 53) and inform the provisioners that they may log in again.

Guest Manager will place the log file in the location you specified in the **log4j.properties** file. Additionally, if you have also changed the default name for the log file, Guest Manager will display the new name for the log file the next time you view it.

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 will need an Ignition Server Administrator login in order to use Dashboard.



Hint! If you are in a hurry to simply create some guest users, then you will be happy to know you can skip most of the policy setup procedure. See "Creating a Minimal Authorization Policy" on page 83.

Contents

- "Dashboard Configuration Checklist" on page 59
- "Setting Authorization Policies for Guest Users" on page 60
- "Sample Authorization Policies to be Used in This Chapter" on page 63
- "Step-by-Step Configuration in Ignition Dashboard" on page 65
- "Creating a Minimal Authorization Policy" on page 83

Dashboard Configuration Checklist

In order to set up Ignition Server to support guest users, use Ignition Dashboard to complete the steps in the order shown here.

Dashboard Configuration Checklist

	Configuration Step	See
☐	Create New Internal User Groups	page 66
☐	Create a Directory Set for the Guest Users	page 67
☐	Create the RADIUS Access Policy	page 68
☐	Set Up the Allowed Authentication Types	page 69
☐	Set Up Identity Routing	page 70
☐	Create Your Authenticator Hierarchy to Label Your Locations	page 70
☐	Create Your Authenticators	page 71
☐	Optional: Create a Device Template for the Authenticator	page 73

Dashboard Configuration Checklist

	Configuration Step	See
☐	Optional: Create the Authenticator and Apply the Device Template	page 74
☐	Create Outbound Values For Assigning Users to VLANS	page 74
☐	Sketch Out Your Guest Authorization Policy	page 76
☐	Write Authorization Rules That Limit Access Types	page 77
☐	Write Authorization Rules That Limit Network Rights	page 82
☐	Write Authorization Rules That Limit Access Zones	page 81
☐	Sort the Rules to Create Your Policy	page 82

Beginning on page 63, this chapter provides an example configuration to show you how to perform these steps.

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 screen 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 screen appears as shown below.

Figure 11 Example Guest User Provisioning Form

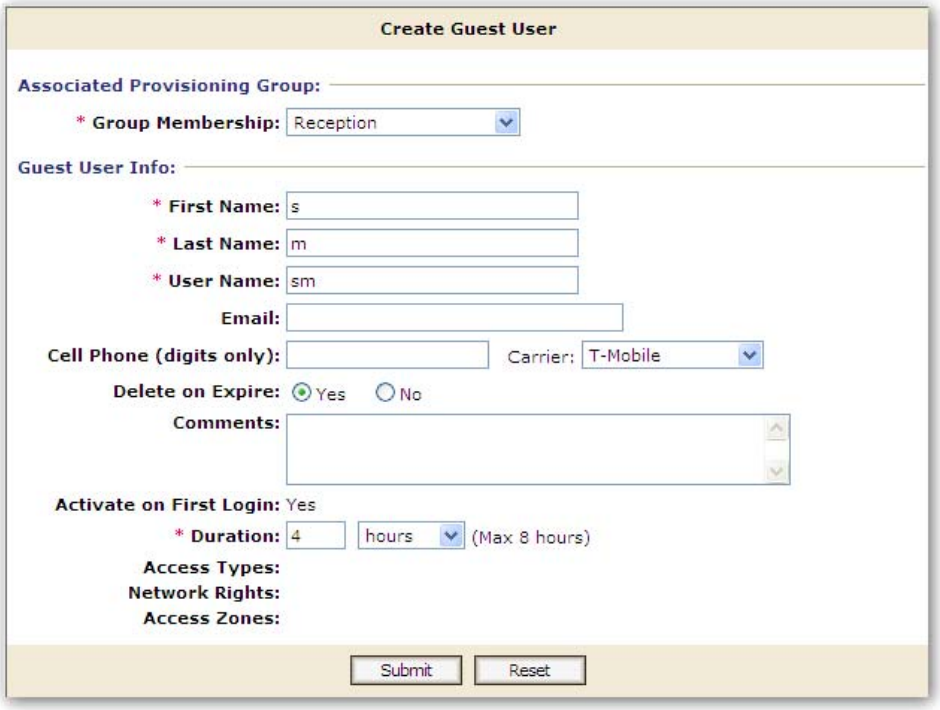
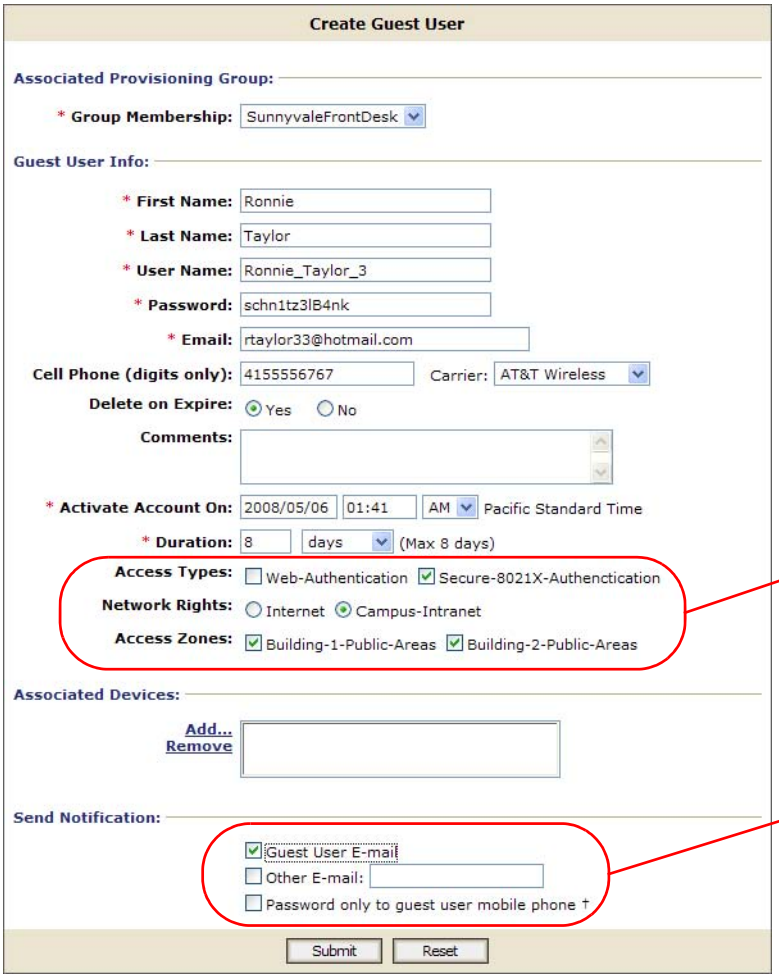


Figure 12 Example Guest User Provisioning Form



Access Constraint check boxes allow the provisioner to dictate the allowed Access Types, Network Rights, and Access Zones for each guest user.

E-mail check boxes: These appear only if your administrator has configured Guest Manager to send e-mail.

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.



Tip: 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. Starting on page 65, this document explains how to set up an example policy. For additional information, consult the "User Authorization Policy" chapter in the *Ignition Server Administration Guide*.

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.



Tip. 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 65 shows you how to make these settings in Ignition Dashboard.

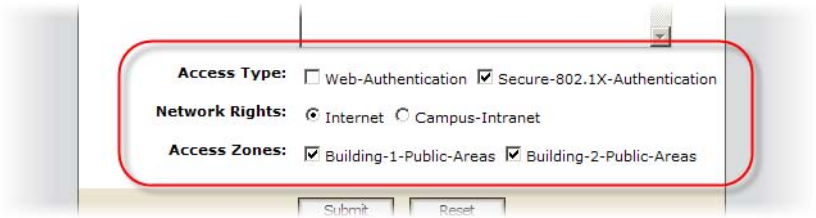
The Example

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 (a) 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"); (b) what parts of the network the guest can visit ("Internet" only or the "Campus-Intranet" which includes the local network and the Internet); and (c) 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."

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

1. Run Ignition Dashboard

Run Ignition Dashboard (see page 142) and log in as the Ignition Server Administrator.

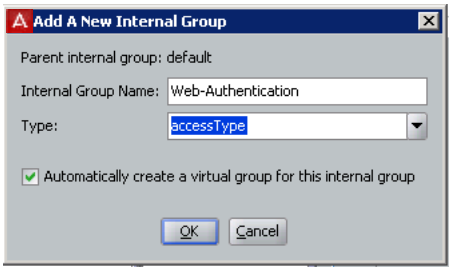
2. Create New Internal User Groups

Follow the steps below to create these new internal user groups:

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

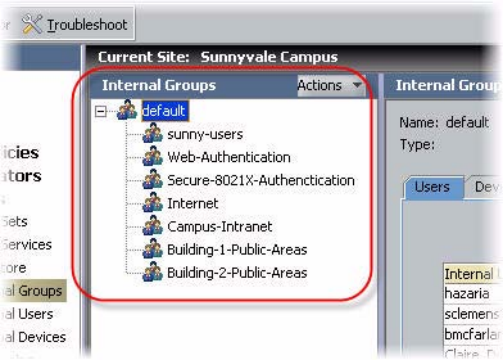
2.1. In the Ignition Dashboard main navigation tree, click **Directories: Internal Store: Internal Groups**. The application displays the Internal Groups panel.

2.2 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:

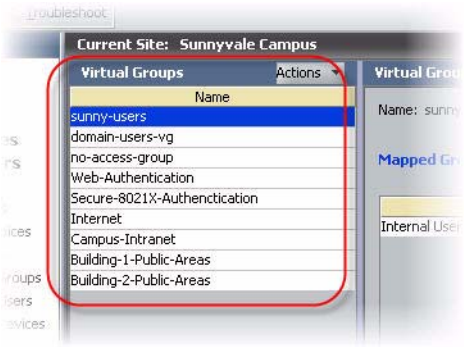


- Enter the **Internal Group Name**, “Web-Authentication”.
- In the **Type** field, specify the group type (also known as the access constraint class); this is also the name of the Access Constraint check box that will appear in the Guest Manager application. For the “Web-Authentication” group, specify 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**.)



2.3 Repeat Step 2.2 for the remaining internal groups to be created. If you are replicating the example, create all the groups listed in the preceding table. 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.



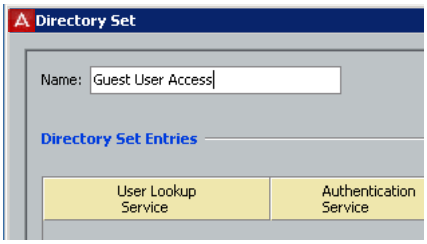
When you have added the final new internal group entry, the Internal Groups panel and the Virtual Groups panel will look similar to the figures shown at the right.

3. Create a Directory Set for the Guest Users

Next, you must 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:

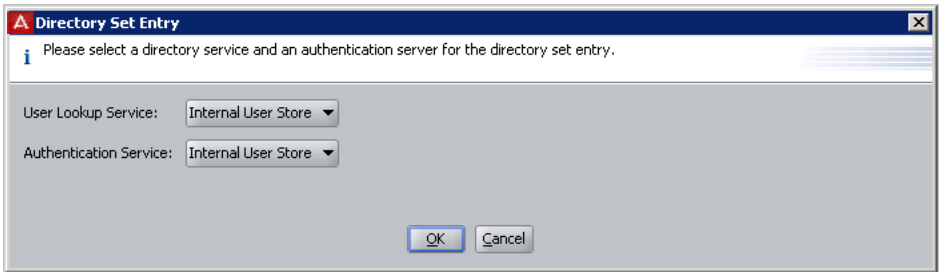
3.1 In Ignition Dashboard's navigation tree, select **Directories: Directory Sets**. The Directory Sets panel appears.

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

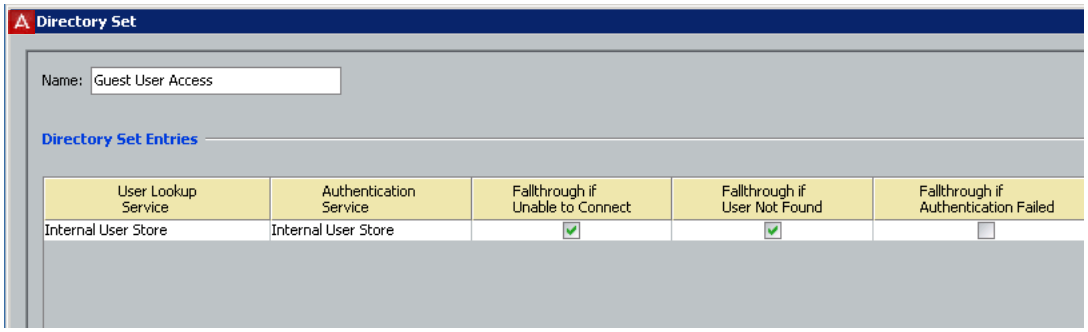


3.3 Type in the name for the directory set ("Guest User Access" in the example). Click **Add**.

3.4 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.



