



Identity Engines Guest & IoT Manager Configuration

Release 9.4
NN47280-501
Issue 10.01
November 2017

© 2017, Extreme Networks, Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU

REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS, INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND EXTREME NETWORKS, INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE ("EXTREME NETWORKS").

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

License type(s)

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part,

including any code and software unless expressly authorized by Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Service Provider

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

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR

THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Compliance with Laws

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

Preventing Toll Fraud

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

Security Vulnerabilities

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

Downloading Documentation

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

Contact Extreme Networks Support

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Extreme Networks are the registered or unregistered Marks of Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

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

For additional information on Extreme Networks trademarks, please see: <http://www.extremenetworks.com/company/legal/>

Contents

Chapter 1: Preface	11
Purpose.....	11
Training.....	11
Providing Feedback to Us.....	11
Getting Help.....	12
Extreme Networks Documentation.....	13
Subscribing to service notifications.....	13
Chapter 2: New in this Document	14
Chapter 3: Guest and IoT Manager Introduction	16
Guest and IoT Manager application in context.....	16
Types of accounts in your Ignition Server installation.....	16
The Guest and IoT Manager administrator role.....	18
Provisioners role.....	18
Guest users.....	18
Guest user example.....	19
Device example.....	20
Chapter 4: Installing Guest and IoT Manager	22
System requirements.....	22
Ignition Server compatibility.....	22
VMware ESXi server requirements.....	22
Network configuration for Guest and IoT Manager-based authentication.....	25
Installing the Guest and IoT Manager virtual appliance.....	25
Configuring the Guest and IoT Manager virtual appliance.....	33
Configure HTTPS connections.....	34
Configuring HTTPS access.....	35
Chapter 5: Configuring Guest and IoT Manager	36
Command Line Interface.....	36
certificate.....	37
show certificates.....	38
dns.....	38
show dns.....	39
httpd.....	39
show httpd.....	40
interface.....	41
show interface.....	42
route.....	42
show route.....	42
ping.....	43
sshd.....	43

tomcat.....	44
clear.....	45
help.....	45
About usernames and passwords.....	46
Launching Guest and IoT Manager	47
Creating a Provisioner access policy.....	48
Creating an Advanced Provisioner access policy.....	52
Installing the SOAP certificate.....	54
Making SOAP settings on the Ignition Server.....	56
Making SOAP settings in Guest and IoT Manager	58
Guest and IoT Manager Fail-Over	59
Making RADIUS Settings on the Ignition Server.....	60
Making RADIUS settings in Guest and IoT Manager.....	61
Testing Guest and IoT Manager RADIUS connection settings.....	62
Setting up Email notification parameters.....	62
Setting up SMS notification parameters.....	65
Exporting and importing Guest and IoT Manager configurations.....	67
Exporting a Guest and IoT Manager configuration.....	68
Scheduling Export for Guest and IoT Manager configuration.....	69
Importing a Guest and IoT Manager configuration.....	70
Managing HTTPD certificates.....	72
Adding a certificate.....	72
Adding a key.....	73
Binding certificate.....	73
Binding a chain.....	74
Deleting Certificates.....	75
Chapter 6: Managing Guest and IoT Manager.....	76
Running the Guest and IoT Manager Administrator application.....	76
Performing as both Administrator and Provisioner.....	77
Restarting Guest and IoT Manager.....	77
Connecting Guest and IoT Manager to the Ignition Server Appliance.....	78
Disconnecting Guest and IoT Manager from the Ignition Server Appliance.....	78
Setting the Administrator Username and Password.....	79
Setting Administrator Preferences.....	80
Customizing the IDE Ignition Guest and IoT Manager Logo and Login Page.....	80
Changing Application Name and Page Color.....	83
Changing the Language Preference.....	84
Editing E-mail notification settings.....	88
Editing SMS Notification Settings.....	88
Creating SMS Gateways.....	88
Deleting SMS Gateways.....	88
Configuring Timeout settings.....	89
Provisioner Idle Timeout Threshold.....	89

Setting Administrator Session Timeout Threshold.....	89
SOAP Client Timeout Threshold.....	89
Logs.....	90
Viewing the log files.....	90
Chapter 7: Setting guest authorization policies.....	92
Setting authorization policies for guest users.....	92
Access constraint check boxes on the Create Guest User page.....	92
Authorization policies.....	94
Mapping internal user groups to virtual groups.....	94
Sample authorization policies	94
The Example.....	95
Access constraint check boxes.....	95
Components of the authorization policy.....	96
Step-by-step configuration in Ignition Dashboard.....	96
Creating a minimal authorization policy.....	116
Chapter 8: Setting Up Self-Provisioning.....	118
Creating a Self-Provisioning service.....	118
Deploying Self Provisioning Service.....	121
Guest User Self-Provisioning Portal with Sponsor Approval.....	123
Entering Sponsor details manually.....	123
Selecting Sponsor details from AD Group.....	125
Fixed Sponsor.....	128
Managing self-provisioned users.....	129
Deleting a self-provisioning portal.....	130
Chapter 9: Administrator application: managing provisioners, guests, and devices....	131
Setting up provisioners.....	131
Creating a provisioning group.....	132
Configuring the common details.....	133
Configuring the Guest User account details.....	135
Creating Guest User Provisioning using Social Media login.....	143
Configuring sponsor approval.....	144
Configuring the device record details.....	150
Configuring Non Guest and IoT Manager devices.....	152
Custom Device Types and Sub Types.....	154
Configuring the account notification templates.....	157
Configuring advanced details.....	161
Creating a provisioner in the internal store.....	162
Creating a provisioner from an account in an LDAP or AD store.....	163
Bulk importing provisioner accounts from a file.....	163
Checklist: Before your provisioners start working.....	165
Writing SMS and Email templates for account notifications.....	165
Administrator access to the provisioner application.....	167
Managing provisioners.....	167

Viewing the internal provisioners list.....	167
Modifying a provisioner account.....	168
Assigning a provisioner to a provisioning group.....	169
Deleting a provisioner account.....	169
Changing a provisioners password.....	170
Setting the provisioner time-out period.....	170
Monitoring provisioner and guest logins.....	170
Managing provisioning groups.....	171
Managing provisioning groups.....	171
Copying a provisioning group.....	173
Modifying a provisioning group.....	175
Viewing Provisioning Group Summary.....	176
Setting provisioner groups for provisioners stored in LDAP and AD.....	177
Managing group memberships.....	177
Reassigning a provisioner’s guest user accounts and devices to another provisioner.....	177
Moving provisioners, guests, or devices to a new provisioning group.....	178
Assigning unmanaged guests or devices to a provisioner.....	178
Operations on Guest Users.....	179
Retrieving the guest users owned by a provisioner.....	179
Retrieving the guest users that belong to a provisioning group.....	180
Retrieving the guest users first login pending accounts	180
Retreiving Guest Users based on sponsor response.....	181
Retrieving the guest users activated in last X hours.....	182
Viewing expired guest users accounts.....	182
Extending expiry of a guest user account.....	183
Resending Password to Guest User(s).....	184
Retrieving guest users based on sponsor E-mail.....	185
Viewing and Printing Guest User account details.....	186
Deleting the guest users of a provisioner or provisioning group.....	187
Deleting expired guest users.....	187
Exporting guest user records to a file.....	187
Operations on Devices.....	188
Retrieving the devices owned by a provisioner.....	188
Retrieving the devices owned by a provisioning group.....	188
Retrieving the devices activated in last X hours.....	189
Viewing a device record summary.....	189
Viewing the pending devices list.....	191
Viewing expired device accounts.....	192
Exporting device records to a file.....	192
Customizing End User Web Portals.....	193
Customizing Printer Friendly Page.....	193
Chapter 10: Provisioner application: Managing guests and devices.....	196
Introduction to guest user accounts.....	196

What limits you can set on a guest user account.....	196
Guest user account attributes.....	197
Guest user account validity period.....	199
How a guest user logs in.....	199
Launching the provisioner application.....	200
Failed connection.....	200
Application time-out.....	201
Main page of the provisioner application.....	201
Managing guests.....	202
Creating guest user accounts.....	202
Bulk importing guest user accounts from a file.....	203
Sending guest account notifications.....	204
Viewing guest user accounts.....	205
Finding guest user account.....	207
Modifying guest user accounts.....	207
Checking validity of guest user account.....	208
Viewing and Printing Provisioner Guest User account details.....	209
Renewing a guest user account.....	210
Deleting guest user accounts.....	211
Extending expiry of a guest user account.....	211
Resending Password to Guest User(s).....	212
Managing devices.....	213
Creating a device record.....	213
Bulk importing device records from a file.....	215
Assigning a device to a guest user.....	219
Viewing a device record summary.....	219
Bulk modifying the Non Guest and IoT Manager devices	222
Extending expiry of a device.....	226
Managing Sponsored Guests.....	228
Chapter 11: Identity Engines Ignition Device Registration Android App.....	231
Installing Identity Engines IDR Android App.....	231
Identity Engines IDR App Icons.....	232
Launching Identity Engines IDR Android App.....	234
Configuring hostname as Extreme-IGM.....	236
Registering a Device using Identity Engines IDR Android App.....	237
Viewing Device List.....	240
Chapter 12: Troubleshooting and FAQs.....	243
Trouble Ticket	243
Creating a trouble ticket.....	243
Problem: Provisioner cannot login.....	243
Problem: Connection to appliance fails.....	244
Problem: Errors reported during bulk saves and deletes.....	244
Problem: Guest and IoT Manager Email Sending Failed.....	245

Contents

Problem: SOAP Service might be disabled.....	245
Launching Ignition Dashboard.....	245
Problem: Virtual machine issues.....	246
Launching IDR Android App.....	246
Could not resolve hostname.....	246
Connection timeout error.....	247
Ignition Guest and IoT Manager not connected to Ignition Server.....	247
No provisioning group configured for device registration.....	247
Import Configuration Troubleshooting.....	247
VM Configuration Troubleshooting.....	248

Chapter 1: Preface

This chapter provides basic background information that sets the support information of the guide into its perception.

Purpose

The Identity Engines Guest and IoT Manager Configuration guide explains how to Install, Configure, and Manage Guest and IoT Manager.

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

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

Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.extremenetworks.com/education/.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at internalinfodev@extremenetworks.com

Getting Help

Product purchased from Extreme Networks

If you purchased your product from Extreme Networks, use the following support contact information to get help.

If you require assistance, contact Extreme Networks using one of the following methods:

- [GTAC \(Global Technical Assistance Center\) for Immediate Support](#)
 - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- [GTAC Knowledge](#) – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- [The Hub](#) – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- [Support Portal](#) – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Product purchased from Avaya

If you purchased your product from Avaya, use the following support contact information to get help.

Go to the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service

request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Extreme Networks Documentation

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

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

Open Source Declarations

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

Subscribing to service notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

About this task

You can modify your product selections at any time.

Procedure

1. In an Internet browser, go to <http://www.extremenetworks.com/support/service-notification-form/>.
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

Chapter 2: New in this Document

The following sections detail what is new in Identity Engines Guest and IoT Manager for Release 9.4.

IoT Onboarding and Administration

Guest and IoT Manager Application now allows Provisioners to manage Non Guest and IoT Manager devices. New field **All Non-GIM Devices** is available in the **Devices** tab for Administrator to allow Provisioners belonging to this Provisioning Group to manage Non Guest and IoT Manager devices. It also provides an optional Static group selection to further limit the access of the Provisioner managing these devices. For more information, see [Configuring Non Guest and IoT Manager devices](#) on page 152.

Provisioners can now use Bulk Modify feature to edit Non Guest and IoT Manager devices. New field **Bulk Modify** is available when logged in as **Provisioner > Device > View**, and selecting the Provisioning group that contains Non Guest and IoT Manager devices from the **Provisioned by** drop-down field. For more information, see [Bulk modifying the Non Guest and IoT Manager devices](#) on page 222.

CSV Device Import Flow Changes

Override Duplicate MAC Entries:

Provisioner's can now update existing Devices in the Ignition Server using the Import Devices from a CSV file. A new **Override Duplicate Records** field is available in *Load Devices* screen flow to achieve the same. For more information, see [Bulk importing device records from a file](#) on page 215.

Group Assignment of Devices from CSV File:

Provisioners can now Import Network Access Groups from the GUI or CSV file, if the Provisioning Group selected has access to modify Network Access Rights of a Device. **Group Assignment (Input from)** field with **CSV** and **GUI** option is available in the *Load Device* screen. For more information, see [Bulk importing device records from a file](#) on page 215.

Customizing Guest User Notification Template

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

Notification template. For more information, see [Writing SMS and Email templates for account notifications](#) on page 165.

Creating Permanent Guest User Accounts

The Administrator can now allow a Provisioner to create Permanent Guest User Accounts. For more information, see [Account Validity Duration](#) on page 141 details in Configuring the Guest User account details section.

Sponsor URL Multiple Interfaces Support

Administrator can now select the required interface to allow a sponsor to have access to a certain network to approve or deny received requests. The **Select Interface** drop-down field is available in the **Sponsor** tab. For more information, see [Configuring sponsor approval](#) on page 144.

Modify Random Password Special Characters

Administrator can now set the password complexity by selecting the alphanumeric check boxes: lower case, upper case, number, and special character along with the required number of characters condition. If **Random Generated Password** option is selected in **Guest User** tab, then the system generates a random password and send an email to the Guest User containing special characters. For more information, see [Configuring the Guest User account details](#) on page 135.

Special Characters in Provisioning Group Name

Administrator can now create a provisioning group name using special characters and space in between words. For example, use only these special characters: # = () _ - . ! [] . For more information, see [Configuring the common details](#) on page 133.

Providing Passphrase for Key

Administrator can now generate private key for the certificate with passphrase and provide the passphrase while binding the certificate and chain. Ensure that the valid passphrase is provided, so that the bind does not fail and result in HTTPD restart failure. The **Passphrase** field is available *Bind Certificate and Key* pop up window and *Bind Chain* pop up window. For more information, see [Binding certificate](#) on page 73 and [Binding a chain](#) on page 74.

Chapter 3: Guest and IoT Manager Introduction

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

Guest and IoT Manager application in context

The Identity Engines portfolio system for provisioning and managing guest network access consists of the following components:

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

Types of accounts in your Ignition Server installation

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

- *The Guest and IoT Manager administrator* use Guest and IoT Manager to create *provisioners*, and the Guest and IoT Manager administrator is the only person who can create provisioners. Often, the same person who acts as the Ignition Server Administrator acts as the Guest and

IoT Manager administrator, but each account has its own user name and password. There is only one Guest and IoT Manager administrator account. This user account is stored internally in Guest and IoT 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 79.