3.5 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.”

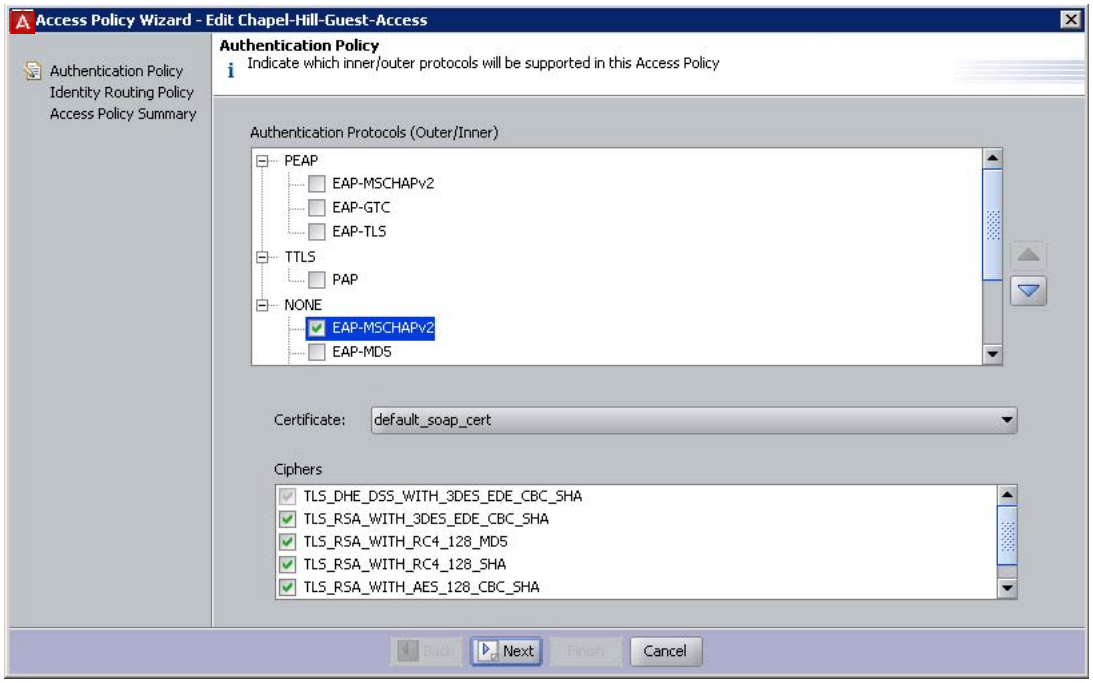
4.1. In Ignition Dashboard’s main navigation tree, expand **Access Policies** and click on **RADIUS**. At the bottom of the main panel, click **New**.

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

4.3 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:



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

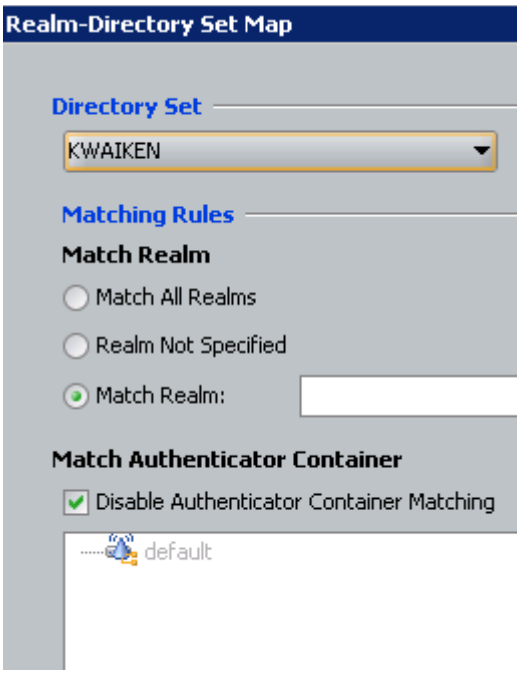
- Under PEAP, tick *EAP-MSCHAPv2*
- Under NONE, tick *EAP-MSCHAPv2*, *MSCHAPv2*, and *PAP*
- Leave the **Certificate** and **Ciphers** fields set to their defaults.
- Click **Next**.

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:



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

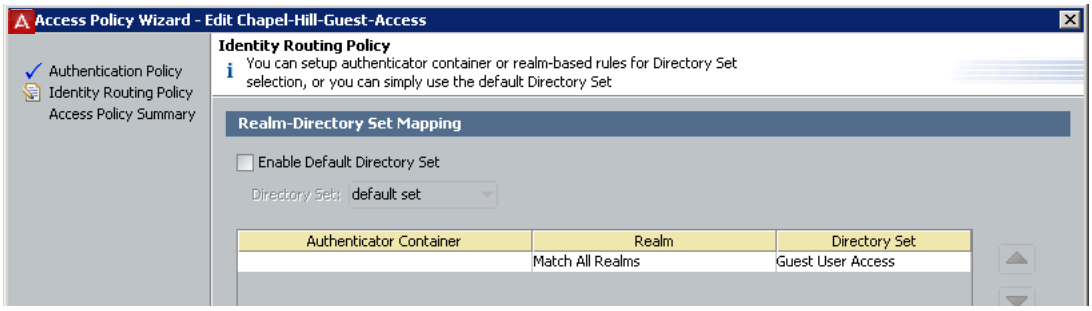
6.2 In the Realm-Directory Set Map window:

- In the **Directory Set** dropdown 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:

6.3 Click **Next**.

6.4 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:

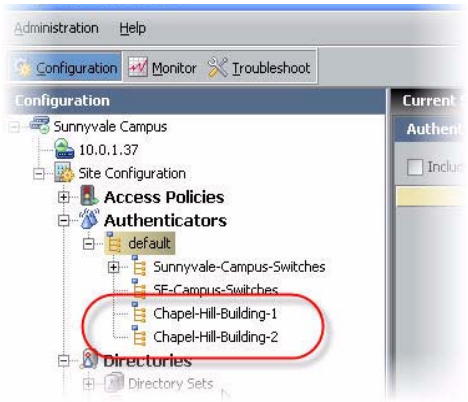
7.1. In Dashboard’s main navigation tree, expand the **Authenticators** node. This displays the root node of your **Authenticator Container Hierarchy**. Click on the root node (usually called, “default”).

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

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

7.4 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.**

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



8. Create Your Authenticators

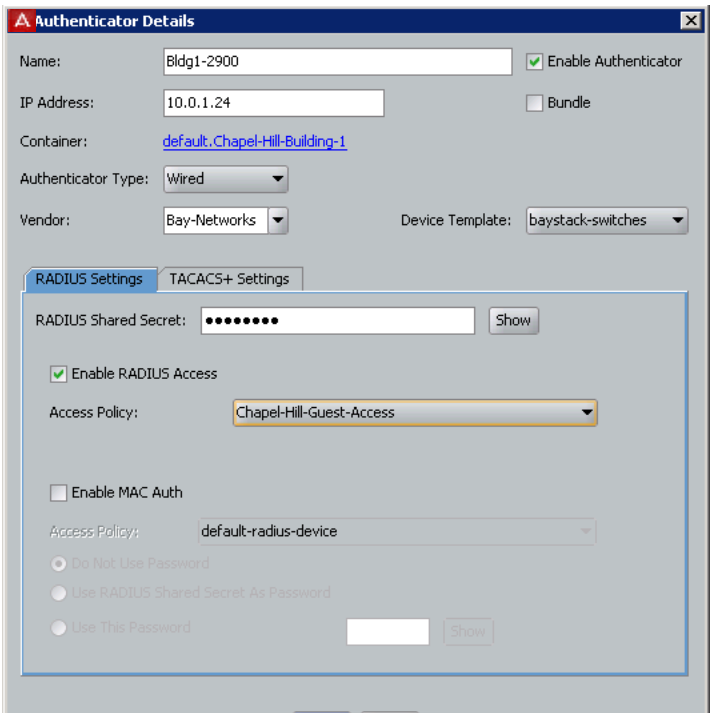
Next, create an Ignition Server *authenticator record* for each switch, access point, and web authentication portal that guests will use. The authenticator record makes Ignition Server aware of the switch, and specifies how Ignition Server communicates with it.

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:

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

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



8.3 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** dropdown 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** dropdown 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 and turn to "Create Outbound Values For Assigning Users to VLANS" on page 74.

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:

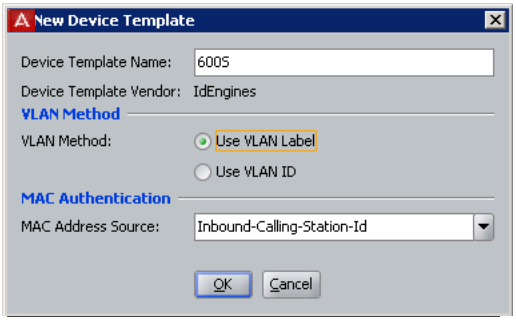
9.1. From the Dashboard main navigation tree, expand **Provisioning** and click **Vendors/VSAs**.

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

9.3 Click **New**.

9.4 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**.

9.5 Click **Done** to dismiss 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 and turn to "Create Outbound Values For Assigning Users to VLANS" on page 74.

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.)

10.1. 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*).

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

10.3 Create your authenticator record just as you did in "Create Your Authenticators" on page 71, but with the following changes:

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

10.4 Click **OK**.

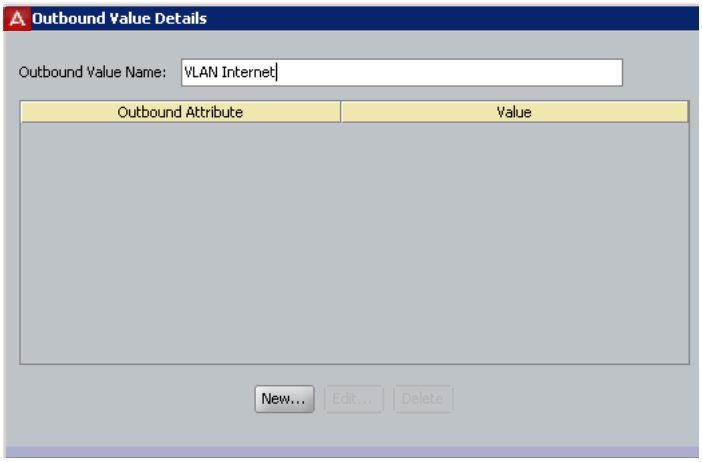
If you have additional 600S devices deployed, repeat these steps for each, taking care to place each device correctly in the container hierarchy. If following this example, add a 600S authenticator in *Chapel-Hill-Building-2*.

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 *Inter*net"), and one with a VLAN ID of "20" that offers access to the Internet and the campus network (we'll call this one "VLAN *Intra*net"). 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 the chapter titled "Session Provisioning" in the *Ignition Server Administration Guide*.

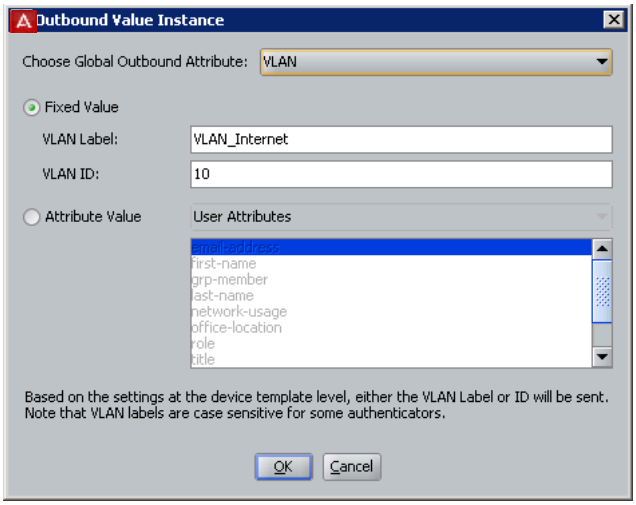


11.1 In Dashboard's navigation tree, expand the **Provisioning** node and click **Outbound Values**. At the bottom of the Outbound Values panel, click **New**.

11.2 In the Outbound Value Details window, in the **Outbound Value Name** field, type "VLAN Internet".

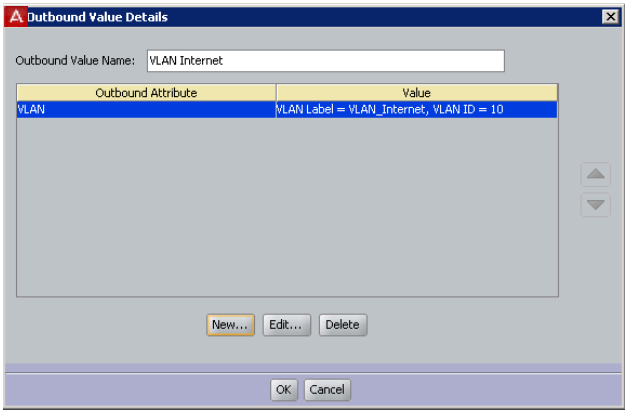
11.3 Below the **Outbound Attribute** table. click **New**

11.4 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*" a sample ID of "*10*".
- Click **OK**.

11.5 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.

11.6 Create another outbound value, this time calling it "VLAN *Intra*net" instead of "VLAN *Inter*net". Use the same steps you used to create the "VLAN *Inter*net" 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-802.1X-
    Authentication]
  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 80.

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

13.1. In Ignition Dashboard's main navigation tree, expand **Access Policies**, expand **RADIUS**, and click the name of the policy your created in Step 4.

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

13.3 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.

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

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

13.6 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.

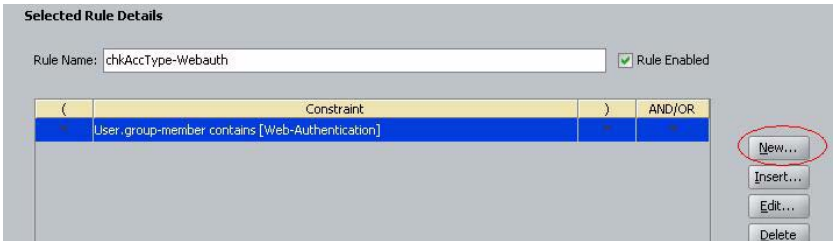
Your rule consists of *constraints* that can be ANDed and ORed together. It is a good idea to sketch out your desired constraints now. Bearing in mind that the limits applied to a guest user are expressed as “group-member” attributes, and that the authenticator's model name is expressed as an “Authenticator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

13.7 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.

13.8 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.

13.9 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.

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

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

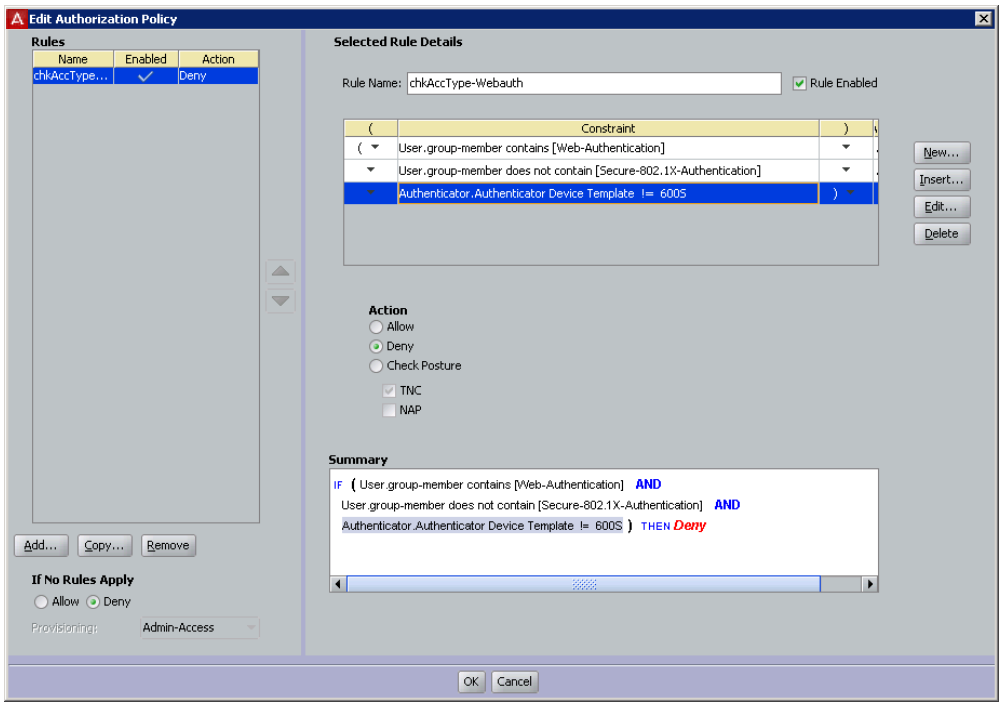
- Select an Attribute Category of **Authenticator**.
- In the list, click **Authenticator Device Template**.
- In the dropdown list on the right, select **Not Equal To**.
- Click the **Static Value** radio button.
- In the dropdown list, choose **600S**.
- Click **OK** to close the Constraint Details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

13.12 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 *Ignition Server Administration Guide* for further information.

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-802.1X-Authentication 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-802.1X-Authentication 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 page 71.

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 is any one of [Building-1-Public-Areas]   AND
User.group-member is not any one of [Building-2-Public-Areas]   AND
Authenticator.Authenticator Hierarchy != [Chapel-Hill-Building-1] )
THEN Deny.
```

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

```
IF  ( User.group-member is any one of [Building-2-Public-Areas]   AND
User.group-member is not any one of [Building-1-Public-Areas]   AND
Authenticator.Authenticator Hierarchy != [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. Recall that we created the VLAN outbound values on page 74. 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 *Inter*net"):

```
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 *Intra*net"):

```
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

Finally, you may optionally 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.

Next Steps

Next, create the Provisioner accounts as explained in Chapter , “Administrator Application: Managing Provisioners, Guests, and Devices”.

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 “Creating an Authentication-Only Policy” of the *Ignition Server Ignition Server Administration Guide*.

Next Steps Next, create the Provisioner accounts as explained in Chapter , “Administrator Application: Managing Provisioners, Guests, and Devices”.

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 119.

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.

Contents

- "Creating a Self-Provisioning Service" on page 85
- "Deploying a Self-Provisioning Service" on page 89
- "Managing Self-Provisioned Users" on page 90
- "Deleting a Self-Provisioning Portal" on page 91

Creating a Self-Provisioning Service

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

Prerequisites

When you create a self-provisioning portal, Guest Manager deploys it automatically on the Tomcat server where Guest Manager is running. Make sure your Tomcat server is in autoDeploy mode to support new portal deployments. (Check your Tomcat *web.xml* file for the “autoDeploy” setting.)

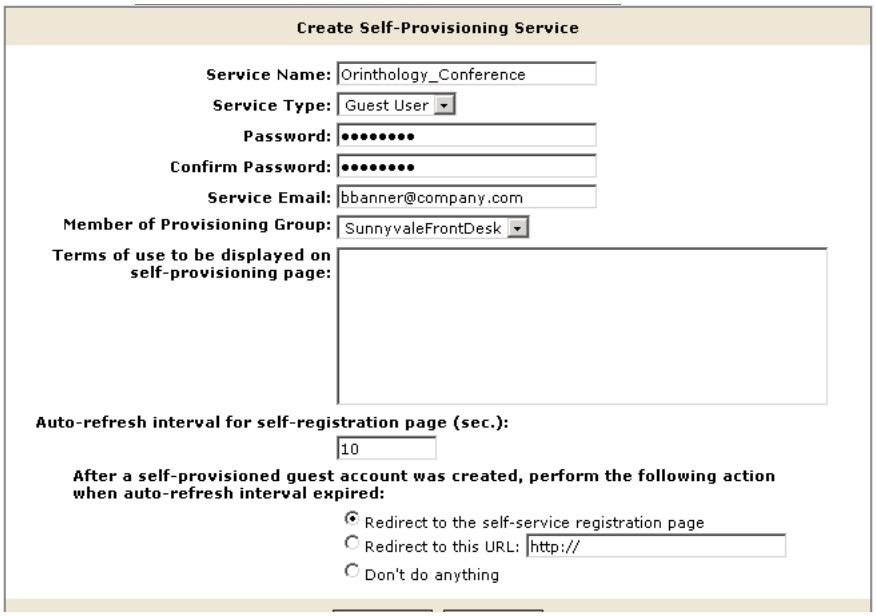
Make sure you have configured Guest Manager to send new guest users their account passwords via SMS or e-mail. Do one or both of the following:

- Set Guest Manager to send e-mail notifications, as explained in “Set Up E-Mail Notification Parameters” on page 46
- Set Guest Manager to send SMS messages, as explained in “Set Up SMS Notification Parameters” on page 47.

To create a self-provisioning service:

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.

Figure 13 Create Self-Provisioning Portal Screen

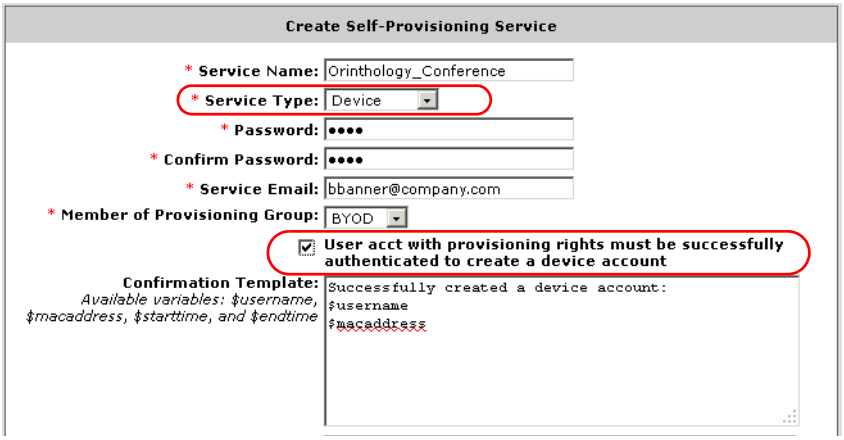


3. Set the portal’s account details. The service you are creating will consist of a Self-Provisioning Service and the account, so you must provide the information needed to set up the service.
   - The **Service Name** is the name of the provisioner account that manages the portal and is also used as 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. **Note**: If you select this check box, only provisioners who are successfully authenticated are allowed to create a device account (i.e. 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.

Figure 14 Service Type: Device



- **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. 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 E-Mail**: Enter the e-mail 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** dropdown 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.
Note: 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. **After a self-provisioned guest account was created, perform the following action when auto-refresh interval expired** – 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.

Figure 15 Successful Creation of a Guest User Portal

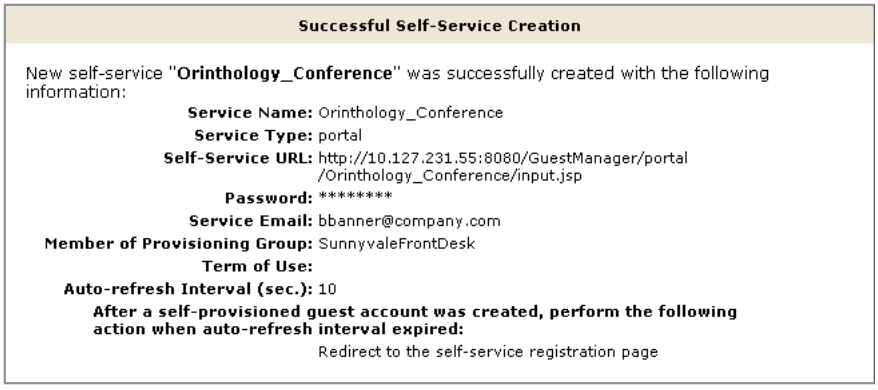
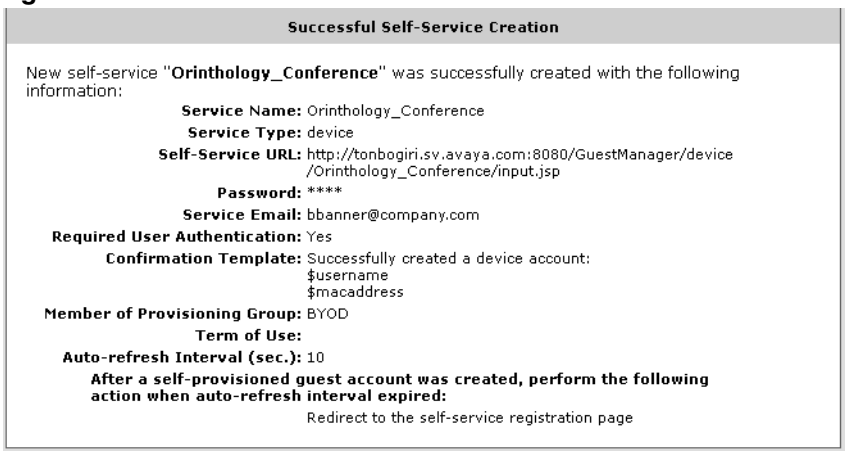


Figure 16 Successful Creation of a Device Portal



Next steps: Finish deploying the portal as shown in the next section.