- The *SOAP API user credentials* allow Guest and IoT Manager to connect to the Ignition Server. See [Making SOAP settings on the Ignition Server](#) on page 56.
- 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 and IoT Manager. For example, if you want to give your company's receptionist the ability to hand out temporary passwords for wireless access, you would define that receptionist as a *provisioner*.
- Each provisioner account is stored either in the Ignition Server internal store or in your LDAP or Active Directory store. Your installation can store provisioners in both places at once.
 - To create provisioner accounts in the Ignition Server internal store, see [Creating a Provisioner access policy](#) on page 48. We refer to internally stored provisioners as *internal provisioners*.
 - To have Guest and IoT Manager authenticate provisioners against your LDAP or AD store, see [Creating a provisioner from an account in an LDAP or AD store](#) on page 163.
- A *portal provisioner* is a provisioner bound to an Ignition Server self-provisioning portal. With a self-provisioning portal in place, guests can create their own guest user accounts, which are then owned by the portal provisioner who owns the portal where the guest account was created. See [Creating a Self-Provisioning service](#) on page 118.
- 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 and IoT 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 196.
- A *user* is any user that Ignition Server can authenticate. The account for such a user can reside in an LDAP directory, an Active Directory store, or in the Ignition Server internal store. Guest users are a subset of users, and the Guest and IoT Manager application can view and update *only guest users* and *provisioners*; you cannot view other types of users through Guest and IoT Manager.
- A *device record* stores the details of a guest user's device so that Ignition Server can enforce rules that allow a guest to connect only using his or her own device. See [Creating a device record](#) on page 213.

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

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

The Guest and IoT Manager administrator role

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

- Creates and manages the provisioner accounts.
- Configures Guest and IoT Manager application settings.
- Connects Guest and IoT Manager to the Ignition Server appliance. The Guest and IoT 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 and IoT Manager administrator can delete expired guest user accounts and can export guest user accounts to file.

Provisioners role

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

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

 **Important:**

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

Guest users

A guest user account has the following attributes:

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

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

Guest user example

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

Create Guest User

Associated Provisioning Group:

* **Group Membership:** SunnyvaleFrontDesk ▼

Guest User Info:

* **First Name:** Johnnie

* **Last Name:** Taylor

* **User Name:** jtaylor

* **Password:** F0rmula4D

Email: jtaylor@company.com

Cell Phone: 4155554343 **Carrier:** AT&T Wireless ▼

Delete on Expire: Yes No

Comments:

Guest Details:

* **Activate Account On:** 2015/11/18 10:13:16 AM ▼ GMT+00:00

* **Duration:** 8 hours ▼ (Max 8 hours)

Network Rights: Internet Campus-Internet

Access Zones: Building-1-Public-Areas

Associated Devices:

[Add...](#)

[Remove](#)

Send Notification:

Other Email:

Submit **Cancel**

Figure 1: Create Guest User window

Device example

Guest and IoT Manager allows you to create device records and assign them to guest users for the purpose of limiting users to using only certain devices, such as, for example, allowing each guest to connect using only his or her own laptop. Also, you can create rules that assign each device to the

appropriate VLAN, part of the network, or physical location in your facility. The following figure is an example of a device creation window.

Common

Associated Provisioning Group:

* **Group Membership:** Guest_Standard ▼

Device Info:

* **MAC Address:**

Name:

Type: ----- Select One ----- ▼

Sub Type:

Source: GM-Guest_Standard

Comments:

Record Enabled: Yes No

Asset Type: Permanent Temporary

Delete on Expire: Yes No

* **Activate Account On:** 2015/12/07 08:42:14 AM ▼ GMT+00:00

* **Duration:** 8 hours ▼ (Max 8 hours)

Associated Users:

[Add...](#)

[Remove](#)

Figure 2: Create Device window

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

You can create device records individually:

- [Creating a device record](#) on page 213
- [Bulk importing device records from a file](#) on page 215

Chapter 4: Installing Guest and IoT Manager

This chapter describes how to install Identity Engines Guest and IoT Manager. You can install Guest and IoT Manager as a virtual appliance on a VMware ESXi 5.5 server.

System requirements

To install Guest and IoT Manager, you need:

- A running Ignition Server appliance, reachable on the network from where you run Guest and IoT Manager. The SOAP interface must be enabled on the Ignition Server.
- An OVA file, if you are deploying the Guest and IoT Manager in ESXi.
- Guest and IoT Manager (VMware ESXi 5.5, 6.0 or 6.5 server)
- An installation of the Ignition Dashboard management application on a PC. Make sure you also have a copy of *Identity Engines Ignition Server Configuration, NN47280-600*.

Ignition Server compatibility

Guest Manager 9.3.2 is compatible only with Ignition Server 9.3.2.

VMware ESXi server requirements

Hardware platforms supported by VMware's ESXi server versions 5.5, 6.0 or 6.5. See <http://www.vmware.com/> for a list of supported hardware platforms for ESXi.

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

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

 **Warning:**

Guest and IoT Manager is provided as a Virtual Appliance. Do not install or configure any other software on the VM shipped.

- Extreme Networks does not support the installation of any VMware specific, RHEL specific, or any third-party vendor package or RPM on its VM, other than what Extreme Networks ships as a package, image, or OVA.
- Do not install or uninstall any software components unless Extreme Networks specifically provides the software and / or instructs you to do so. Do not modify the configuration or the properties of any software components of the VMs (including VMware Tools) unless Extreme Networks documentation and / or personnel specifically instructs you to do so. Extreme Networks does not support any deviation from these guidelines.
- Extreme Networks determines which VMware Tools to install and configure. When required, Extreme Networks provides these tools as part of the installation package. Extreme Networks provides these tools because VMware Tools configures the kernel and network settings and unless Extreme Networks tests and approves these tools, Extreme Networks cannot guarantee that the VM will work after the tool is installed and configured.

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

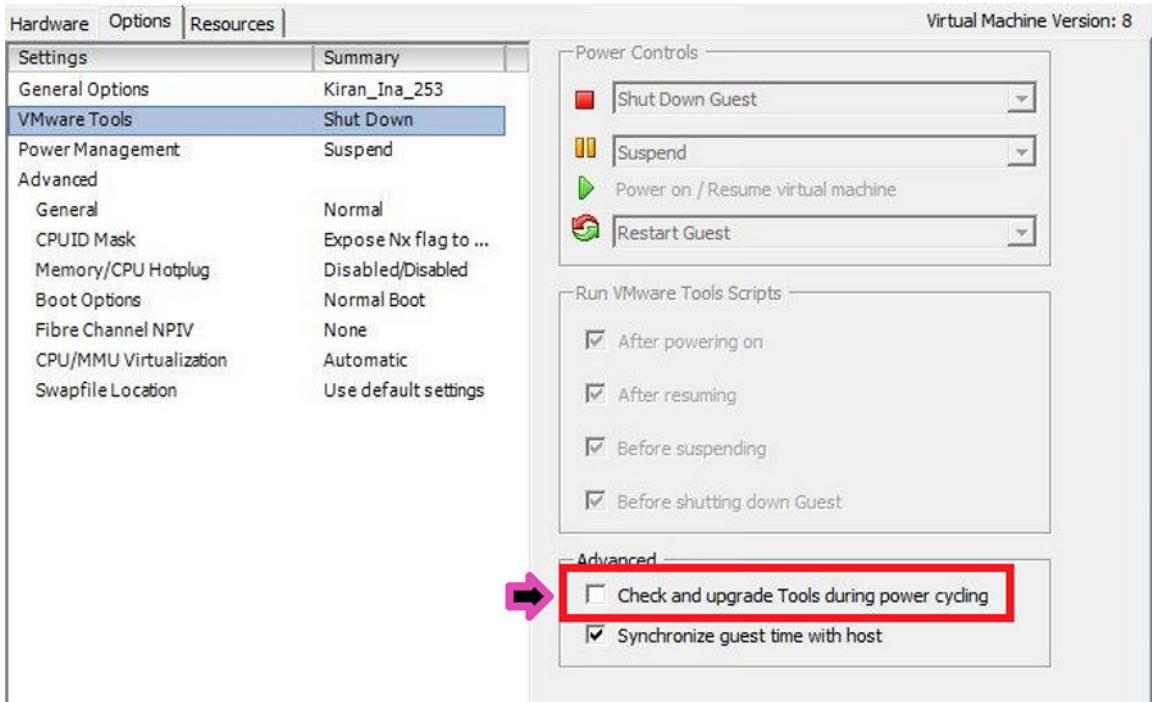
Preventing Automatic VMware Tools Updates

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

To prevent automatic VMware Tools updates:

Procedure

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



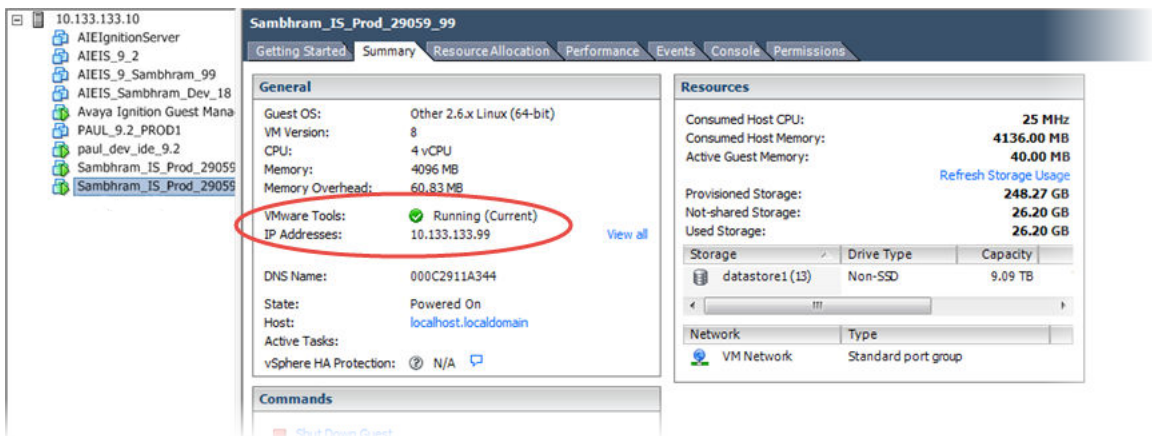
Checking the VMware Tools status on an ESXi Server

The **Summary** tab of the VM describes the VMware Tools status. The following procedure allows you to check the VMware Tools status on an ESXi server versions 5.5, 6.0 or 6.5.

Procedure

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

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



*** Note:**

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

Network configuration for Guest and IoT Manager-based authentication

Guest and IoT Manager has three network interfaces:

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

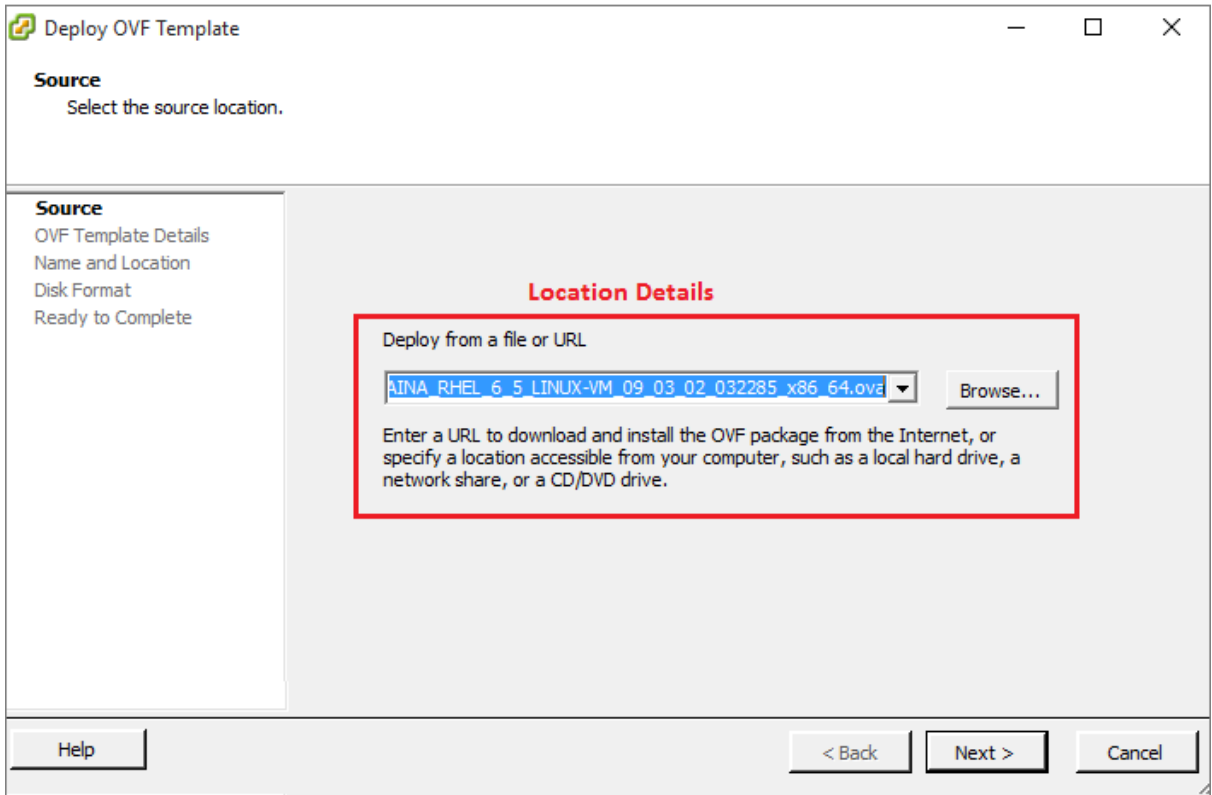
Installing the Guest and IoT Manager virtual appliance