Deploying a Self-Provisioning Service

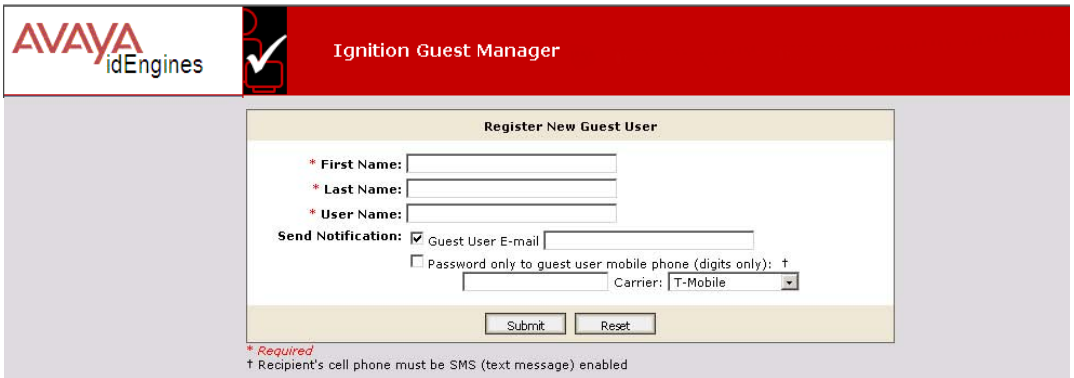
When you create a self-provisioning service (see the preceding section, "Creating a Self-Provisioning Service"), Guest Manager deploys it automatically on the Tomcat server where Guest Manager is running. Complete the deployment as follows:

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:
   http://localhost:8080/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:
   http://localhost:8080/GuestManager/device/Orinthology_Conference/input.jsp

NOTE! With Internet Explorer 8.0 browser you may see the URL truncated especially if you are viewing with larger fonts; in those cases please do the following 1) Decrease font size in that case you will not have problem getting the complete URL in spite of visibility issue 2) use older version of browser (6.0) or other browsers which do not have this problem.

3. Test the page. The **Register New Guest User** page should appear as follows. Note that the **Send Notification** fields shown in the illustration below appear only if you have configured the sending of SMS and/or e-mail notifications.

Figure 17 Register New Guest User Page



When a new user clicks **Submit**, his or her account is created, and the account details are sent to the specified e-mail 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:

Figure 18 Register New Device



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. If you wish to customize the look and feel of the **Register New Guest User** page, you may edit the JSP files in your self-provisioning portal application. The application resides in Tomcat's *webapps* directory. The path is: \webapps\GuestManager\portal\

   For example, a portal called ZoologyConference installed on a Windows machine will have the following path:

```
C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\GuestManager\portal\
ZoologyConference
```

6. **Important!** Tomcat must be running and Guest Manager must remain connected to the Avaya Identity Engines Ignition Server appliance at all times in order for the self-provisioning portal to operate. To connect, see "Connecting Guest Manager to the Ignition Server Appliance" on page 53.

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.

Follow the steps here to manage self-provisioned guest user accounts:

1. Run the Provisioner Application. (For instructions, see "Launching the Provisioner Application" on page 123.)
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 129 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. Follow these steps:

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, the portal provisioner is deleted.

Note! 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 such user accounts, see the instructions in "Retrieving the Guest Users Owned by a Provisioner" on page 114.)

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 17.

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.

Note: If you are a provisioner, you may skip this chapter and proceed to "Provisioner Application: Managing Guests and Devices" on page 119.



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.

Contents of This Chapter

- "Setting Up Provisioners" on page 95
  - "Creating a Provisioning Group" on page 95
  - "Creating a Provisioner in the Internal Store" on page 99
  - "Creating a Provisioner From an Account in an LDAP or AD Store" on page 102
  - "Bulk Importing Provisioner Accounts from a File" on page 102
  - "Checklist: Before Your Provisioners Start Working" on page 104
  - "Writing SMS and E-mail Templates for Account Notifications" on page 104
  - "Administrator Access to the Provisioner Application" on page 105

- "Managing Provisioners" on page 105
  - "Viewing the Internal Provisioners List" on page 106
  - "Modifying a Provisioner Account" on page 107
  - "Assigning a Provisioner to a Provisioning Group" on page 108
  - "Deleting a Provisioner Account" on page 108
  - "Changing a Provisioner's Password" on page 109
  - "Setting the Provisioner Timeout Period" on page 109
  - "Monitoring Provisioner and Guest Logins" on page 109
- "Managing Provisioning Groups" on page 110
  - "Creating a Provisioning Group" on page 95
  - "Managing Provisioning Groups" on page 110
  - "Modifying a Provisioning Group" on page 112
  - "Setting Provisioner Groups for Provisioners Stored in LDAP and AD" on page 112
- "Managing Group Memberships" on page 112
  - "Reassigning a Provisioner's Guest User Accounts and Devices to Another Provisioner" on page 112
  - "Moving Provisioners, Guests, or Devices to a New Provisioning Group" on page 112
  - "Assigning Unmanaged Guests or Devices to a Provisioner" on page 113
- "Bulk Operations on Guest Users" on page 114
  - "Retrieving the Guest Users Owned by a Provisioner" on page 114
  - "Retrieving the Guest Users That Belong to a Provisioning Group" on page 115
  - "Deleting the Guest Users of a Provisioner or Provisioning Group" on page 115
  - "Deleting Expired Guest Users" on page 115
  - "Exporting Guest User Records to a File" on page 116
- "Bulk Operations on Devices" on page 116
  - "Retrieving the Devices Owned by a Provisioner" on page 116
  - "Exporting Device Records to a File" on page 117

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.

The following sections explain how to prepare for and create provisioner accounts:

- "Creating a Provisioning Group" on page 95
- "Setting Provisioner Groups for Provisioners Stored in LDAP and AD" on page 112
- "Creating a Provisioner in the Internal Store" on page 99
- "Creating a Provisioner From an Account in an LDAP or AD Store" on page 102
- "Checklist: Before Your Provisioners Start Working" on page 104
- "Bulk Importing Provisioner Accounts from a File" on page 102
- "Writing SMS and E-mail Templates for Account Notifications" on page 104

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 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 (also known as "sponsors") that requires a unique set of rules for creating guest users. Every provisioner must belong to at least one provisioning group.

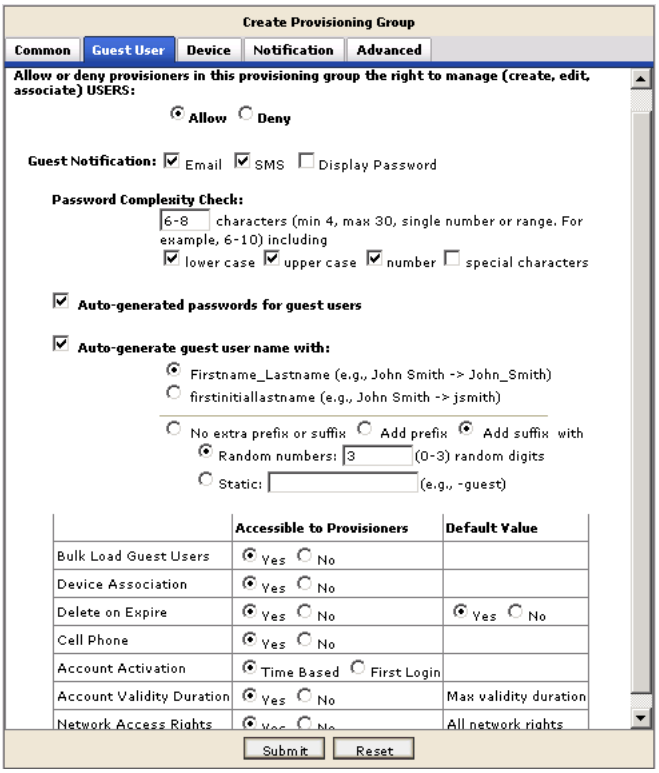
To create a provisioning group:

1. Run the Administrator Application:
   - With your Tomcat Server running and the Guest Manager application running, open a browser and navigate to the Administrator Application URL. The Guest Manager admin URL will be similar to https://pluto:8443/GuestManager/admin/ or http://pluto:8080/GuestManager/admin/ as explained on page 31.
   - Type your Guest Manager administrator username and password.
   - **Note:** 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 53.
2. Click on the **Provisioning Groups** section in the main toolbar. The **Provisioning Groups** screen appears.
3. Click on **Actions > New Provisioning Group**. In the Common tab, type a Group Name for the group.
4. If the provisioners in this group will collaborate to manage guest users, select the **Provisioners in this group can view and edit each other's records** check box under the **Common** tab. 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 tick this check box.
5. 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 typing the number of minutes, hours or days in the preceding field.
6. 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.**

   Tick 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 60”.)

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, you would tick the check boxes as follows:



7. Check the check box **Auto-generated passwords for guest users** under the Guest User tab if you want the provisioner to be able to auto-generate passwords for the guest users he or she owns.
8. In the **Guest Notification** section under the Guest User tab choose the ways that this group’s provisioners will be allowed to notify guests of their new guest accounts.
9. Select the **Auto-generate guest user name with** check box under the Guest User tab to pre-populate a guest user name and increase the likelihood that it will be unique. Use the radio buttons below the **Auto-generate guest user name with** check box to define the format of the guest user name. The default auto-generated guest user name format is: Firstname_Lastname (e.g. John Smith -> John_Smith) 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 “Tom_Jones_xxx” where “xxx” is a three digit random number.

10. .If provisioners in this group can create and edit *device records*, tick the **Allow** check box under the heading, **Allow or deny provisioners in this provisioning group the right to manage (create, edit, associate) devices** in the **device tab**. Note that if a provisioner is a member of more than one provisioning group, then he can save and edit devices only if *all* of his provisioning groups grant him this right.
11. You may elect to limit the locations from which provisioners can log into the Provisioner Application and manage users. To do this, tick the **Allow provisioner/self-service to connect from these hosts only** check box under the Advanced tab and type 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”, you will type “birne.idengines.com”.
12. In the **Time Zone** drop-down box, select a time zone.
13. In the **Idle Timeout** field under the Advanced tab, set the period of inactivity after which a provisioner's session in the Provisioner Application will automatically disconnect. After it disconnects, the provisioner must log in again. Set the threshold in minutes.

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

    Note! Idle Timeout does not set an idle timeout for *guest* user accounts — only for *provisioners*.
14. The **SMS Template** under the Notification tab is the template for the text message sent to the guest's cell phone when a provisioner saves the guest's account. For instructions on writing the SMS template, see the section, “Writing SMS and E-mail Templates for Account Notifications” on page 104
15. The **Email Template** under the Notification tab determines the contents of the confirmation e-mail sent to the guest when a provisioner saves the guest’s account. For instructions on writing the e-mail template, see the section, “Writing SMS and E-mail Templates for Account Notifications” on page 104
16. The **Additional information to be included as part of guest account confirmation page** field under the Notification tab specifies a message that is displayed on the guest account confirmation page when an account is created. The provisioner can print this confirmation and hand it to the guest.

    Note! Text you type the **Additional information** field does not appear on the e-mail confirmation sent to the user. To include a message in the confirmation e-mail to the guest, add the *$comment* variable to the

Email Template (see Step 15, above) and have your provisioners type the message in the **Comment** field when creating the guest user.

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

Next steps: Next you must assign provisioners to the provisioning group. Do one of the following:

- If your provisioners are internal provisioners, see "Assigning a Provisioner to a Provisioning Group" on page 108.
- If your provisioners are stored in LDAP or Active Directory, see "Create a Provisioner Access Policy" on page 33.

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*.

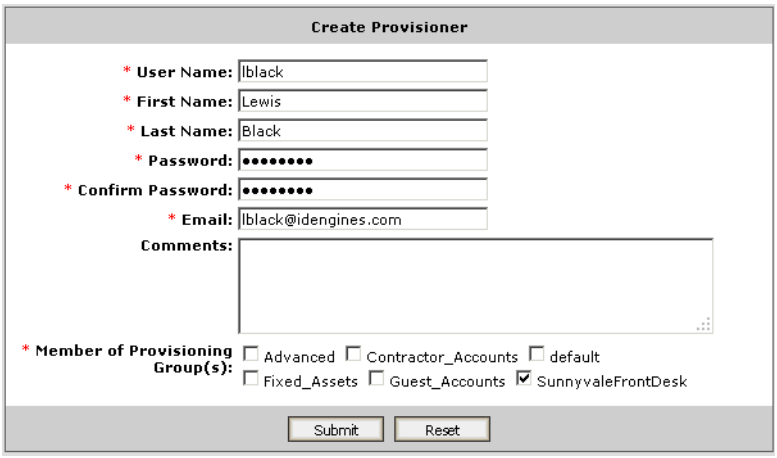
(**Note:** If you would prefer to authenticate provisioners against LDAP or AD, see "Creating a Provisioner From an Account in an LDAP or AD Store" on page 102; if you would prefer to bulk-import provisioners, see "Bulk Importing Provisioner Accounts from a File" on page 102.)

Prerequisites 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 95.

To create a provisioner account:

1. Run the Administrator Application (Note that you cannot use Ignition Dashboard for this!):
   - With your Tomcat Server running and the Guest Manager application running, open a browser and navigate to the Administrator Application URL. The URL will be similar to http://pluto:8080/GuestManager/admin as explained on page 31.
   - Type your Guest Manager administrator username and password.
   - **Note:** 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 53.
2. Click on the **Create Provisioner** section in the main toolbar. The **Internal Provisioners** screen appears. Select **Actions > New Internal Provisioner**. The Create Provisioner screen appears.

Figure 19 Create Provisioner Screen



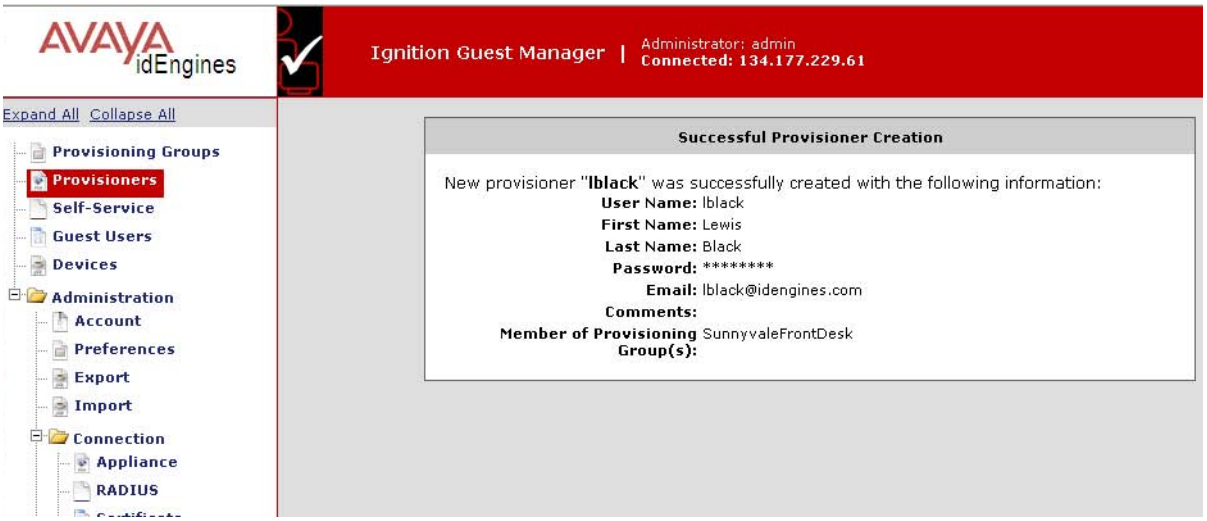
3. Set the provisioner's account details:
   - **Username, First Name,** and **Last Name:** Fill in the appropriate information for the provisioner. Only numbers and characters are allowed in the name. No spaces or periods may be used. The length of the name must be 30 characters or less.
   - **Password**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

- **E-Mail**: Enter the e-mail address of the provisioner.
- In **Comments**, type any notes you wish to make. These comments are not sent to the provisioner.

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

   Note: 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.

Figure 20 Successful Creation of a Provisioner



6. Notify the provisioner of his or her new provisioner username and password, and give him or her the URL of the provisioner application, which is

```
http://<Guest Manager machine>:8080/GuestManager/provisioner/
```

or

```
https://<Guest Manager machine>:8443/GuestManager/provisioner/
```

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

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

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 "Create a Provisioner Access Policy" on page 33 or "Create an Advanced Provisioner Access Policy" on page 36 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.

Note! 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 102.

Procedure: Use these steps to bulk-import provisioner accounts:

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.

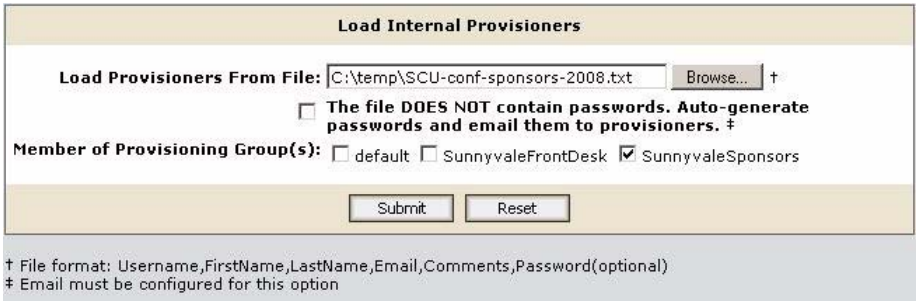
   For example, a file containing the following lines would create three provisioners:

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

Warning! 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** to select it.
5. If you wish to import passwords from the file, un-tick the "**File DOES NOT contain passwords**" check box. With this check box ticked, Guest Manager automatically chooses a password for each provisioner you import.
6. In the **Member of Provisioning Group(s)** section, tick 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** button 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 56.

Troubleshooting: If errors occur, see "Problem: Errors Reported During Bulk Saves and Deletes" on page 141.

Checklist: Before Your Provisioners Start Working

Before you 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 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 e-mail notifications to new guest users. See "Set Up E-Mail Notification Parameters" on page 46. If desired, make sure you have configured Guest Manager to send SMS messages. See "Set Up SMS Notification Parameters" on page 47.

Next Steps If you have created your guest authorization policies and set up your provisioner accounts, you should now train the provisioners in using the Guest Manager Provisioner Application. As the basis for this training, use Chapter , "Provisioner Application: Managing Guests and Devices".

Writing SMS and E-mail 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 e-mail, 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 e-mail templates. To edit these templates, do the following:

Prerequisite: Make sure you have set up your e-mail and/or SMS gateways as shown in "Set Up E-Mail Notification Parameters" on page 46 and "Set Up SMS Notification Parameters" on page 47.

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** 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 e-mails, 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 you policies), you must have a *provisioner account* for your own use.

Managing Provisioners

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

- "Creating a Provisioner in the Internal Store" on page 99
- "Viewing the Internal Provisioners List" on page 106
- "Modifying a Provisioner Account" on page 107
- "Assigning a Provisioner to a Provisioning Group" on page 108
- "Deleting a Provisioner Account" on page 108
- "Retrieving the Guest Users Owned by a Provisioner" on page 114

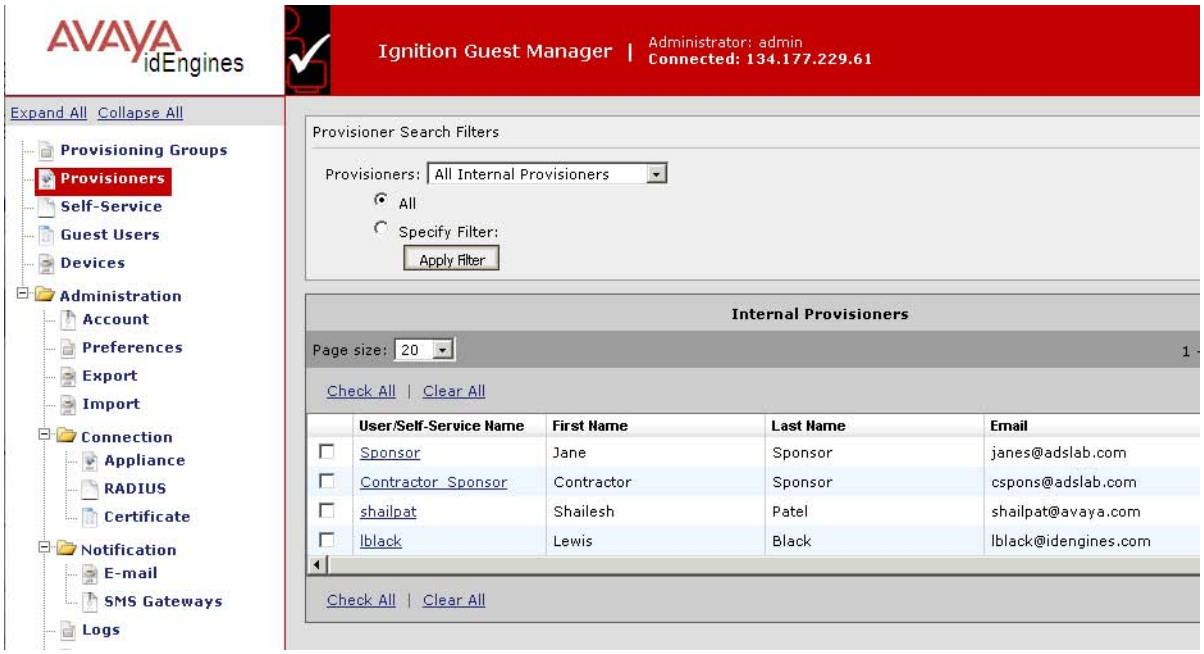
- "Changing a Provisioner's Password" on page 109
- "Setting the Provisioner Timeout Period" on page 109

Your site may also use provisioner accounts that are stored externally in your corporate LDAP or Active Directory store. You cannot edit such users in Guest Manager, but you can set up rules that place them in the appropriate provisioning groups. See "Create a Provisioner Access Policy" on page 33 for details.

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.

Figure 21 Internal Provisioners List



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

- a check box to select the row containing the provisioner account data
- the **User/Self-Service,** which is the active link to the details of that 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 de-select 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 108.
- **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 115.
- **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 116.
- **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 117.

Modifying a Provisioner Account

In order to modify an existing internal provisioner account,

1. Click the **Provisioners** button 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.
4. 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 99 for an explanation of each field. 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.

Note: This procedure works only for *internal provisioners* stored in Ignition. If your provisioners are stored in LDAP or AD, turn instead to "Create a Provisioner Access Policy" on page 33.

Procedure:

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

Deleting a Provisioner Account

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

Note! 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.

In order to delete a provisioner account:

1. Run the Guest Manager Administrator Application.
2. Click the **Provisioners** button. The Internal Provisioners screen appears (Figure 21).
3. 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 112.
4. In the Provisioners window, tick the check box of the provisioner account(s) you wish to delete.
5. 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:

1. Run the Guest Manager Administrator Application.
2. Click the **Provisioners** button.
3. Click the **User/Self-Service Name** of the provisioner whose password you wish to change. The Edit Provisioner window appears.
4. Type the new password in the **Password** field.
5. Retype the password in the **Confirm Password** field.
6. Click **Submit**.

Setting the Provisioner Timeout Period

See "Provisioner Idle Timeout Threshold" on page 55.

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:

1. Run Ignition Dashboard (see page 142) 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 “Access Record Details” in the *Avaya Identity Engines Ignition Server Administration Guide* for more information.