About this task

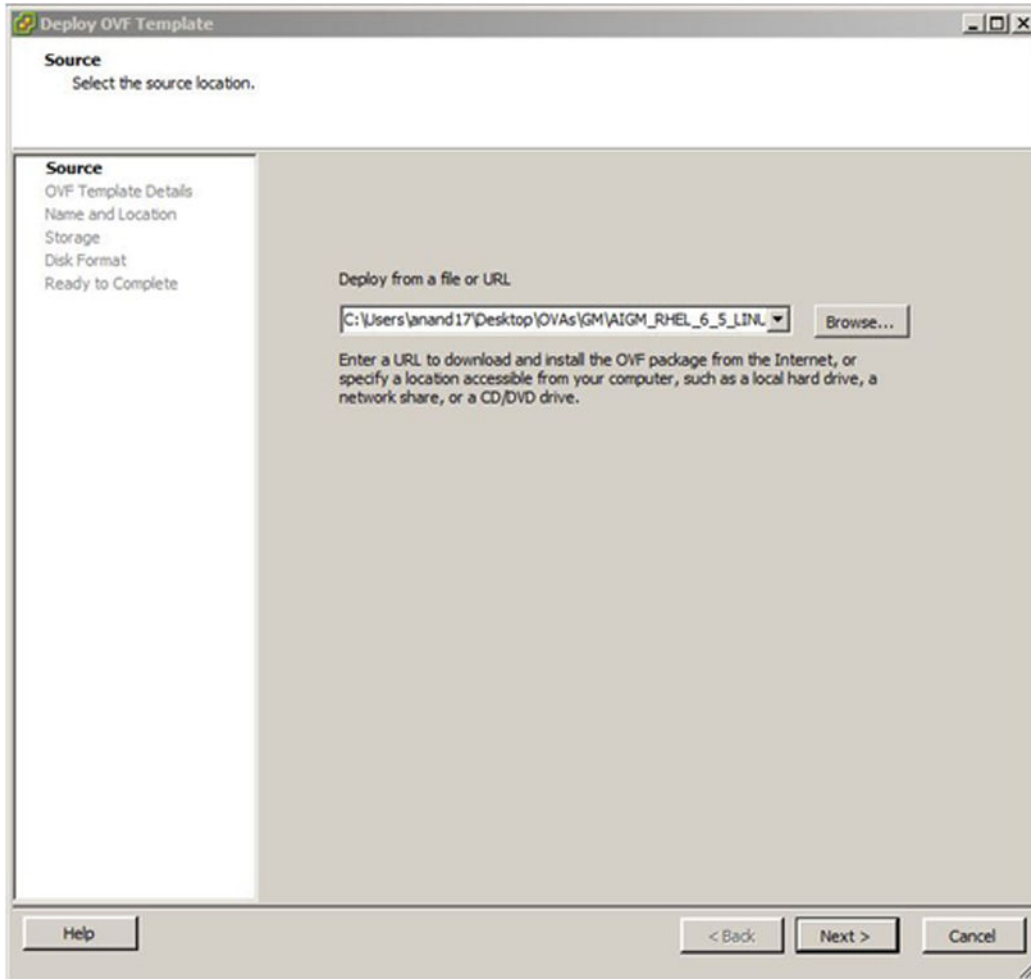
Extreme Networks strongly recommends that you use VMware vSphere Client to import the VM into your system. Start the VMware vSphere Client and log in to the ESXi server on which you want to install Guest and IoT Manager. Use the **Virtual Appliance Deploy OVF** option.

Procedure

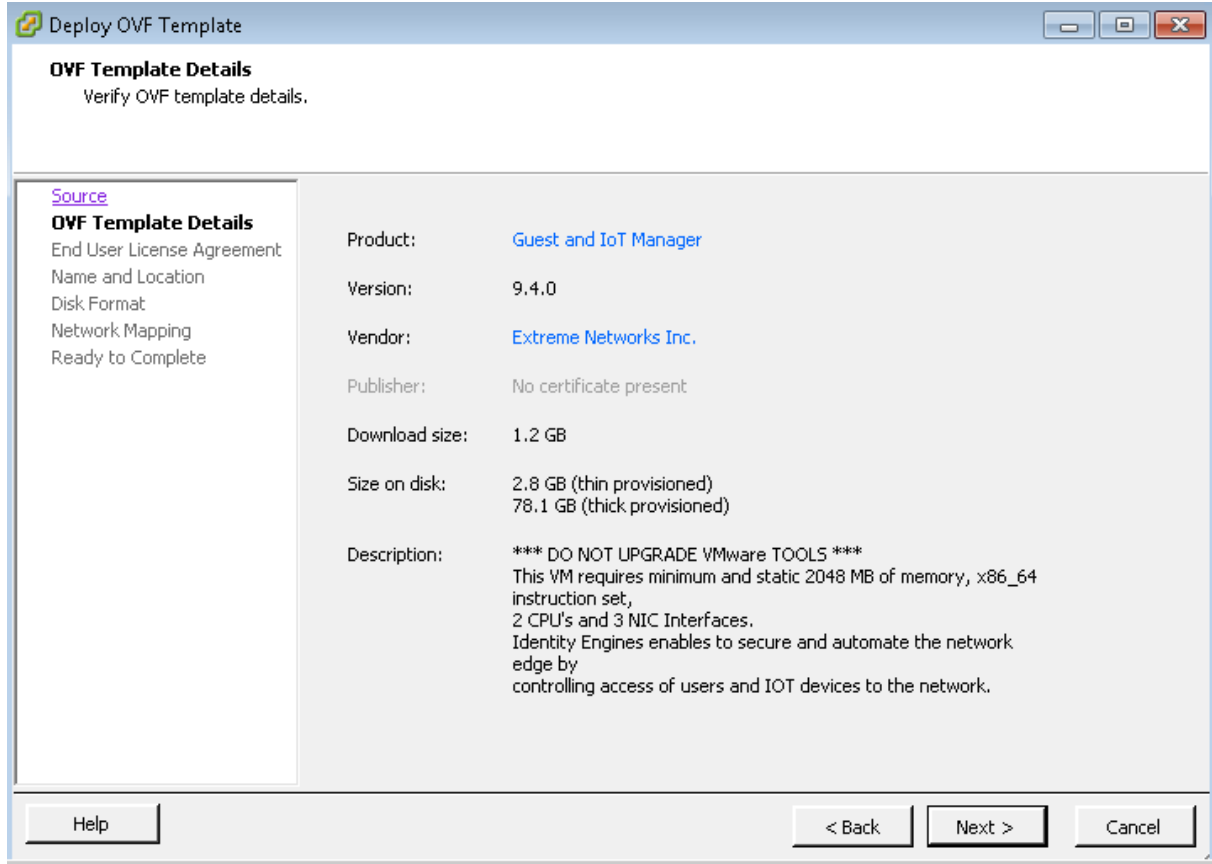
1. From the vSphere Client, select **File > Deploy OVF Template**.



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

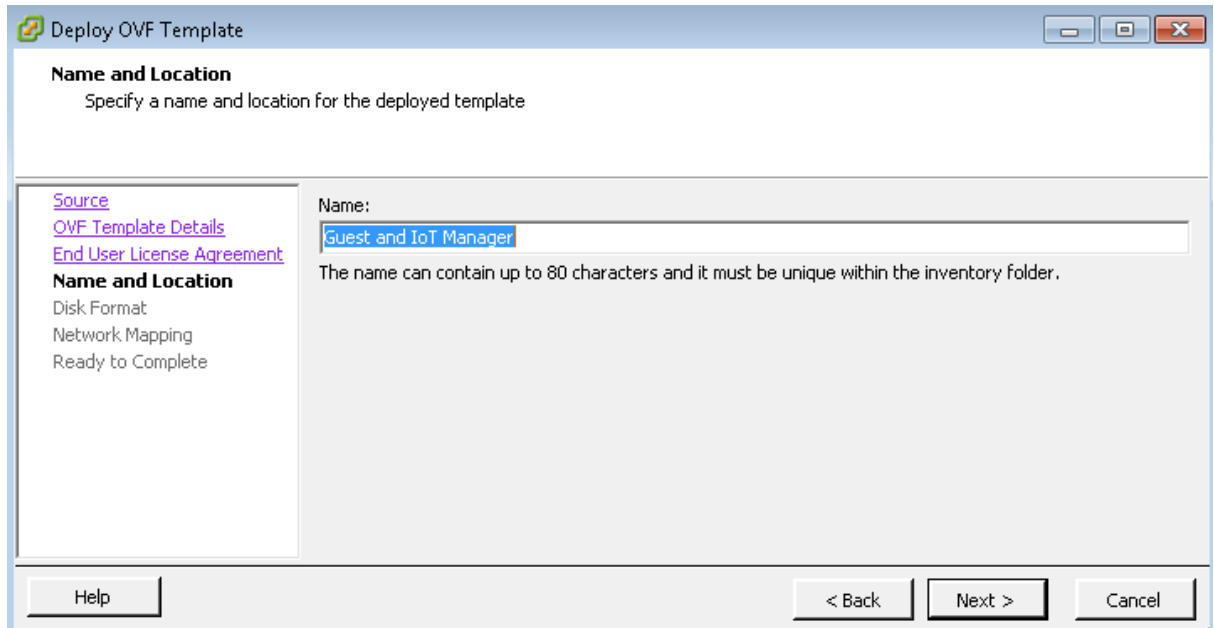


3. On the OVF Template Details screen, review your settings. Click **Back** to make changes, or click **Next** to continue.

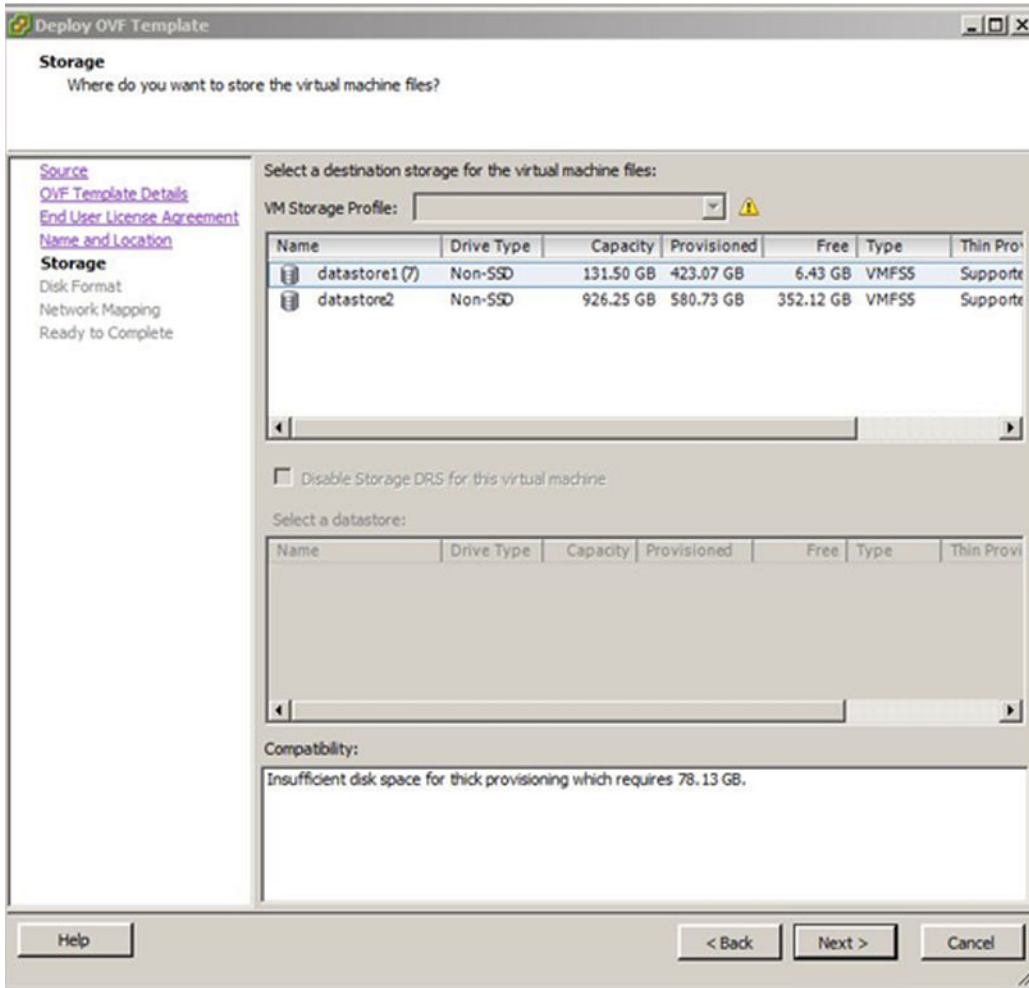


4. On the *End User License Agreement* screen, click **Accept** to accept the license and click **Next**.

5. On the **Name and Location** screen, enter a name for the virtual machine and click **Next**.



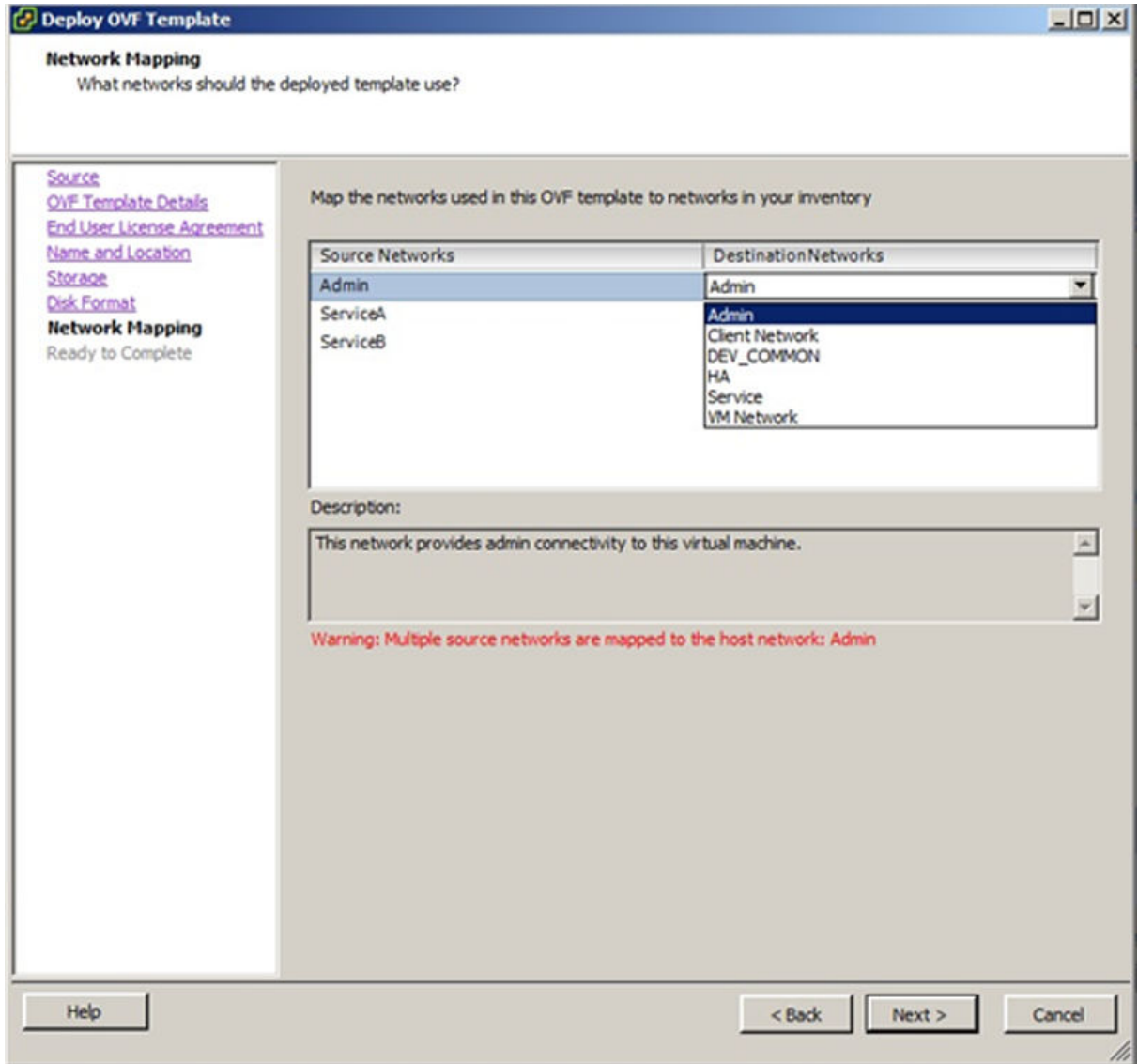
6. On the **Storage** screen, select the location where you want to store the files for the virtual appliance (requires approximately 79 GB) and click **Next**.



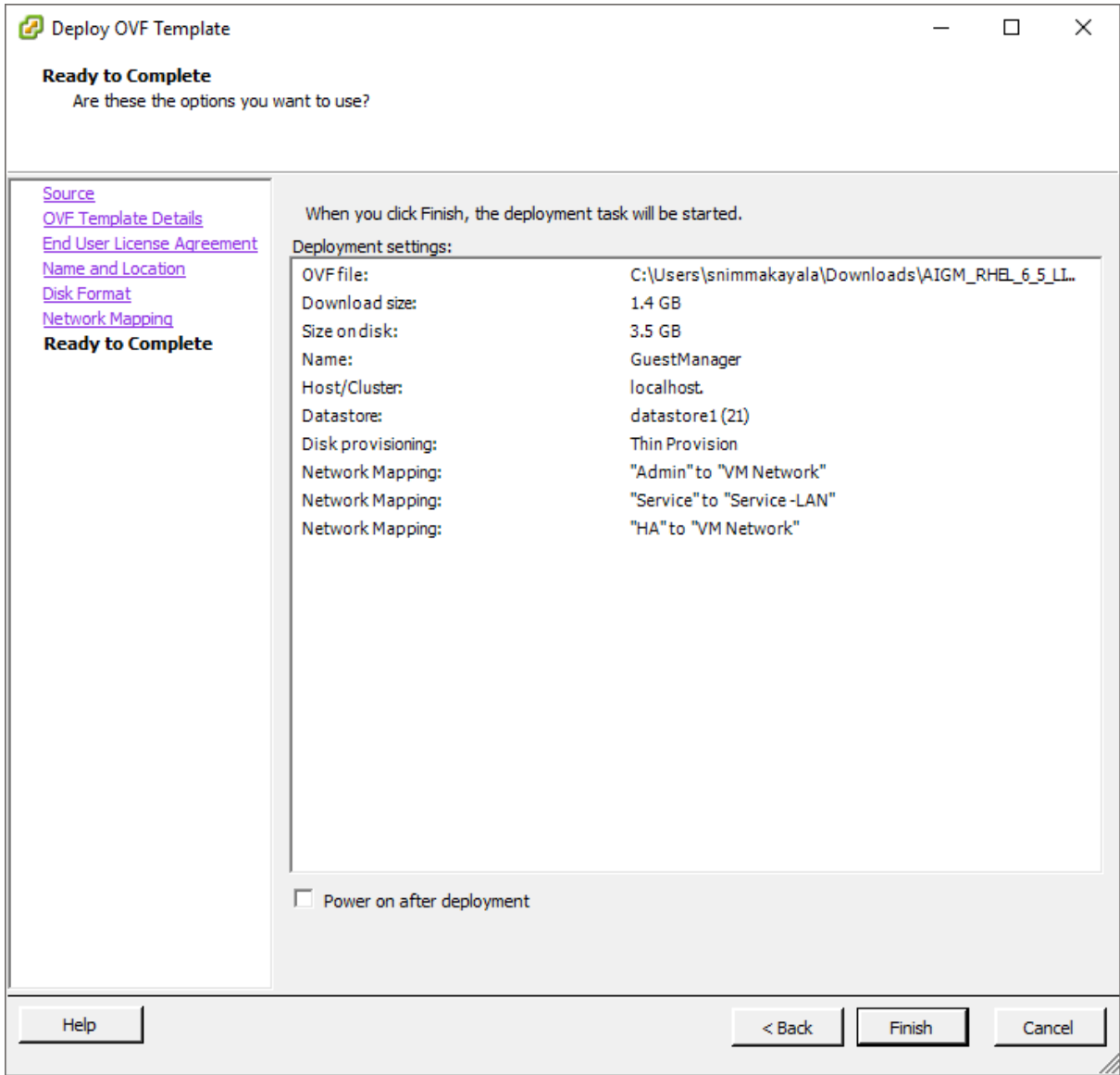
7. On the Disk Format screen, select a format in which to store the virtual machine's virtual disks and click **Next**.

The screenshot shows a window titled "Deploy OVF Template" with a "Disk Format" section. The question "In which format do you want to store the virtual disks?" is displayed. On the left, a navigation pane lists steps: Source, OVF Template Details, End User License Agreement, Name and Location, Storage, Disk Format (selected), Network Mapping, and Ready to Complete. The main area shows "Datastore:" set to "datastore2" and "Available space (GB):" set to "352.1". Three radio buttons are present: "Thick Provision Lazy Zeroed" (selected), "Thick Provision Eager Zeroed", and "Thin Provision". At the bottom, there are buttons for "Help", "< Back", "Next >", and "Cancel".

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



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



Configuring the Guest and IoT Manager virtual appliance

About this task

Configure the VM settings after you complete the importing the VM to your system. This is the minimum configuration required to start Guest and IoT Manager.

Procedure

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

The system displays the Guest and IoT Manager login screen.

```
Guest & IoT Manager 09.04.00.032606
Host: VMware ESX Server
Node: localhost.localdomain
Linux Server using Kernel 2.6.32-642.11.1.el6.x86_64 for x86_64
Hypervisor time sync is: Enabled
URL: https://192.168.220.5/GuestManager/admin
localhost login: _
```

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

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

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

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

4. Configure the primary or secondary DNS Server settings using the following commands:

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

Enter `dns server secondary NNN.NNN.NNN.NNN`.

5. Restart the Tomcat service.

Enter `tomcat restart`.

6. Enter `httpd restart`.

Configure HTTPS connections

Guest and IoT Manager supports HTTPS access only and comes with a default certificate to be used with HTTPS access.

Important:

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

Configuring HTTPS access

About this task

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

Important:

If you add a custom certificate, note the following:

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

Important:

Guest and IoT Manager HTTPS mode supports only TLSv1 and above.

Procedure

1. Log in to the Guest and IoT Manager VM as admin.
2. Add a custom certificate. Enter
 - a. `certificate installkey <url> [Display Name]`
 - b. `certificate installcert <url> [Display Name]`The display name is optional. If you do not specify a display name, the file name is used as the display name. The name can have white space but must be enclosed in single or double quotes.
3. Enter `httpd key <Display Name>` where Display Name is the display name given when you installed the key. The name can have white space but must be enclosed in single or double quotes.
4. Enter `httpd cert <Display Name>` where Display Name is the display name given when you installed the certificate. The name can have white space but must be enclosed in single or double quotes..
5. Enter `httpd restart`.

Chapter 5: Configuring Guest and IoT Manager

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

Command Line Interface

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

The CLI has a default timeout of 5 minutes.

Command	Description
certificate	Use to manage certificates.
clear	Clear the Terminal screen.
dns	Configure the DNS setting.
exit	Guest and IoT Manager
halt	Halt the running system and power off the Guest and IoT Manager virtual machine.
help	Display the list of Guest and IoT Manager CLI commands.
httpd	Control the httpd server.
interface	Configure the interface settings.
ping	Ping the remote host password.
reboot	Reboot the Guest and IoT Manager virtual machine.
reinit	Reinitialize the Guest Guest and IoT Manager virtual machine to factory defaults.
route	Configure the route settings.

Table continues...

Command	Description
show certificates	Shows information about the certificates and keys in the certificate/key database.
show dns	Show the current DNS setting.
show httpd	Show information about the configuration and state of the httpd web server.
show interface	Show the current interface settings for a specific port or ports..
show route	Show the active routes in the system.
sshd	Enable or disable the sshd service.
tomcat	Control the tomcat server using the tomcat command to either start, stop, restart, or stop.

certificate

The `certificate` command manages certificates.

Important:

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

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

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

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

Syntax

```
certificate [installchain, installkey, installcert, delete, list, timeout, reset]
```

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

reset Resets the configuration database with only the default certificates.

Example

```

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

```

show certificates

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

Syntax

```
show certificates
```

Example

```

GuestManager>show certificates
Name                Delete Allowed    Type
Default_Cert        False             certificate
Default_Chain        False             chain
Default_Key          False             key

httpd is using certificate: Default_Cert
httpd is using key      : Default_Key
httpd is using chain    : Default_Chain
GuestManager>

```

dns

The `dns` command configures the DNS settings.

Syntax

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

```
dns server secondary NNN.NNN.NNN.NNN
```

```
dns server <domain.com>
```

```
dns clear server all
```

```
dns clear server primary
```

```
dns clear server secondary
```

```
dns clear domain
```

Example

```
GuestManager>dns
dns server primary NNN.NNN.NNN.NNN
dns server secondary NNN.NNN.NNN.NNN
dns domain <domain.com>
dns clear server all
dns clear server primary
dns clear server secondary
dns clear domain
GuestManager>dns server primary 10.2.3.4
Changing the DNS Setting.
Stopping tomcat6: [ OK ]
Starting tomcat6: [ OK ]

GuestManager>_
```

Figure 3: dns command example

show dns

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

```
show dns
```

Example

```
GuestManager>show dns
Domain          : None
Primary DNS Server : 135.27.4.226
Secondary DNS Server: None
GuestManager>_
```

httpd

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

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

Syntax

```
httpd <start|stop|restart|key|cert <cert or key name>
```

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

Example

```
GuestManager>httpd
Insufficient Parameters.
httpd <start|stop|restart|key|cert <Cert or key name>
start
stop
restart
key <key name>
cert <cert name>
<key|cert name> is Name shown by the
show certificates command.
key/cert names with whitespace/spaces need to quoted.
single or double quotes are allowed.
    where interface is one or more of: Admin|ServiceA|ServiceB|all
    where interface is one or more of: eth<0..N>|,eth<0..N>|all

GuestManager>_
```

show httpd

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

Syntax

```
show httpd
```


Example

```

GuestManager>show httpd
httpd server enabled      : True
httpd server active      : True
https port enabled       : True
httpd is using certificate : Default_Cert
httpd is using key       : Default_Key
httpd is using chain     : Default_Chain
httpd server is listening on https: : Admin      10.133.140.102
httpd server is listening on https: : ServiceA
httpd server is listening on https: : ServiceB
Active listening addresses from netstat:
tcp 10.133.140.102:https      LISTEN
GuestManager>_

```

interface

The `interface` command configures the interface settings.

! Important:

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

Syntax

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

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

Example

```

GuestManager>interface eth0 ipaddr 10.133.133.77/24
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:50:56:8b:c7:0a brd ff:ff:ff:ff:ff:ff
    inet 10.133.133.77/24 scope global eth0
    inet6 fe80::250:56ff:fe8b:c70a/64 scope link
        valid_lft forever preferred_lft forever

Restart the httpd server to listen on the new IP Addresses.
Disable and then enable the sshd service to listen
on the new IP Addresses.
Warning: A default route is not present, if a default route
Warning: is required in your environment use the route command
Warning: to specific a default route. Enter help route for more information.
GuestManager>_

```

show interface

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

Syntax

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

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

Example

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

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

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

route

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

Syntax

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

Example

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

show route

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

Syntax

```
show route
```

Example

```
GuestManager>show route
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
10.133.140.0     *                255.255.255.0   U      0      0      0 eth0
default          10.133.140.1    0.0.0.0         UG     0      0      0 eth0
GuestManager>_
```

ping

The `ping` command pings a remote system to test the connection between Extreme Networks Guest and IoT Manager and another network device. After you ping a device, the switch sends an Internet Control Message Protocol (ICMP) packet to the target device. If the device receives the packet, it sends a ping reply. After the switch receives the reply, a message appears that indicates traffic can reach the specified IP address. If the switch does not receive a reply, the message indicates the address is not responding.

Syntax

```
ping
```

```
ping [ttl <nnn> [ count <nnn> ]] <NNN.NNN.NNN.NNN >:<DNS Name >
```

Example

```
GuestManager>
GuestManager>ping 10.133.133.10
PING 10.133.133.10 (10.133.133.10) using timeout of 5 seconds.
200 bytes from 10.133.133.10 icmp_seq=0 ttl=5 time=1.28602981567 ms
200 bytes from 10.133.133.10 icmp_seq=1 ttl=5 time=0.189065933228 ms
200 bytes from 10.133.133.10 icmp_seq=2 ttl=5 time=0.308036804199 ms
200 bytes from 10.133.133.10 icmp_seq=3 ttl=5 time=0.230073928833 ms
GuestManager>
```

sshd

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

Syntax

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

! Important:

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

Example

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

tomcat

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

Syntax

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

To restart the Tomcat service, enter `tomcat restart`.

Example

```
GuestManager>
GuestManager>tomcat
tomcat <start|stop|restart|status>
GuestManager>
GuestManager>
GuestManager>tomcat stop
Stopping tomcat6: [ OK ]

GuestManager>
GuestManager>tomcat start
Starting tomcat6: [ OK ]

GuestManager>
GuestManager>tomcat restart
Stopping tomcat6: [ OK ]
Starting tomcat6: [ OK ]

GuestManager>_
```

Figure 4: Tomcat command

clear

The `clear` command clears the terminal screen.

Syntax

```
clear
```

Example

```
GuestManager>clear_
```

help

The `help` command displays the list of Guest and IoT Manager CLI commands.