You can filter the set of records. See “Filtering Your View of the Logs” in the *Avaya Identity Engines Ignition Server Administration Guide*.

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:

- “Creating a Provisioning Group” on page 95
- “Managing Provisioning Groups” on page 110
- “Modifying a Provisioning Group” on page 112
- “Setting Provisioner Groups for Provisioners Stored in LDAP and AD” on page 112

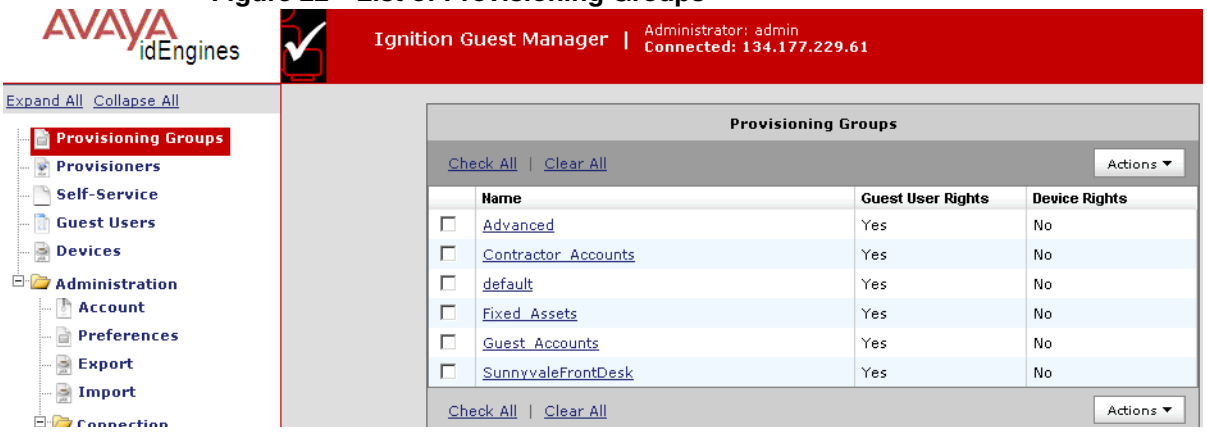
Creating a Provisioning Group

See “Creating a Provisioning Group” on page 95.

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.

Figure 22 List of Provisioning Groups



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 115.
- **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 116.
- **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

In order to modify an existing provisioning group:

1. Click the **Provisioning Groups** button in the main toolbar of the Administrator Application.
2. In the table, click the name of the provisioning group you wish to modify.
3. In the Edit Provisioning Group window, make you 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 up as shown in "Create a Provisioner Access Policy" on page 33 or "Create an Advanced Provisioner Access Policy" on page 36.

Managing Group Memberships

Reassigning a Provisioner's Guest User Accounts and Devices to Another Provisioner

1. Run the Guest Manager Administrator Application.
2. Click the **Provisioning Groups** button.
3. Click the name of the provisioning group of the provisioner whose guests and/or devices you wish to reassign.
4. Click **Actions: Reassign Provisioning Group Membership**.
5. In the *middle part* of the window, tick the check box, "**Reassign members of**."



6. Tick the **Guest Users** and/or **Devices** check boxes, as applicable.
7. In the "**being managed by provisioner**" field, type the name of the provisioner who currently owns the users or device records.
8. In the "**to provisioner**" field, type the name of the provisioner to whom you will assign the users or device records.
9. Click **Submit**.

Moving Provisioners, Guests, or Devices to a New Provisioning Group

1. Run the Guest Manager Administrator Application.

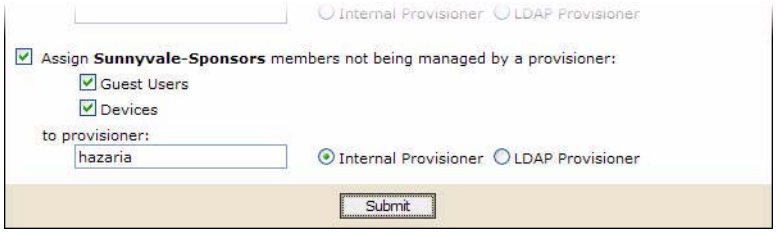
2. Click the **Provisioning Groups** button.
3. Click the name of the provisioning group whose provisioners, guests, or devices you wish to reassign.
4. Click **Actions: Reassign Provisioning Group Membership**.
5. In the *top part* of the window, tick the check box, "**Reassign members of**."



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

Assigning Unmanaged Guests or Devices to a Provisioner

1. Run the Guest Manager Administrator Application.
2. Click the **Provisioning Groups** button.
3. Click 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.
4. Click **Actions: Reassign Provisioning Group Membership**.
5. In the *bottom part* of the window, tick the check box, "**Assign <GROUP> members no being managed by a provisioner**" (where "<GROUP>" is the provisioning group name.)



6. Tick the **Guest Users** and/or **Devices** check boxes, as applicable.

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**.

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.

This section explains the most common bulk operations:

- "Retrieving the Guest Users Owned by a Provisioner" on page 114
- "Deleting the Guest Users of a Provisioner or Provisioning Group" on page 115
- "Deleting Expired Guest Users" on page 115
- "Exporting Guest User Records to a File" on page 116

Retrieving the Guest Users Owned by a Provisioner

In order to find the guest user accounts that are owned by a provisioner:

1. Run the Guest Manager Administrator Application.
2. Click the Guest Users button. This will show all Guest users provisioned in the system. Use Specify Filter select Provisioner from drop down menu in select filter, enter operation (Start with, Equal, Not Equal) and the name of the Provisioner, click Apply Filter. A list of Guest Users provisioned by the selected Provisioner will appear click the check box for the user that needs to be deleted, click Delete (Figure 21).

Figure 23 Guest user accounts, as the Guest Manager administrator sees them



Retrieving the Guest Users That Belong to a Provisioning Group

In order to find the guest user accounts that belong to a particular provisioning group:

1. Run the Guest Manager Administrator Application.
2. Click the Guest Users button. This will show all Guest users provisioned in the system. Use Specify Filter select Provisioning Group from drop down menu and select one of group listed under drop down menu of provisioning groups, click Apply Filter. A list of Guest Users provisioned by the selected provisioning group will appear(Figure 22).

Figure 24 Guest user accounts, as the Guest Manager administrator sees them



Deleting the Guest Users of a Provisioner or Provisioning Group

In order to delete a provisioner's guest user accounts:

1. Load the users as explained in "Retrieving the Guest Users Owned by a Provisioner" on page 114 or as explained in "Retrieving the Guest Users That Belong to a Provisioning Group" on page 115.
2. Tick 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

In order to delete expired guest user accounts:

1. Run the Guest Manager Administrator Application.
2. Click the **Provisioners** button. The Internal Provisioners screen appears (Figure 21).

3. Click the check box(es) of the provisioner(s) whose expired guest users you wish to delete.
4. 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

In order to export guest user accounts to a CSV file:

1. Run the Guest Manager Administrator Application.
2. Click the **Provisioners** button. The Provisioners screen appears (Figure 21).
3. Select the Export Devices from **Action** button.
4. Use your browser's **Save** command 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" on page 116
- "Exporting Device Records to a File" on page 117

Retrieving the Devices Owned by a Provisioner

In order to find the device accounts that are owned by a provisioner:

1. Run the Guest Manager Administrator Application.
2. Click the Devices button. This will show all Devices provisioned in the system.
3. Use Specify Filter select Provisioner from drop down menu in select filter, enter operation (Start with, Equal, Not Equal) and the name of the Provisioner, click Apply Filter. A list of Devices provisioned by the selected Provisioner will appear.

Retrieving the Devices Owned by a Provisioning Group

In order to find the device accounts are owned by a Provisioning Group

1. Run the Guest Manager Administrator Application
2. Click the Devices button. This will show all Devices provisioned in the system.

3. Use Specify Filter select Provisioning Group from drop down menu and select one of group listed under drop down menu of provisioning groups, click Apply Filter. A list of Devices provisioned by the selected provisioning group will appear.

Exporting Device Records to a File

In order to export device accounts to a CSV file:

1. Run the Guest Manager Administrator Application.
2. Click the **Provisioners** button. The Provisioners screen appears.
3. Click the check box(es) of the provisioner(s) whose devices you wish to export.
4. Select the Export Devices from Action button.
5. Use your browser's **Save** command to save the file.

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.

Contents of this Chapter

- "Introduction to Guest User Accounts" on page 120
  - "What Limits You Can Set on a Guest User Account" on page 120
  - "Guest User Account Validity Period" on page 122
  - "Guest User Account Attributes" on page 120
  - "How a Guest User Logs In" on page 123
- "Launching the Provisioner Application" on page 123
  - "Failed Connection" on page 124
  - "Application Timeout" on page 124
  - "Main Page of the Provisioner Application" on page 124
- "Managing Guests" on page 124
  - "Creating Guest User Accounts" on page 125
  - "Bulk Importing Guest User Accounts from a File" on page 126
  - "Sending Guest Account Notifications" on page 129
  - "Viewing Guest User Accounts" on page 129
  - "Finding Guest User Accounts" on page 131
  - "Modifying Guest User Accounts" on page 131
  - "Checking the Validity of Guest User Accounts" on page 133
  - "Printing Guest User Account Details" on page 133

- "Renewing a Guest User Account" on page 134
- "Deleting Guest User Accounts" on page 134

- "Managing Devices" on page 134
  - "Creating a Device Record" on page 134
  - "Bulk Importing Device Records from a File" on page 135
  - "Assigning a Device to a Guest User" on page 137

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 17.)

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.

Table 1 The Attributes of a Guest User Account

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. When the page opens, this field contains a unique default user name. If you need to quickly create many guest accounts, then you can use the default name. Otherwise, you can replace it with a name of your choice.
Password	Click the label, "**Change**", to edit the password. *If the provisioning group does not allow the editing of passwords*, the **Change** label does not appear. In this case a password is generated by the Guest Manager application.
Email	E-mail 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 E-Mail Notification to**" 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 e-mailed to the guest user. See "Writing SMS and E-mail Templates for Account Notifications" on page 104.
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. **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.
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 dropdown list. See "Guest User Account Validity Period" on page 122 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."
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.

Table 1 The Attributes of a Guest User Account

Field	Description
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."
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 to assign the device to the user you are editing.
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 e-mail or via SMS messaging. See "Sending Guest Account Notifications" on page 129 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.



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 the Validity of Guest User Accounts" on page 133 and
- "Renewing a Guest User Account" on page 134

How a Guest User Logs In

Once you've given the guest his or her temporary user name and password, how does he or she log in? Typically, the guest will 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

To begin using the Provisioner Application:

1. Open your web browser and type the URL of the Provisioner Application, which is

```
http://<Guest Manager machine>:8080/GuestManager/provisioner/
```

   or

```
https://<Guest Manager machine>:8443/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 **Sign In**. If your login attempt succeeds, the following window 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.

If your login attempt fails, see "Problem: Provisioner Can't Log In" on page 139.

Failed Connection

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

Figure 25 Example of a Failed Connection into Guest Manager



If this happens, contact your Guest Manager Administrator and ask him or her to reconnect Guest Manager to the Ignition Server. (See “Make SOAP Settings in Guest Manager” on page 42.)

Application Timeout

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:

Figure 26 Main Page of the Provisioner Application



Managing Guests

See the following sections for instructions:

- “Creating Guest User Accounts” on page 125
- “Bulk Importing Guest User Accounts from a File” on page 126
- “Sending Guest Account Notifications” on page 129
- “Viewing Guest User Accounts” on page 129
- “Modifying Guest User Accounts” on page 131
- “Checking the Validity of Guest User Accounts” on page 133

- "Printing Guest User Account Details" on page 133
- "Renewing a Guest User Account" on page 134
- "Deleting Guest User Accounts" on page 134

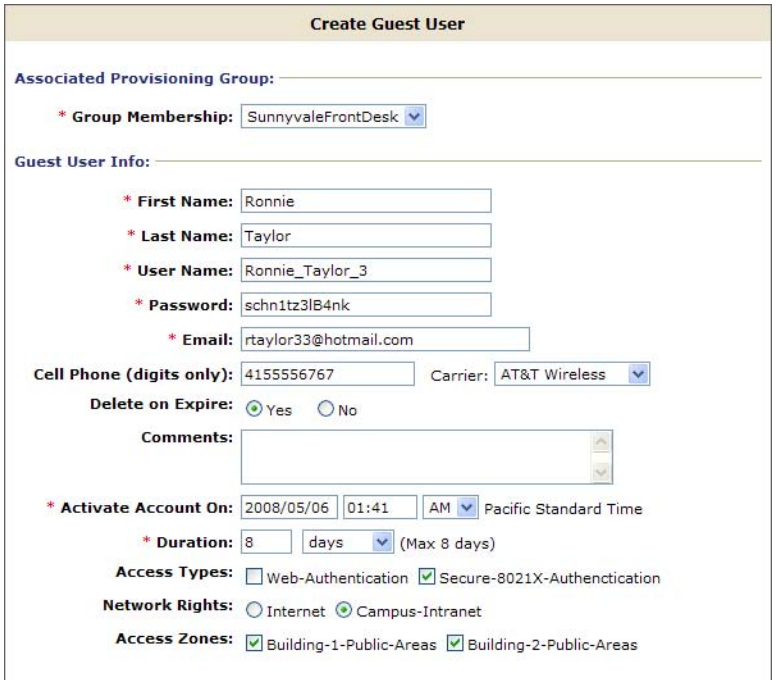
Creating Guest User Accounts

Note: If you want to create many accounts at once, you may want to use the "**Load Guest Users**" command, instead, as explained on page 126. Device management is only available if all provisioning groups the provisioner is a member of have this privilege enabled.

To create a guest user account, use the steps below:

1. Log in to the Provisioner **Application**. (See "Launching the Provisioner Application" on page 123.)
2. Click the **Guest Users > New** button in the toolbar on the main page of the Provisioner Application. (See Figure 26.)

Figure 27 Example of a Completed Create Guest User Form



3. In the **Create Guest User** screen, provide the account details. Do the following:
   - In the **Group Membership** dropdown list, choose the provisioning group this guest will belong to. Each provisioning group imposes certain account guidelines (max. validity period, allowable access zones, and so on), so the fields and defaults of the window may change after you choose a provisioning group.

- Type the user's **First Name** and **Last Name**. The window creates a default user name that you can edit. The user name must be unique before you can save the user.
- Depending on the rules of the provisioning group, you may be able to edit the user's **Password**.
- See Table 1 for an explanation of the rest of the fields.
- To reset the fields to their default values, click **Reset**.
- **Hint:** If you have login instructions for the user, type them in the **Comments** field. Later when you send the user a notification e-mail, or print the user's login information sheet, the comments will be included.

4. Click **Submit**. The Guest Manager application creates the guest user account and e-mails notifications to the people you specified in the **Send Notifications** section. See "Sending Guest Account Notifications" on page 129 for details.Guest Manager displays the **Successful Guest Creation** page to confirm the account was saved.
5. If you like, you may 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 123.

To view the guest user you created, click the **Users > View** button 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:

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,Password
     ```

   - *If you do not wish to import passwords,* then Guest Manager will generate a password for each user. Format the file 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 guest users:

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

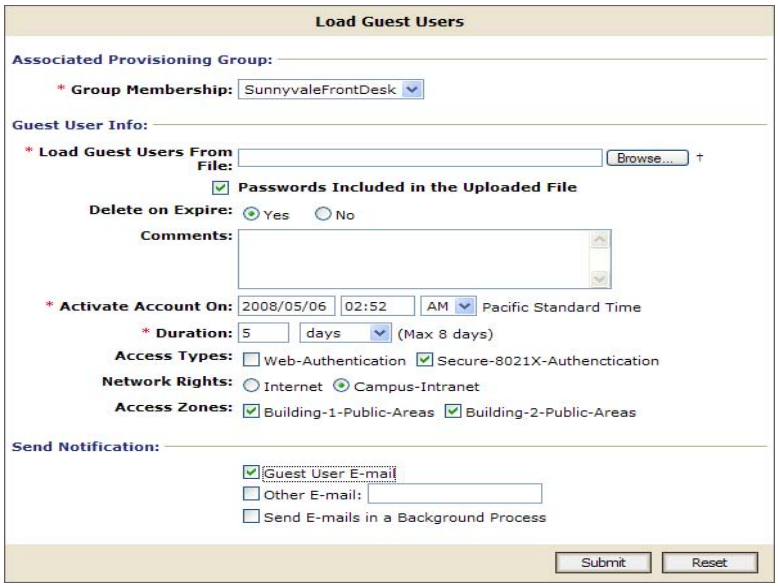


Important! Please observe the following guidelines when bulk loading guest users:

- 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. (See page 31 for the 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** dropdown 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. If you wish to import passwords from the file, tick the **Use Passwords Included in the Uploaded File** check box. *Note! 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 dropdown 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 e-mail the new user names and passwords to your desired recipients:
   - Tick **Guest User E-mail** to send each user his or her username and password. One e-mail will be sent per guest user, and it will be sent to the guest's e-mail address provided in the CSV file.
   - If you wish to send a notification e-mail to an additional address, tick the **Other E-mail** check box and provide an e-mail address or a comma-separated list of e-mail addresses. Send notifications only to people who you trust with the guest user password. One e-mail 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, you may view them by clicking Guest **Users > View** button in the command bar on the left of the window. 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 56.

Troubleshooting: If errors occur, see "Problem: Errors Reported During Bulk Saves and Deletes" on page 141.

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 e-mail has the format of the e-mail 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 "Set Up E-Mail Notification Parameters" on page 46 and "Set Up SMS Notification Parameters" on page 47.

To send a notification:

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 E-mail** sends the guest an e-mail with his account details. Only the fields specified in the guest's provisioning group's **Email template** are sent.
   - **Other E-mail** 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 ticked.

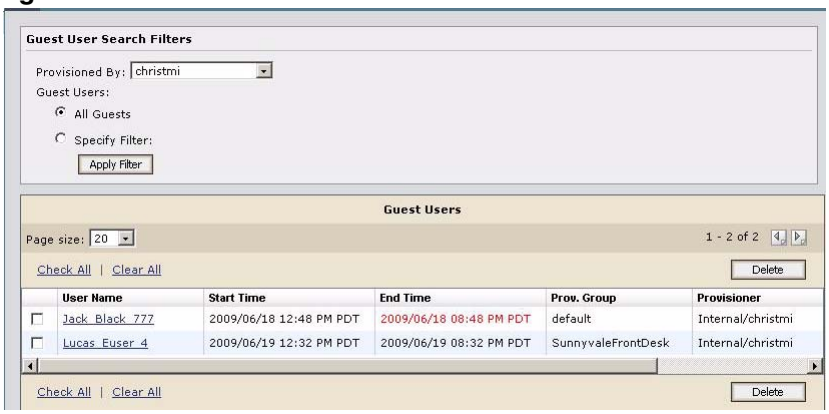
To set up your templates, see "Writing SMS and E-mail Templates for Account Notifications" on page 104.

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. (But note that the Guest Manager Administrator can use the Administrator Application to view all guest users.)

Figure 28 Guest Users Screen



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** and **E-mail** address (The password is visible only if the Guest Manager Administrator has given you permission to view it.)
- 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.
- **Provisioning Group and Provisioner**

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.

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 20, 30, 40, 50, 60, 70, 80, 90, or 100. To do so, select the page size from the dropdown 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 link 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, Password etc.) 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 Accounts

To find a guest user account,

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 (as shown above in Figure 22).
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**.

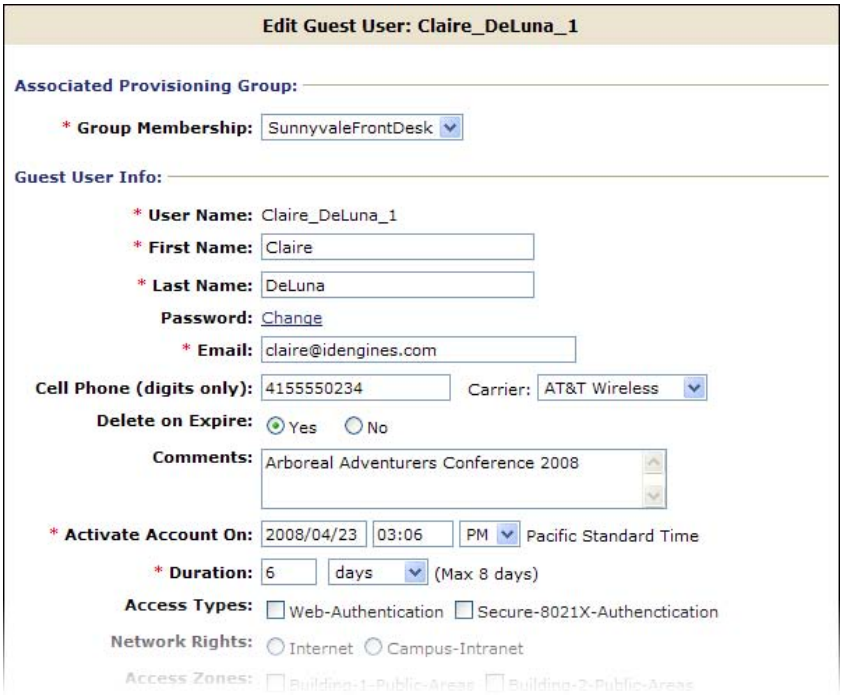
Modifying Guest User Accounts

In order to modify an existing guest user account,

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 (as shown above in Figure 22).
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.

For example, clicking on **apuser4** in Figure 22 displays the following:

Figure 29 Edit a Guest User Account



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

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 e-mails notifications to the people that you specified in the **Send Notifications** section. See "Sending Guest Account Notifications" on page 129 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. If you like, you may 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 the Validity of Guest User Accounts

To check the validity of guest user accounts:

1. Run the Provisioner Application.
2. Click **Guest Users > View** in the command bar 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:



Red text indicates the account is expired.

Red text indicates an account start time in the future. The account will become usable at the start time.

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" below.

Printing Guest User Account Details

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

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. To renew an expired account:

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. To delete one or more existing guest user accounts:

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 (Figure 22).
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

See the following sections for instructions:

- “Creating a Device Record” on page 134
- “Bulk Importing Device Records from a File” on page 135
- “Assigning a Device to a Guest User” on page 137

Note: Device management is only permitted if your provisioning group allows it. If you are a member of more than one provisioning group, then you can only edit devices if *all of your provisioning groups* are set to allow device management.

Creating a Device Record

Ignition Server can enforce rules that allow a guest to connect *only using his or her own device*. (See “Example Device” on page 21 for details.) To create a device record, use the steps below.

Note: If you wish to create many device record at once, you may wish to use the “Load Devices” command, instead.

1. Log in to the Provisioner **Application**. (See “Launching the Provisioner Application” on page 123.)
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 w group or user.
5. In the **Type** dropdown 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, tick the **Record Enabled: No** check box.
7. Specify whether this is a temporary device. Do one of:
   - 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. Refer to Table 1 for an explanation of each field.
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 the Devices > View button from the main toolbar of the Provisioner Application.

To assign the device to a user, see “Assigning a Device to a Guest User” on page 137.

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,VLAN Label,VLAN ID,Attribute 1,
   Attribute 2,Attribute 3,Attribute 4,Attribute 5,
   Attribute 6,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! Please 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. (See page 31 for the URL.)
   - Type your provisioner **Username** and **Password**.
3. In the toolbar on the left, click **Devices > Load**. The Load Devices screen appears.
4. In the **Group Membership** dropdown 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, tick 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:
   - 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, click the **Delete on Expire: Yes** button.

9. Specify where and how the device can be used by clicking the appropriate **Access Type**, **Network Rights**, and **Access Zone** check boxes. Refer to Table 1 for an explanation of each field.
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** button in the command bar 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 56.

Troubleshooting: If errors occur, see "Problem: Errors Reported During Bulk Saves and Deletes" on page 141.

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 "Example Device" on page 21 for details.) To assign a device to a guest user account:

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 (as shown above in Figure 22).
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's not there, see "Creating a Device Record" on page 134.) Click the check box of the desired device and click **Add Devices to User**.
5. In the Edit Guest User screen, click **Submit**.

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.

Contents of this Chapter

- "Problem: Provisioner Can't Log In" on page 139
- "Problem: Connection to Appliance Fails" on page 139
- "Problem: Installer Gives Errors and Warnings" on page 140
- "Problem: Not Sure Whether Tomcat is Running" on page 140
- "Problem: Errors Reported During Bulk Saves and Deletes" on page 141
- "Problem: No Log File Displayed" on page 141
- "Launching Ignition Dashboard" on page 142

Problem: Provisioner Can't Log In

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 shared secret of your Guest Manager host machine. Follow the steps in "Make RADIUS Settings on the Ignition Server" on page 44 and follow the steps in "Make RADIUS Settings in Guest Manager" on page 45.

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

When you restart the Guest Manager application (anytime you restart the Tomcat server), 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 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 page 142), connect to the appliance, click on **Configuration** tab, select the site, click on Services tab, click your node, and click the **SOAP** tab. See page 40 for details.
- Check that the correct admin root certificate has been installed in Guest Manager. See "Install the SOAP Certificate" on page 39.
- Check that your Tomcat keystore is set up correctly. If your Guest Manager application runs on an HTTPS-enabled Tomcat server, or if your browser warns you that the server certificate has expired, you may need to update your Tomcat keystore configuration. See "Set Up Tomcat to Require HTTPS Connections" on page 25.

Problem: Installer Gives Errors and Warnings

The Guest Manager installer writes its error log to