Syntax

```
help
```

Example

```

GuestManager>help
certificate      : Manage Certificates.
clear            : Clear the Terminal Screen
dns             : Configure DNS setting.
exit            : Exit GuestManager cli
halt            : Halt GuestManager Virtual Machine.
help            : Display list of GuestManger CLI
                : commands.
httpd           : Control the httpd server.
interface       : Configure interface settings.
ping           : Ping remote system.
reboot         : Reboot GuestManager Virtual Machine.
reinit         : Reinitialize GuestManager UM to
                : factory defaults.
route          : Configure route settings.
show certificates : Show Certificates.
show dns       : Show current dns settings.
show httpd    : Display httpd information.
show interface : Show current interface settings.
show route    : Show current route settings.
ssh           : Enable/disable configure sshd service.
tomcat       : tomcat <start|stop|restart|status>
user        : user <user name> [enable|disable]
GuestManager>_

```

Figure 5: Help command

About usernames and passwords

! Important:

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

- Guest and IoT Manager administrator: The principal administrator of the Guest and IoT Manager application. Only the Guest and IoT Manager administrator can configure Guest and IoT Manager and create Provisioners. By default, the user name and password for the Guest and IoT Manager administrator are `admin / admin`. After installation, it is recommended to change the password as shown on [Setting the Administrator Username and Password](#) on page 79.
- Guest and IoT Manager virtual appliance administrator: These are the credentials that you use to configure the Guest and IoT Manager virtual appliance. By default, the user name and password for the Guest and IoT Manager virtual appliance administrator are `admin / admin`.
- Ignition Server SOAP API user credentials: These are the credentials the Guest and IoT Manager application uses to connect to the SOAP API on the Ignition Server appliance. Instructions for this appear in the section [Making SOAP settings on the Ignition Server](#) on page 56.
- Ignition Server administrator administrator: The administrator who runs Ignition Dashboard and manages the Ignition Server appliance. You need these credentials in order to configure the Ignition Server appliance and to create guest user authorization policies.

- **Guest and IoT Manager provisioners:** These are the login accounts of front desk personnel who create and manage guest users in Guest and IoT Manager. Their user accounts can be stored locally in Ignition, or they can be accounts in your LDAP or AD user store.

For additional information on the various accounts used to configure and run Guest and IoT Manager, see [Types of accounts in your Ignition Server installation](#) on page 16.

Launching Guest and IoT Manager

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

Guest and IoT Manager is made up of two applications:

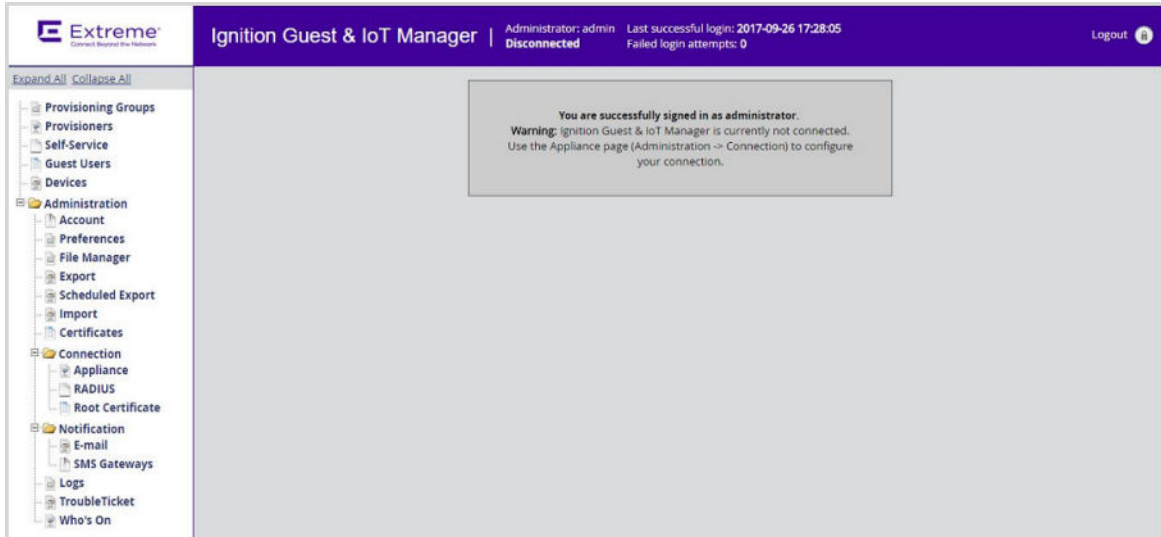
- **Administrator Application:** The application that the Guest and IoT Manager administrator uses to configure Guest and IoT Manager and to create provisioner accounts. Only the Ignition Dashboard administrator can use it.
- **Provisioner Application:** The application that provisioners use to create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

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

Procedure

1. Open a web browser and point the web browser to the Guest and IoT Manager Administrator application at `https://<GM_IPAddr >/Guest&IoTManager/admin`.
2. Enter the login credentials of the Guest and IoT Manager administrator. By default, these are:
 - **Username:** `admin`
 - **Password:** `admin`
3. Click **Login**.

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



When Administrator logs into Guest and IoT Manager Web UI, the **last successful login time** and the **number of failed attempts** between two successful logins of the Admin account are displayed on the header of admin page.

4. Change the administrator password.

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

! Important:

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

Next steps

Do one of the following:

- If your provisioner accounts will be stored on the Ignition Server only (that is, if you will create all of your provisioners in Guest and IoT Manager, you can skip the following policy sections and go immediately to [Installing the SOAP certificate](#) on page 54.
- If any of your provisioner accounts are stored in LDAP or AD, go to [Creating a Provisioner access policy](#) on page 48.

Creating a Provisioner access policy

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

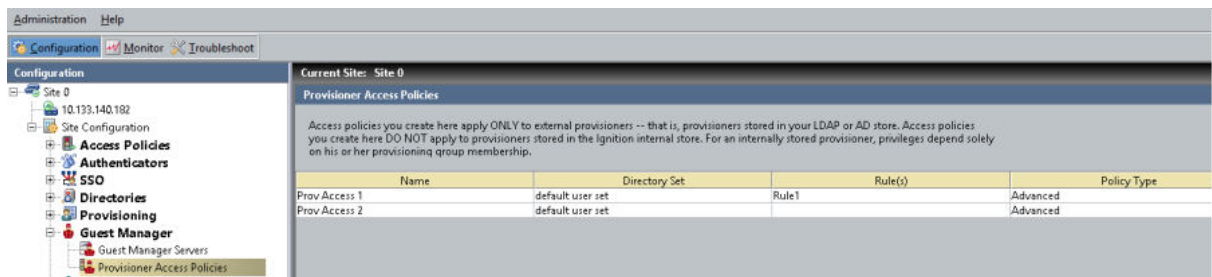
determines how Ignition Server looks up provisioner accounts in LDAP or AD, and what type of provisioner access it grants to each provisioner.

Provisioner access policies do not apply to internal provisioners (provisioners stored in the Ignition Server internal store). If you plan to use only internal provisioners, skip this section and go to [Making RADIUS Settings on the Ignition Server](#) on page 60.

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

Procedure

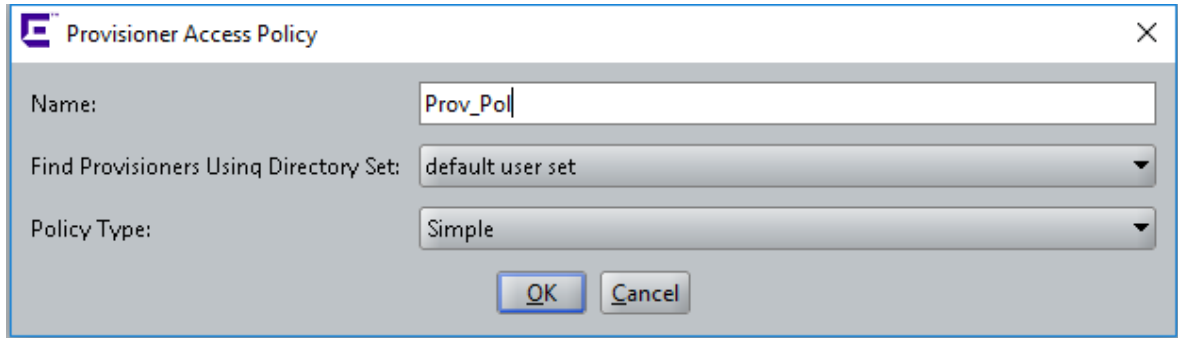
1. Create the directory services, directory sets, and virtual groups that let Ignition Server look up your provisioners and find the groups that contain them. In Ignition Dashboard (not Guest and IoT Manager), do the following:
 - Create a directory service for each LDAP or AD store that holds provisioner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



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

The provisioner access policies are only needed for LDAP- and AD-stored provisioners, not for internal provisioners (provisioners kept in the Ignition Server internal store). Internal provisioners are granted privileges based on their provisioning group membership, assigned as described in [Managing provisioning groups](#) on page 171.

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



- In the **Find Provisioners Using Directory Set** drop-down list, choose the directory set you created or found in Step [1](#) on page 49.
- In the **Policy Type** drop-down list, choose **Simple** or **Advanced**.

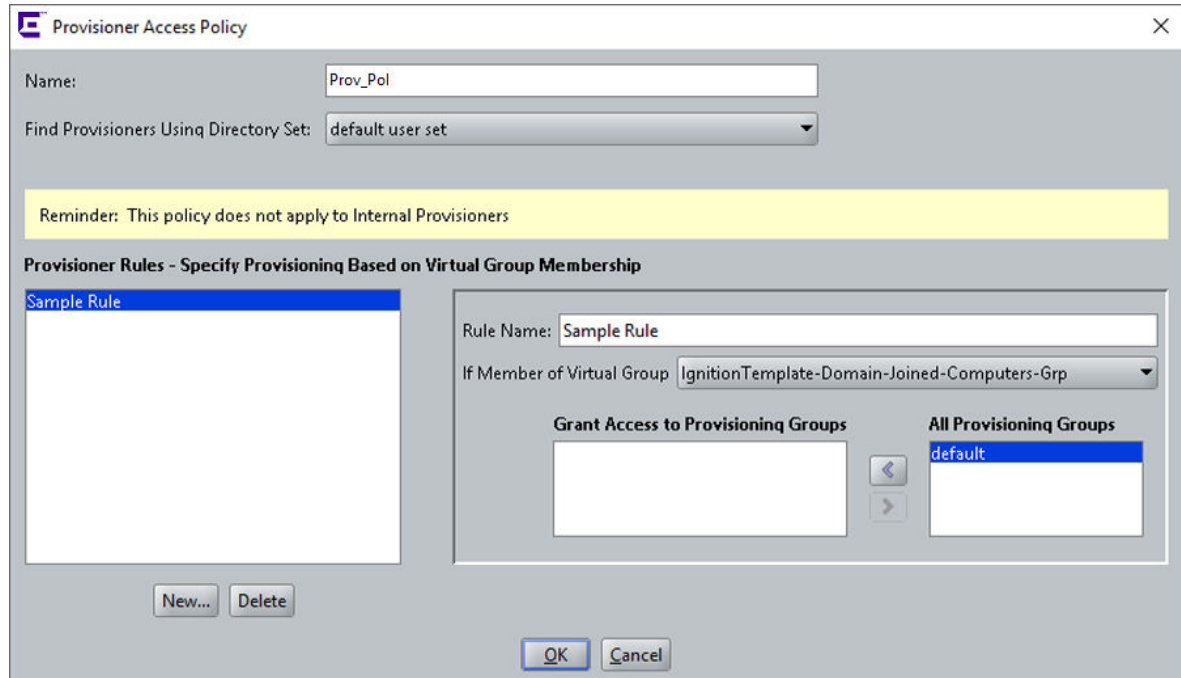
A Simple policy lets you map each virtual group to one or more provisioning groups; an Advanced policy lets you consider more criteria. If you choose Simple, continue to follow this procedure. If you choose **Advanced**, go to [Creating an Advanced Provisioner access policy](#) on page 52.

- Click **OK**.

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

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

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



3. Working in the Provisioner Access Policy window, write the rules that form your provisioner access policy:
 - Below the **Provisioner Rules** list, click **New**.
 - In the **Create New Rule** window, type a name for the rule and click **OK**.
 - In the panel on the right, in the **If Member of Virtual Group** field, choose a virtual group (you found or created the virtual groups in [1](#) on page 49).
 - 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 and IoT Manager, you have the option of creating a unique policy for each installation, if needed. To do this, click **New** at the bottom of the **Access Policies** panel and repeat the procedure to create another provisioner access policy.

Next steps

Go to [Installing the SOAP certificate](#) on page 54.

Creating an Advanced Provisioner access policy

This section explains how to create a provisioner access policy with complex rules that assign provisioner rights. If you do not understand provisioner access policies, read the section, [Creating a Provisioner access policy](#) on page 48, before you create your advanced policy.

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

Procedure

1. Create the directory services, directory sets, and virtual groups that contain your provisioner accounts. See the [Creating a Provisioner access policy](#) on page 48 for instructions.
2. Create the provisioner access policy in Ignition Dashboard. In Dashboard's **Configuration** tree, open the **Guest Manager** node and click on **Provisioner Access Policies**.
3. Click **New** at the bottom of the window.
4. In the Provisioner Access Policy window, enter a name for this policy. In the **Find Provisioners Using Directory Set** drop-down list, choose the directory set that contains your provisioners.
5. In the **Policy Type** drop-down, choose **Advanced**.
6. Click **OK**.

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

7. In the Authorization Policy section of the window, click **Edit**.

The Edit Authorization Policy window appears. The left side of the window lists the rules that form your policy, and the right side of the window lets you edit a rule. The Constraint table shows the logical statement that must be satisfied to allow or deny access to the provisioner. You use the AND/OR conjunctions to assemble a series of tests into a constraint.

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

Constraint Details [Close]

Match The Following Rule:

Attribute Category: **User**

- Authentication Service
- Authentication Service Name
- Authentication Service Type
- Lookup Service
- Lookup Service Name
- Lookup Service Type
- account-locked
- avaya-rm-data
- avaya-rm-principal-name
- email-address
- enable-max-retries
- enable-password-expiration
- enable-start-time
- first-name
- group-member**
- last-name
- max-retries
- network-usage
- office-location
- password-expiration

Attribute: group-member
Data type: integer
Description: User's group membership (internal store)

Contains Any

Static Value Dynamic Value of Attribute

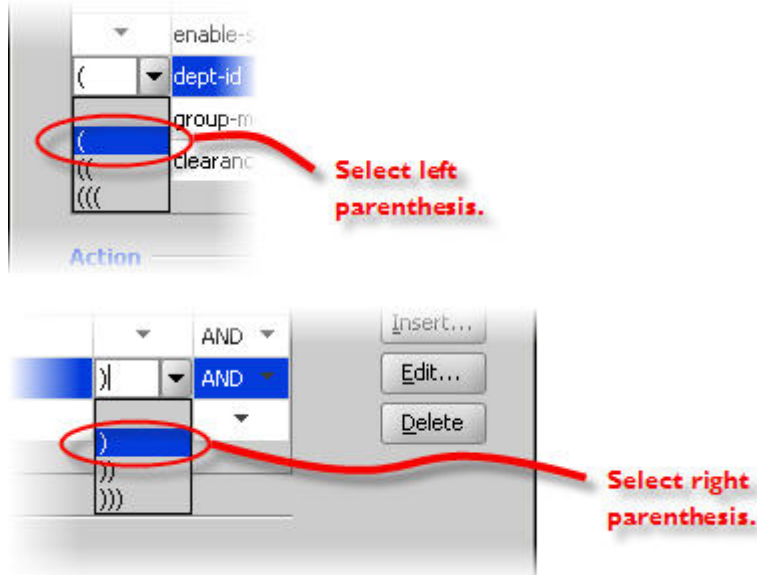
IgnitionTemplate-Guests-Grp

Add... Delete

OK Cancel

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

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



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

Installing the SOAP certificate

Guest and IoT Manager and the Ignition Server each have installed copies of a common SOAP *service certificate* to secure their communications. Guest and IoT Manager cannot connect without this. Your installation comes with a default certificate that is acceptable for test installations. In a production installation, you should replace both copies with your own certificate for added security. If you intend to continue using the default certificate, you may skip this section and proceed to [Making SOAP settings in Guest and IoT Manager](#) on page 58.

! Important:

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

About this task

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

Procedure

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

! Important:

Do not confuse the *Guest and IoT Manager keystore* with the *browser keystore* and the certificates that secure HTTPS browser sessions. For information on setting up HTTPS security, see [Configure HTTPS connections](#) on page 34.

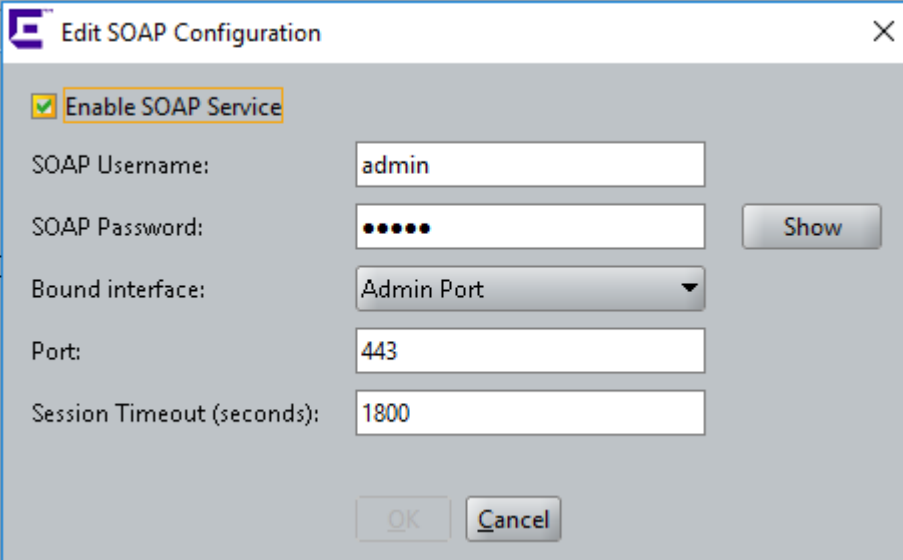
Making SOAP settings on the Ignition Server

In this and the next few sections, you will make the settings that allow Guest and IoT Manager and the Ignition Server to communicate. Guest and IoT 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 and IoT 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 *Identity Engines Ignition Server Configuration, NN47280-600*. Always check that document for the latest information on the SOAP service.

Procedure

1. Launch Ignition Dashboard (see [Launching Ignition Dashboard](#) on page 245) 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 *Identity Engines Ignition Server Configuration, NN47280-600*.
4. In the Sites panel, click the **Services** tab and click the **SOAP** tab. If there is no SOAP tab, it means your SOAP license is expired. See the preceding step.
5. Click on the **Edit** button in the SOAP tab. The Edit SOAP Configuration window appears.



The screenshot shows the "Edit SOAP Configuration" dialog box. It features a title bar with the Identity Engines logo and a close button. The main content area includes a checked checkbox for "Enable SOAP Service". Below this are five input fields: "SOAP Username" (containing "admin"), "SOAP Password" (masked with dots and a "Show" button), "Bound interface" (a dropdown menu set to "Admin Port"), "Port" (containing "443"), and "Session Timeout (seconds)" (containing "1800"). At the bottom of the dialog are "OK" and "Cancel" buttons.

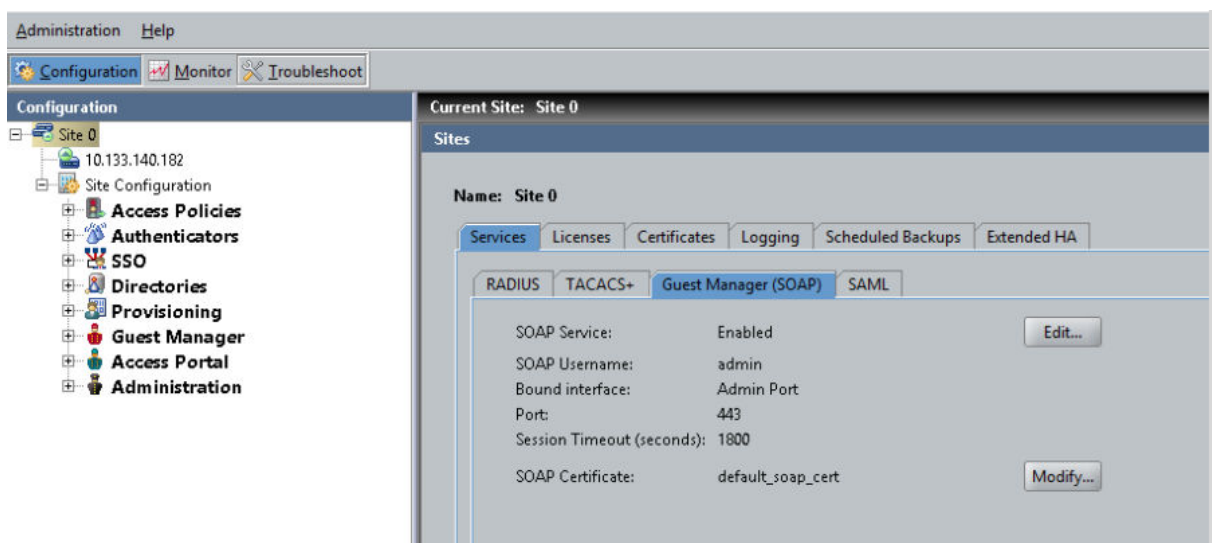
6. Edit the entries as follows, and make a note of these entries. You will use them to connect Guest and IoT Manager to the appliance in [Make SOAP settings in Guest to IoT Manager](#) on page 58.

7. Set the SOAP connection parameters:

- **Enable SOAP Service:** Check this check box to make the SOAP API service available.
- **SOAP Username:** This is the login name that Guest and IoT Manager and other SOAP API clients use to connect to the service. This is not an account in the internal store; by typing a name and password here, you are creating the SOAP user account. Do not use spaces or *hyphens*. Type only letters and numbers.
- **SOAP Password:** Password that SOAP user account uses to connect.
- **Bound Interface:** From the drop-down list, choose the Ignition Server Ethernet interface that is intended to handle SOAP traffic. You can bind the SOAP service to any port on the Ignition Server. If you are running an HA pair of Ignition Servers, you can choose to bind to a VIP interface. The VIP names are also listed in the drop-down list. For further information on using VIPs, see *Identity Engines Ignition Server Configuration, NN47280-600*.
- **Port:** Enter the port number to which API clients should connect. Traffic through this port is HTTPS traffic.
- **Session Timeout:** This is the SOAP *client timeout* setting. Enter the period, in seconds, after which the SOAP API connection is automatically reset. This timeout ensures that unused sessions are closed at the expiration of the timeout period, but it does not cause Guest and IoT Manager to become disconnected since Guest and IoT Manager automatically reconnects. It is recommended that you set this interval to 1800 seconds. See [SOAP Client Timeout Threshold](#) on page 89.

! Important:

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

8. Click **OK**.

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

Making SOAP settings in Guest and IoT Manager

Specify your SOAP settings in Guest and IoT Manager.

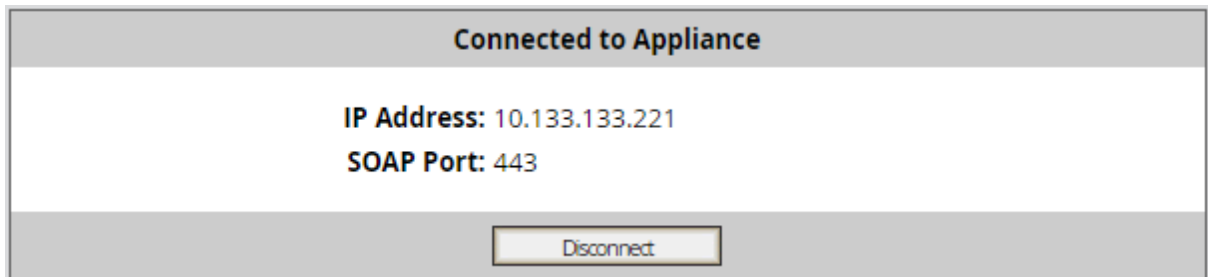
Procedure

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

This command lets you connect to and disconnect from an Ignition Server appliance.

4. In the Login to Appliance screen, enter the SOAP service connection settings of your Ignition Server appliance. These are the settings you established in [Making SOAP settings on the Ignition Server](#) on page 56.
 - **IP Address:** Enter the IP address of the Ignition Server Admin Port (or its VIP port if your SOAP service is bound to a VIP port). To find this IP address, launch Ignition Dashboard and look in the System Explorer window.
 - **SOAP Port:** Enter the HTTPS port of the appliance's SOAP service.
 - **Username** and **Password** for the Ignition Server SOAP API user account. These are the credentials you created in [Making SOAP settings on the Ignition Server](#) on page 56.
5. Click **Connect**.

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



The connection disconnects after the timeout interval specified in [Making SOAP settings on the Ignition Server](#) on page 56.

Guest and IoT Manager Fail-Over

The Guest and IoT Manager administrator can now configure a Second Appliance IP Address. With this functionality there are two appliances configured on the Guest and IoT Manager, so when the first appliance goes down the Guest and IoT Manager maintains an active SOAP connection with the second appliance and vice versa.

*** Note:**

The Guest and IoT Manager Fail-Over works only when both first and second appliances are always in sync. They work in the High Availability configuration.

About this task

The Guest and IoT Manager **Administration > Connection > Appliance** page consists of a check box to configure a **Second Appliance** IP address. By default the check box is unchecked.

By checking the **Configure Second Appliance IP Address** check box:

- The label **IP Address** changes to **First IP Address**.
- The Guest and IoT Manager administrator can see the option to enter the **Second IP Address**.

Figure 6: Appliance page – Second Appliance option

*** Note:**

When you click **Connect**, the message "You have successfully connected to Ignition Server: <IP Address>" is displayed and then you are forwarded to Connected to Appliance Table.

When the Guest and IoT Manager administrator clicks **Connect** after configuring the second appliance, the system displays the following **Connected to Appliance** page:

Connected to Appliance			
IP Address	SOAP Port	Status	Connection
10.133.133.192	443	Up	Connected
10.133.133.191	443	Up	-

Disconnect

Figure 7: Appliance page – two appliances configured

*** Note:**

You can view the connection status in the log entries also. For example,

```
2016-05-10 22:54:54, Connected to 192.168.10.3 by 135.123.148.143  
2016-05-10 22:54:54, Connected to 192.168.10.4 by Ignition Guest & IOT Manager
```

For more information, see [Viewing the log files](#) on page 90.

The Appliance page shows the following information:

- Up or down status of the two appliances configured
- Appliance to which Guest and IoT Manager is having an active SOAP connection

*** Note:**

- Guest and IoT Manager will maintain only one active SOAP connection.
- On start-up Guest and IoT Manager will connect to the first IP address. Guest and IoT Manager will toggle between the two IP addresses, when the Ignition Server SOAP connection fails subsequently.
- If one of the appliances go down, Guest and IoT Manager will automatically connect to the other appliance with a maximum down time of 20 seconds.
- If both IP addresses go down, the Guest and IoT Manager redirects you to the **Login** page.
- All activities of the Guest and IoT Manager are recorded in the log files. For more information, see [Viewing the log files](#) on page 90.
- If the both the servers are down while configuring the two appliances, Guest and IoT Manager does not allow to proceed until the Admin re-enters the Appliance IP addresses till the time one of the two is up.
- While configuring the two appliances, if both the servers are down; you must re-enter Appliance IP addresses until at least one of the two appliances is up. However, the periodic SOAP tests are not initiated in this case, as Guest and IoT Manager is completely dependent on the Ignition Server for operations and also, to make sure that you are entering the correct IP address.

Making RADIUS Settings on the Ignition Server

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

When a provisioner logs into the Guest and IoT 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 and IoT Manager authenticates the provisioner by sending a RADIUS request to the Ignition Server.

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

Procedure

1. Launch Ignition Dashboard if it is not running already, see [Launching Ignition Dashboard](#) on page 245.
2. In the main Dashboard window, click the **Configuration** button.
3. In the **Configuration** hierarchy tree, expand the **Guest Manager** node and click **Guest Manager Servers**. The **Guest Manager Server Summary** panel appears, displaying all the Guest and IoT Manager installations that can connect to this Ignition Server.
4. Click **New** near the bottom of the window.
5. In the Guest and IoT Manager Server Details window, type a **Name** for your Guest and IoT Manager installation, and type the **IP Address** of the machine on which you installed Guest and IoT Manager.
6. Enter a hard-to-guess string as your **RADIUS Shared Secret**. Make a note of your shared secret. You will need it when you set up the RADIUS connection.
7. In the **Provisioner Access Policy field**, choose the appropriate policy.
8. Click **OK**.
9. Make sure your firewall settings permit RADIUS traffic between Guest and IoT Manager and Ignition Server. Guest and IoT Manager uses RADIUS to authenticate provisioners. Your network must allow RADIUS (UDP) traffic to travel between the Guest and IoT Manager machine and the Ignition Server.

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

Making RADIUS settings in Guest and IoT Manager

Ignition Server uses RADIUS to authenticate provisioners.

Procedure

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

5. Click **Submit**.

Testing Guest and IoT Manager RADIUS connection settings

Follow these steps to test your RADIUS setup.