```
<Tomcat Installation>\webapps\Ignition_Guest_Manager_[version]_InstallLog.xml
```

where "[version]" is your Ignition Server version number. Typically, this path looks similar to

```
C:\Program Files\Apache Software Foundation\Tomcat
6.0\webapps\Ignition_Guest_Manager_7.x.x_InstallLog.xml.
```

You may ignore most warnings. If an error occurs, contact your Avaya support representative, and provide your representative with a copy of the `Ignition_Guest_Manager_[version]_InstallLog.xml` file.

Problem: Not Sure Whether Tomcat is Running

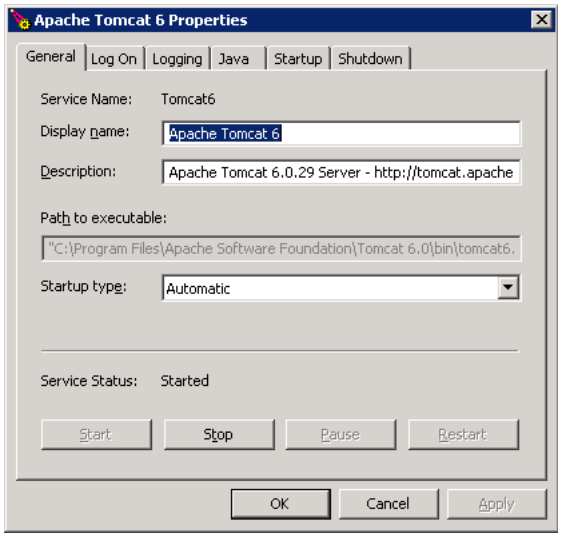
To find out whether Tomcat is running, open the Apache Tomcat Properties General window and look for the Service Status field. In Windows, you can launch this by clicking **Start: Programs: Apache Tomcat 6.0:**

Configure Tomcat. If the **Start** menu fails to launch the window, look in the system tray for an icon that looks like the one shown below. Double-click it to open the Properties window.



Tomcat icon in the Windows system tray

In the Apache Tomcat Properties General screen, the Service Status field indicates whether the Tomcat Server is running.



You can also check the Windows Task Manager to verify that Tomcat is running. In the Task Manager, click on the Processes tab and look for `tomcat6.exe` in the processes list.

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: No Log File Displayed

If the administrator's **View Log Files** fails to display log messages, make sure the path in *log4j.properties* is an absolute path. See "Changing the Default Location of the Log File" on page 57.

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.

To launch Ignition Dashboard:

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*.

Index

A

access constraint checkboxes, 60
  example illustration, 21
  explained, 60
  missing, 63
access constraint class
  assigning to a user, 121
  setting up, 66
access policy
  example, 68
  for provisioner stored in LDAP or AD, 33
Access Type, 60
  assigning to a user, 121
  example, 76
  setting up, 66
Access Zone, 60
  assigning to a user, 121
  example, 76
  setting up, 66
account
  location of user accounts, 17
account types, 17, 29
Active Directory
  provisioner accounts stored in, 33
admin
  default password, 30
administrator
  Guest Manager Administrator, defined, 17
  Guest Manager Administrator, set-up, 54
  Ignition Server Administrator, 18
  logging in to application, 32, 51
  login, 54
  password, 54
  provisioner, 18
  role, 19
  SOAP API user, 18, 30
  Tomcat admin, 18, 25, 30
  types of, 17
  types of admin credentials, 29
  types of administrators, 17
Administrator application, 17
  launching, 51
administrator session timeout, 55
Apache Tomcat
  starting and stopping, 30
  version, 24

appliance
connecting to, 53
troubleshooting, 139
appliance port for Guest Manager, 41
application, 17
launching Administrator application, 51
launching Guest Manager for the first time, 31
launching Provisioner application, 123
list of, 17
application server
troubleshooting, 140
application URL, 31
arrow, 16
asset, 134
asset correlation, 21
audit provisioners, 109
authentication of provisioner, 44
LDAP or AD, 33
troubleshooting, 139
authentication policy, 69
authorization policy, 60
autodelete, 121

B

bold, 16
bulk delete, 115
bulk import, 126
devices, 135
guest users, 126
provisioners, 102

C

caution, 16
cell phone notifications, 129
certificate
errors, 25
PEM-encoded, 39
SOAP root, 39
change password, 54
check
connection, 43
client timeout
SOAP client timeout, 42
components, 17
account types, 17
Guest Manager Administrator application, 51
Guest Manager Provisioner application, 123
list of, 17
confirmation of account creation, 129
connect
connect Guest Manager, 53
connect Guest Manager for the first time, 42
disconnect from Ignition Server, 53
provisioner login fails, 139
troubleshooting, 139

connection
check, 43
create
guest user, 125
provisioner, 99
Create Guest User screen
customizing, 60
using, 125
creating and managing provisioners, 93 to 104

D

database
location of user accounts, 17
default login, 54
Delete on Expire, 121
delete users upon account expiry, 121
device, 134
assign to user, 137
creating, 134
creating in bulk, 135
exporting device accounts to a file, 117
finding devices owned by a provisioner, 116
how the admin finds device accounts, 116
importing device records from a file, 135
permission to save/edit devices, 98
policies for, 21
device record, 134
directory
location of user accounts, 17
directory set
defined, 65
disconnect, 53

E

e-mail confirmation, 129
e-mail set-up, 46
e-mail template, 104
e-mailing password, 129
example policy, 76
expired account, 134
automatic deletion of, 121

F

failover of appliance connection, 41
firewall requirements, 44

G

gateway, 47
creating, 47
deleting, 55
template for, 104
glossary of terms, 17
group type
assigning to a user, 121

example illustration, 21
explained, 60
setting, 66
Guest Manager
Administrator application, 17
connecting, 53
launching Administrator application, 51
launching application for the first time, 31
launching Provisioner application, 123
Provisioner application, 17
software installation, 23 to 27
starting, 31
starting and restarting, 52
URL, 31
version, 24
Guest Manager Servers, 44
guest user, 119 to 134
assign device to user, 137
attributes of a user, 120
checking validity of account, 133
creating, 125
creating in bulk, 126
defined, 18
deleting expired users, 115
deleting upon account expiry, 121
deleting users owned by a provisioner, 115
deleting (as provisioner), 134
device, 137
editing, 131
exporting to a file, 116
finding a guest user account, 131
finding guest users in a provisioning group, 115
finding users owned by a provisioner, 114
how a provisioner finds guest user accounts, 129
how the admin finds guest user accounts, 114
importing user accounts from a file, 126
limit to login with own laptop only, 21
log in, how to, 123
ownership of guest user accounts, 95, 130
printing user account details, 133
renewing an expired account, 134
guest VLAN, 74

H

HA, 41
high availability, 41
how a guest user logs in, 123
HTTPS set-up, 25

I

Ignition Server
authenticating against, 44
connecting for the first time, 42
connecting to, 53
importing

device records, 135
guest user accounts, 126
provisioner accounts, 102
root certificate, 39
install, 23
errors and warnings, 140
installation requirements, 23
internal group, 64
italics, 16

J

Java 2 Platform Standard Edition Runtime Environment. See JRE
java.net.SocketTimeoutException, 141
JRE
version, 24

L

laptop, 134
launching the application, 51
Administrator application, 51
Provisioner application, 123
LDAP
provisioner accounts stored in, 33
location of user accounts, 17
log files, 56 to 58
logging: Provisioner login attempts, 109
login, 51
admin login credentials, 54
audit log, 109
connecting to Ignition Server, 53
e-mailing credentials to a guest, 129
fails for provisioner, 139
how a guest logs in, 123
how to log in as admin, 51
how to log in as provisioner, 123

M

manage appliance, 51 to 54
manage configuration, 53 to 54
messaging gateway, 47
creating, 47
deleting, 55
messaging template, 104
mobile phone notifications, 129
monitor
connection, 43
MTL server timeout, 141

N

network requirements for Guest Manager, 44
Network Rights, 60
assigning to a user, 121
example, 76
setting up, 66

note, 16
notification, 129
e-mail set-up, 46
SMS set-up, 47
template, 104

P

password, 29
admin, default, 30
admin, setting, 54
e-mailing, 129
provisioner, setting, 109
sending via SMS or e-mail, 129
SOAP API, 41
Tomcat admin, 25
PEM-encoded, 39
permissions
for provisioner stored in LDAP or AD, 33
policy example, 76
port
appliance port for Guest Manager, 41
print account details, 133
provisioner, 18, 93 to 104
access policy, 33
access policy, advanced, 36
AD account for, 33
authenticating, 44
authenticating against LDAP or AD, 33
authentication log, 109
can’t log in, 139
creating, 99
creating in bulk, 102
defined, 18
deleting, 108
editing a provisioner account, 107
finding devices owned by a provisioner, 116
finding users owned by a provisioner, 114
how to log in, 123
importing provisioner accounts from a file, 102
internal account for, 99
LDAP account for, 33
logging, 109
password, 109
role, 19, 95
session timeout, 98
viewing the list of provisioners, 106
Provisioner Access Policy, 33
advanced, 36
Provisioner application, 17
launching, 123
provisioning group, 95
creating, 95
finding guest users in a provisioning group, 115

R

RADIUS access policy
example, 68
RADIUS configuration for Guest Manager, 44
read timeout, 141
renew account, 134
restart Guest Manager, 52
restore account, 134
rights for provisioner stored in LDAP or AD, 33
roles, 17, 29
root certificate
importing, 39
purpose, 39
running the application, 51
Administrator application, 51
Provisioner application, 123

S

search for users, 131
self-provisioning portal, 85
creating, 85
deploying, 89
RADIUS-GM configuration and, 45
removing, 91
users created in a portal, 90
server certificate expired, 25
server connection
checking, 43
service category, 68
authentication settings, 69
defined, 65
example, 68
session timeout, 55
Guest Manager administrator, 55
Guest Manager provisioner, 98
SOAP client timeout, 42
SOAP-MTL server timeout, 141
SMS gateway, 47
creating, 47
deleting, 55
SMS password notification, 129
SMS set-up, 47
SMS template, 104
SOAP
certificate for, 39
client timeout, 42
HA mode for SOAP port, 41
MTL server timeout, 141
password, 41
user account for, 18, 30
SOAP-MTL server timeout, 141
socket timeout, 141
software installation
application versions, 24
Guest Manager, 23 to 27

requirements, 23
sponsor: See provisioner.
SSL
troubleshooting, 25
SSL set-up, 25
start
Guest Manager, 31
start Guest Manager, 52
starting the application, 51
Administrator application, 51
Provisioner application, 123
system platform requirements, 23

T

template, 104
terms explained, 17
test message of password, 129
timeout, 55
administrator session timeout, 55
provisioner session timeout, 98
settings, 55
SOAP client timeout, 42
SOAP-MTL server timeout, 141
SocketTimeoutException, 141
tip, 16
Tomcat
starting Tomcat, 30
troubleshooting, 140
troubleshooting, 139
Trusted Certificates window, 40

U

UDP traffic, 44
URL for Guest Manager, 31
user
See guest user, provisioner, or administrator
finding a guest user account, 131
location of user accounts, 17
self-provisioned user account, 90
types of, 17

V

version, 24
Ignition version, 23
VIP, 41
virtual attribute
adding to a policy rule, 37
virtual group, 64
VLAN, 62
example, 74

W

warning, 16
web address of app, 31

Website Certified by Unknown Authority, 25