Procedure

1. Create a provisioner account for yourself as explained in [Creating a Provisioner access policy](#) on page 48.
2. Open a web browser and point the web browser to the Guest and IoT Manager Provisioner application at `https://<server_name>/GuestManager/provisioner`.
3. In the Login screen, enter your provisioner **Username** and **Password**.
4. Click **Sign In**. If your login attempt fails, see [Problem: Provisioner cannot login](#) on page 243.

Setting up Email notification parameters

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

Important:

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

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

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

Note:

Google blocks sign-in attempts from unknown sources. To avoid this issue, you need to allow access to apps to get authenticated. You will find this option in your Google Account Security Setting. Select **Allow less secure apps** as **ON** to use these non-Google apps and

devices despite the risks. For more information, see <https://support.google.com/accounts/answer/6010255?hl=en>.

Procedure

1. Launch the Guest Guest and IoT Manager Administrator application.
2. Select **Administration > Notification > E-mail**.

The system displays the **Email SMTP Configuration** page.

Enable Sending of Email Notification

* From Address: john@extremenetworks.com

* Server: 198.152.7.7

Security: None SSL/TLS STARTTLS

SSL Certificate: Custom System †

* Port Number: 25

User Authentication

User Name: _____

Password: [Change](#)

* Required

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

Example configurations for a few Web Based Mail Servers:

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

3. On the Email SMTP Configuration page, check the **Enable Sending of Email Notification** check box. With this feature turned on, Guest and IoT Manager sends guest users,

provisioners, and/or others an email notification when guest user accounts are created and/or updated.

4. In the **From Address** field, type the email address that will appear in the “From” line of the messages that Guest and IoT Manager sends. For example, user provisioning notifications might contain a **From Address** such as `guestreception@idengines.com`. This address appears in all types of emails that Guest and IoT Manager sends.
5. In the **Server** field, enter the fully-qualified domain name or the IP address assigned to the mail server that will transmit email notifications from Guest and IoT Manager.

You can enter a public main server such as Gmail or Yahoo as the SMTP server.

6. For Secure Connections, select **SSL/TLS** or **STARTTLS** in the **Security** field, and do the following:
 - a. In the **SSL certificate** field, check **Custom** to import the SMTP server certificate (**Administration** > **Connection** > **Certificate**). When you successfully import the certificate, this certificate is used to establish trust with the SMTP server.

 **Important:**

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

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

The SMTP server name can be an email address.

9. **(Optional)** Click **Test** to verify that the application can reach the server at the email address that you have specified, before clicking **Submit**.

The system displays the **Test SMTP Configuration** window, enter the **Test Destination Email** and click **Send Test Email**.

10. Click **Submit**.

Make sure you set up an appropriate email notification template as shown in [Writing SMS and Email templates for account notifications](#) on page 165.

Setting up SMS notification parameters

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

Important:

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

Procedure

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

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

Phone Carrier Gateways			
Phone Carrier	Phone Carrier Gateways	Default	
<input type="checkbox"/> AT&T Wireless	txt.att.net	Yes	
<input type="checkbox"/> Bell	txt.bell.ca	No	
<input type="checkbox"/> Cingular	mycingular.net	No	
<input type="checkbox"/> Rogers	pcs.rogers.com	No	
<input type="checkbox"/> Sprint PCS	messaging.sprintpcs.com	No	
<input type="checkbox"/> T-Mobile	tmomail.net	No	
<input type="checkbox"/> Telus	msg.telus.com	No	
<input type="checkbox"/> Verizon Wireless	vttext.com	No	

3. To add a gateway, click **Add Gateway**.

The system displays the **Add Carrier Gateway** window.

Add Carrier Gateway

* **Carrier Name:**

* **Carrier Gateway:**

Default Gateway

Phone Number: **US & Canada, no leading 1**

US & Canada, leading 1 (uncommon)

Specify length: digits (single number or range. For example, 10-15)

** Required*

4. On the Add Carrier Gateway window, do the following:

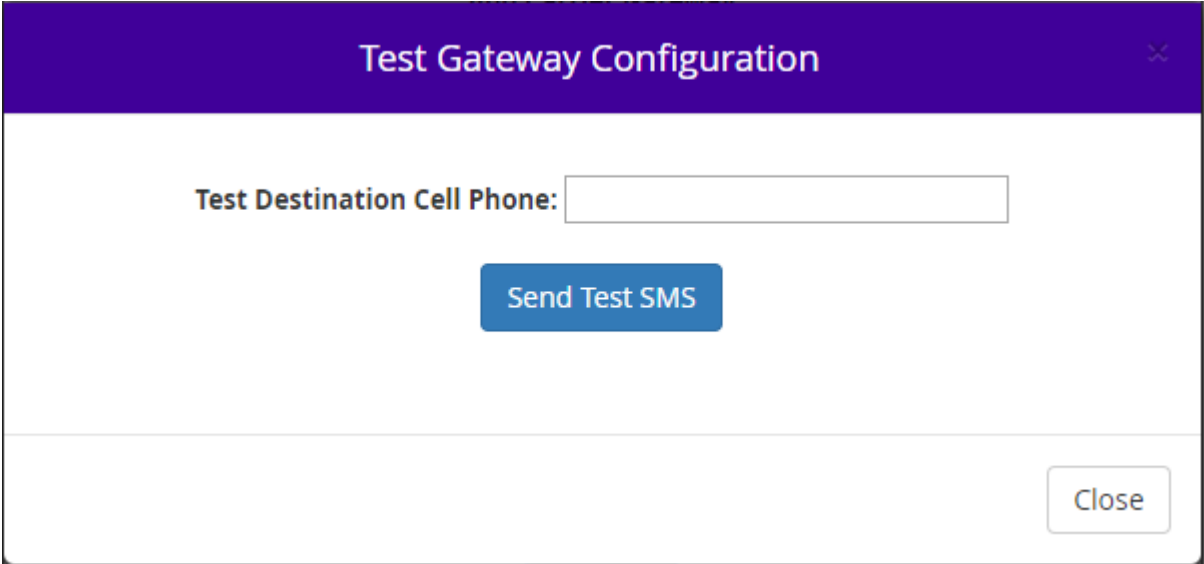
- a. In the **Carrier Name** field, enter the carrier name.
- b. In the **Carrier Gateway** field, enter the carrier gateway address.
- c. If this is the default carrier gateway, check the **Default Gateway** check box.

You can have only one default SMS gateway. If you select this gateway as the default, a warning message indicates that any previously configured default will be overridden. If you do not specify a default gateway, the first gateway in the list becomes the default gateway.

- d. Check the **Phone Number** format.

5. **(Optional)** Click **Test** to test the gateway configuration, before clicking **Submit**.

The system displays the **Test Gateway Configuration** window, enter the **Test Destination Cell Phone** number and click **Send Test SMS**.



The screenshot shows a dialog box titled "Test Gateway Configuration". It features a purple header bar with the title and a close icon. The main content area is white and contains a text input field labeled "Test Destination Cell Phone:" with a blue "Send Test SMS" button below it. A "Close" button is located in the bottom right corner of the dialog.

6. Click **Submit** on successful completion of the **Test Gateway Configuration**.
7. **(Optional)** To edit an existing gateway, click its name. In the Edit window, make the appropriate changes and click **Submit**.

Make sure you set up an appropriate SMS notification template as shown in [Writing SMS and Email templates for account notifications](#) on page 165.

Exporting and importing Guest and IoT Manager configurations

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

The configurations you can export and import include:

- Appliance configurations
- RADIUS configurations
- User certificates

- HTTPD Web server configuration (HTTP, SSL, and so on)
- User preferences
- All Guest and IoT Manager configuration SMTP, SMS Gateway, KeyStore certificates, and files present in the File Manager.

*** Note:**

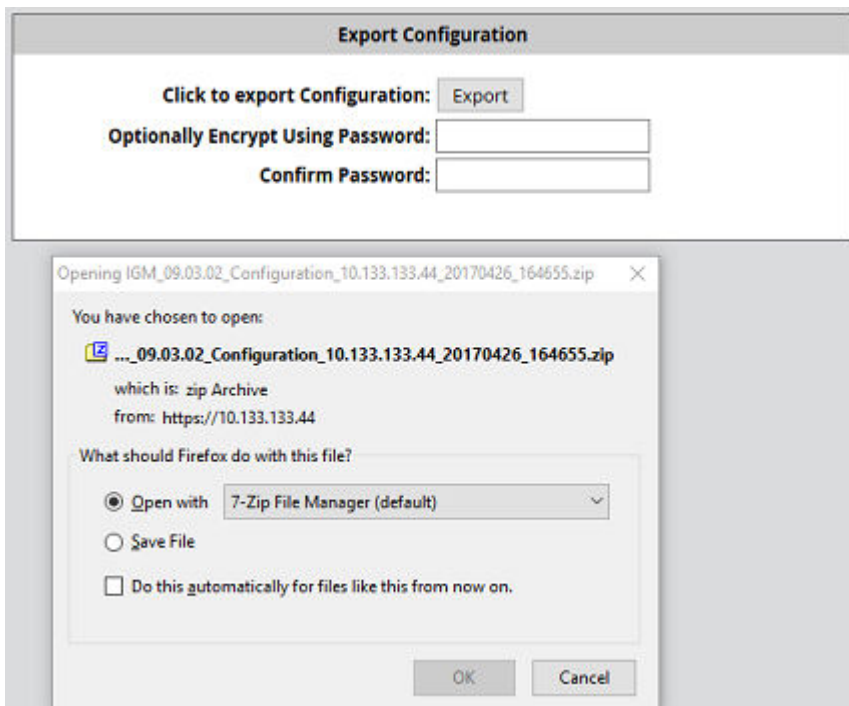
Guest Users, Devices, Provisioners, Self-Service Provisioner, and Provisioner Group configuration are stored on the Ignition Server and are not part of the Guest and IoT Manager export/import function.

Exporting a Guest and IoT Manager configuration

You can export a Guest and IoT Manager configuration.

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Administration > Export**.
2. (Optional) To encrypt and export the configuration, enter the password in the **Optionally Encrypt Using Password** field.
3. Click **Export** to export the configuration.
4. In the File Download Window, click **Save**.



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

*** Note:**

- Do not change the Guest and IoT Manager export file name. File name must be the same while importing the Guest and IoT Manager configuration.
 - Private Keys are always encrypted. The other files in the configuration are encrypted only if Password is entered by Administrator during export.
6. In the Download Complete window, click **Close**.

Scheduling Export for Guest and IoT Manager configuration

Use the following procedure to schedule the export of Guest and IoT Manager configuration.

Procedure

1. In the Guest and IoT Manager Administrator Application, click **Administration > Scheduled Export**.

The **Scheduled Export** panel appears.

2. Select the **Enable Scheduled Export** check box to enable.
3. Enter the start **Time** in hh:mm format and select the **AM** or **PM** from the drop-down.
4. Select the **Recurrence** from drop-down.

If applicable, from the drop-down specify the detailed frequency parameters. For monthly, enter the day of the month in the **Recur on Day** field; for weekly, choose the day of the week from the **Recur on Day** drop-down.

5. In the **Export to host** field, specify the machine name or IP address of destination SFTP server.
6. In **Login Name** and **New Password** field, enter the user name and password of the SFTP server account where the Guest and IoT Manager configuration files are stored.

Type the **New Password** again in the **Confirm Password** field to confirm.

- In the **Destination Path** field, specify the path where the Guest and IoT Manager configuration files are stored on the SFTP server.

- (Optional) To encrypt and export the configuration, enter the password in the **Optionally Encrypt Using Password** field.
- Click **Submit** to save the scheduled export.
- Click **Reset** to reset all the fields entered.

Note that the scheduling status and next scheduled backup information can be found under **Logs**.

Importing a Guest and IoT Manager configuration

You can import a Guest and IoT Manager configuration.

Procedure

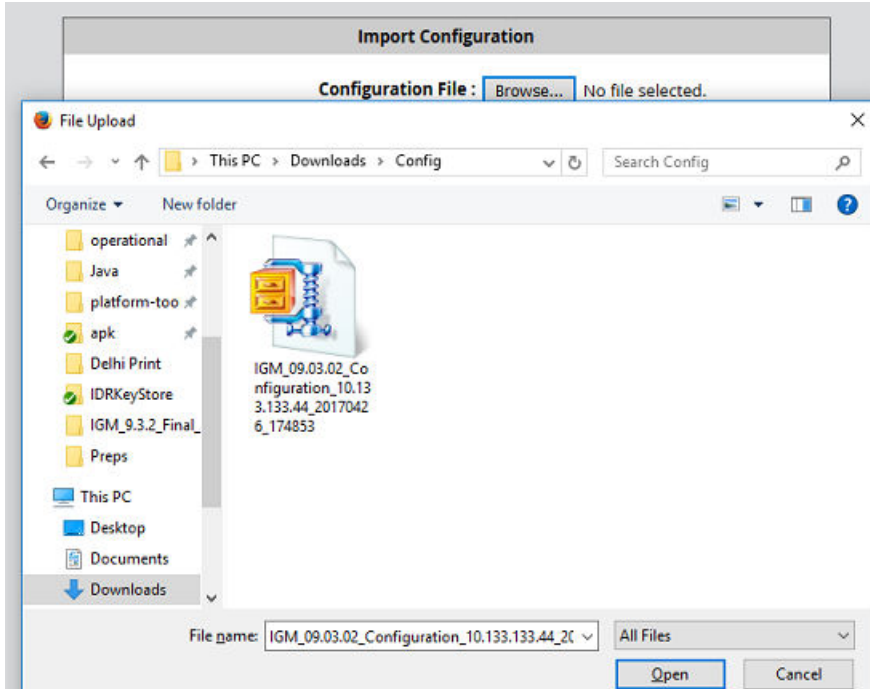
- From the Guest and IoT Manager Administrator Application, click **Administration > Import**.
- On the **Import Configuration** page, click **Browse**.
- In the **Choose file** window, select your configuration zip file, and click **Open**.

*** Note:**

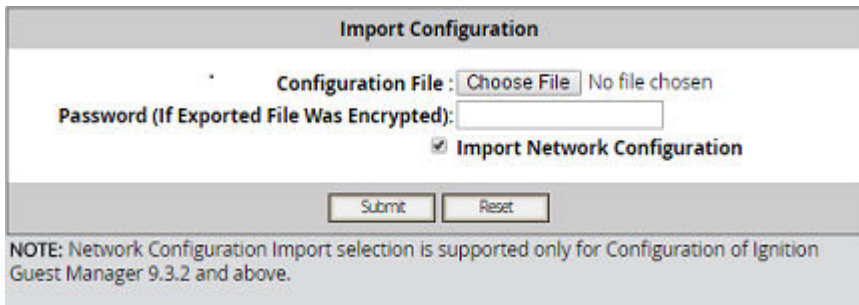
For release 9.3.2 or later, ensure the name of the Guest and IoT Manager Configuration file is IGM_<Release>_Configuration_<ip>_<YYYYMMDD><timestamp>.zip.

For release 9.3.0 or earlier, ensure the name of the Guest and IoT Manager Configuration file is GM_Configuration_<ip>_<YYYYMMDD><timestamp>.zip.

If the file naming convention does not match the format then import fails.



4. On the Import Configuration page, keep the Import Network Configuration check-box unchecked.



- Select the **Import Network Configuration** check-box to optionally include Network Configuration while importing IGM Configuration.

*** Note:**

Network Configuration Import selection is supported only for Configuration of Ignition Guest and IoT Manager 9.3.2 and above. You cannot import any network configuration from IGM 9.3 or below configuration irrespective of the check-box selection.

- Network Configuration includes the following:
 - Interface IP addresses and subnet masks
 - Static Routes
 - DNS IP addresses and domain

- All other configurations are imported irrespective of the check-box selection.
5. Click **Submit**. The Guest and IoT Manager Administrator Application displays the successful import message.
 6. Log on to the Guest and IoT Manager VM .

+ Tip:

The system automatically reboots the VM.

Managing HTTPD certificates

Guest and IoT Manager Administrator can add, bind, or delete a certificate or key.

From the Guest and IoT Manager Administrator Application, click **Administration > Certificates**.

The user can use any of the default certificate, key, and chain or add a new certificate.

Adding a certificate

About this task

Use this procedure to add a new certificate.

Procedure

1. Launch the Guest and IoT Manager Administrator application.
2. Click **Administration > Certificates**.
3. Click **Add Certificate**.
4. In the *Add Certificate* window, click **Browse** to find the new certificate file. Click **Open**.

Add Certificate

*Certificate File: Browse...

*Alias For This Certificate:

Chain Certificate

Submit Reset

NOTE: Certificate encoding format should be either **DER-encoded binary X.509** or **Base64-encoded X.509**.

* Required

5. Click **Submit**.

6. Chain Certificates:

A certificate chain is a sequence of certificates, where each certificate in the chain is signed by the subsequent certificate. The purpose of a certificate chain is to establish a chain of trust from a peer certificate to a trusted CA certificate.

The Chain Certificate check box needs to be selected in order to upload a chain certificate.

The added Certificate details are displayed in the HTTPD Certificates table.

Adding a key

About this task

Use this procedure to add a new key.

Procedure

1. Launch the Guest and IoT Manager Administrator application.
2. Click **Administration** > **Certificates**.
3. Click **Add Key**.
4. In the Add Key window, click **Browse** to find the new key file. Click **Open**.

The screenshot shows a dialog box titled "Add Key". It contains two required fields: "* Private Key File:" with a text input and a "Browse..." button, and "* Alias For Private Key:" with a text input. At the bottom are "Submit" and "Reset" buttons. A red asterisk and the word "Required" are shown at the bottom left of the dialog.

5. Click **Submit**.

Binding certificate

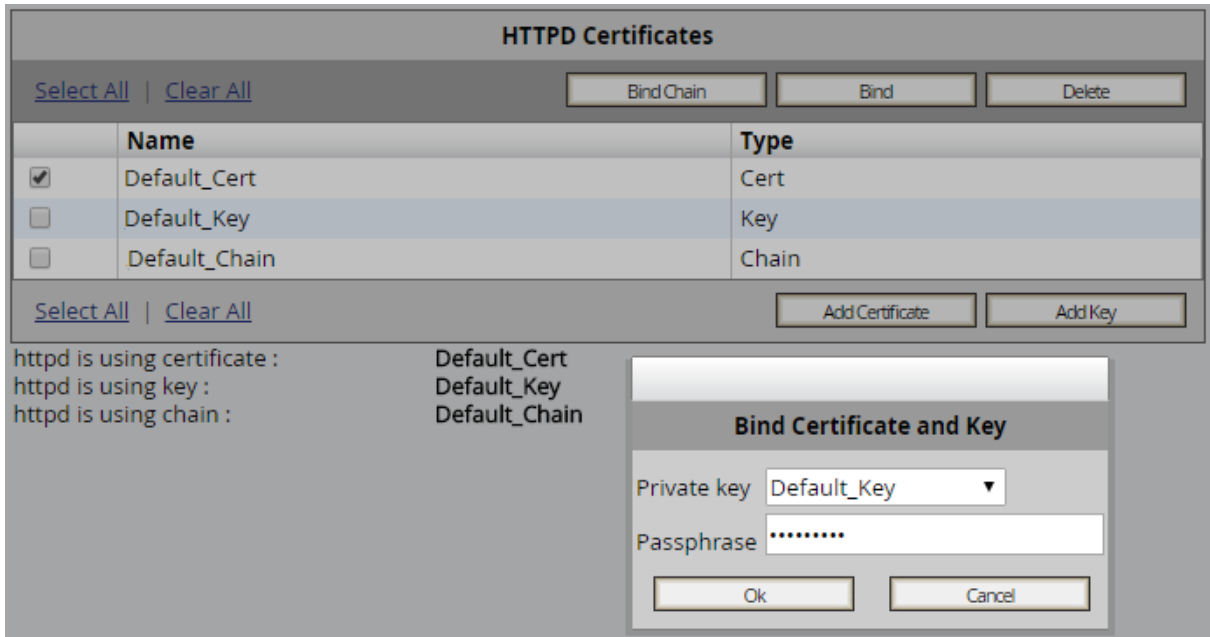
About this task

Use this procedure to bind a Key and a certificate to the HTTPD server.

Procedure

1. Launch the Guest and IoT Manager Administrator application.
2. Click **Administration** > **Certificates**.
3. Select the check box of the certificate you want to bind.

- Click **Bind**.
- In the *Bind Certificate and Key* window, select the required **Private Key** from the drop-down list.



- Optional:** In the *Bind Certificate and Key* window, enter the **Passphrase** for the selected Private Key.

Ensure that you provide the valid passphrase, so that the bind does not fail and result in HTTPD restart failure.

- Click **OK**.

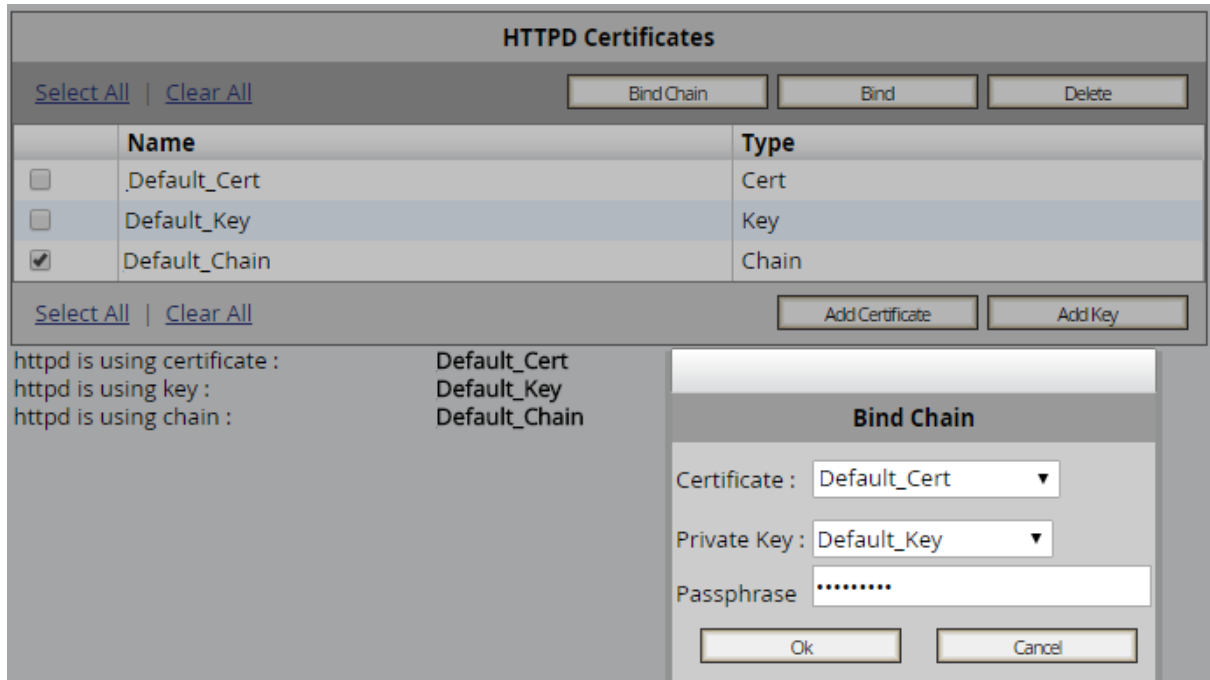
Binding a chain

About this task

Use this procedure to bind a Certificate Chain to HTTPD server.

Procedure

- Launch the Guest and IoT Manager Administrator application.
- Click **Administration > Certificates**.
- Select the check box of the Chain certificate you want to bind.
- Click **Bind Chain**.
- In the *Bind Chain* window, select the required **Certificate** and **Private Key** from the drop-down list.



6. **Optional:** In the *Bind Chain* window, enter the **Passphrase** for the selected Certificate and Private Key.

Ensure that you provide the valid passphrase, so that the bind does not fail and result in HTTPD restart failure.

7. Click **OK**.

Deleting Certificates

About this task

Use this procedure to delete Certificates and Keys except for the active HTTPD Certificate/Key.

Procedure

1. Launch the Guest and IoT Manager Administrator application.
2. Click **Administration > Certificates**.
3. Select the check-box of the Certificate(s)/Keys you want to delete.
4. Click **Delete**.
5. Click **OK** to confirm.

Chapter 6: Managing Guest and IoT Manager

This chapter is intended for the Identity Engines Guest and IoT Manager Administrator and describes how to manage the Guest and IoT Manager applications. If you are a provisioner, you may skip this chapter and proceed to [Provisioner application: Managing guests and devices](#) on page 196.

Important:

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

Running the Guest and IoT Manager Administrator application

Procedure

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

The Guest and IoT Manager Administrator application appears.

Warning:

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

Performing as both Administrator and Provisioner

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

You must have two accounts: the Guest and IoT Manager Administrator account and a Provisioner account. Only the Guest and IoT Manager Administrator may run the Administrator Application, and only provisioners may run the Provisioner Application. See [Guest and IoT Manager application in context](#) on page 16.

Use the following steps to switch between the applications.

 **Warning:**

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

Procedure

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

Restarting Guest and IoT Manager

Procedure

1. Log in to the Guest and IoT Manager virtual appliance and launch the Guest and IoT Manager console. Enter the username and password.
2. Enter `tomcat stop`.
3. Enter `tomcat start`.
4. To restart the httpd server, enter `httpd restart`.
5. Reconnect to the Identity Engines Ignition Server as described in [Connecting Guest and IoT Manager to the Ignition Server Appliance](#) on page 78.

Connecting Guest and IoT Manager to the Ignition Server Appliance

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

Guest and IoT Manager does not automatically connect to the Ignition Server upon start-up. Connect Guest and IoT Manager to the Ignition Server as follows:

Procedure

1. Run the Guest and IoT Manager Administrator Application.
2. Log in as the Guest and IoT Manager Administrator. Do not allow the browser to remember the password.
3. Click on **Administration > Connection > Appliance** in the main toolbar of the Administrator Application.
4. In the **Login To Appliance** window, type the **Username** and **Password** of the Ignition Server SOAP API user account. The **Host** and **Port** settings should have been set already. If they are not set or set incorrectly, see [Making SOAP settings on the Ignition Server](#) on page 56.
5. Click **Connect**.

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



Ignition Guest & IoT Manager

Administrator: admin
Connected: 10.133.133.221 (First Appliance)

Last successful login: 2017-09-20 17:59:41
Failed login attempts: 0

Logout

Disconnecting Guest and IoT Manager from the Ignition Server Appliance

Procedure

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

Once you log out of the Ignition Server appliance, Guest and IoT 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 and IoT Manager Administrator are

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

Use the steps below to change the username or password of the Guest and IoT Manager Administrator. Do not confuse this account with the Ignition Server Administrator account or with the provisioner accounts. See page [Guest and IoT Manager Introduction](#) on page 16 for details.

Procedure

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

 **Note:**

The new password must meet the following complexity checks:

- Use minimum of eight characters in the password.
 - Password must be a combination of the following character types:
 - Include at least one lowercase letter
 - Include at least one uppercase letter
 - Include at least one number
 - Include at least one special character from `!, @, #, $, %, ^, &, *, (,), -, +`
 - New password cannot match the three recently used passwords.
- d. Type the new password again in the **Confirm Password** field.

! Important:

It is recommended that you change the Guest and IoT Manager Administrator password after you have completed the initial setup of Guest and IoT Manager.

6. Click **Submit**.

Example

The system displays the following error message if the password does not meet the complexity criteria:

The screenshot shows a web form titled "Administrator Account". At the top, a red error message reads: "Failed to set the admin account's password. Password Complexity has not been met! Use the following guidelines for passwords: -Use a minimum of 8 characters -Include at least one capital letter -Include at least one lowercase letter -Include at least one number -Include at least one special character from !, @, #, \$, %, ^, &, *, (,), -, +". Below the error, the form fields are: "Administrator User Name" (admin), "Administrator Password" (Cancel), "Current Password" (empty), "New Password" (empty, with "Invalid" in red to its right), "Confirm Password" (empty), and "Administrator Idle Timeout (min.):" (30, with "(1 - 60)" to its right). At the bottom are "Submit" and "Reset" buttons. A red asterisk and the word "Required" are at the bottom left.

Setting Administrator Preferences

This section describes the procedures to change the administrator preferences like changing the application logo, name, color and language.

Customizing the IDE Ignition Guest and IoT Manager Logo and Login Page


Use the following procedure to customize the logo of the IDE Ignition Guest and IoT Manager.

Procedure

1. In a supported web browser, enter the Guest and IoT Manager Administrator URL ([https://<server_name>/Guest and IoT Manager/admin](https://<server_name>/Guest%20and%20IoT%20Manager/admin)).
2. Enter the **User ID** and **Password**. The default **User ID** and **Password** is `admin` and `admin`.
3. Go to **Administration > Preferences** .

The system displays the **User Preferences** page.

User Preferences

Current Logo:  **Extreme**
Connect Beyond the Network

New Logo (GIF format, 160 x 44): No file chosen










Logo URL:

*** Application Name:**

*** Administrator Page Color:** #400099

*** Provisioner Page Color:** #400099

Language Preference:
(Select maximum of 3 languages and 1 among them as default)

Language		Available to Provisioners	Default
English-US		<input checked="" type="checkbox"/>	<input checked="" type="radio"/>
French		<input type="checkbox"/>	<input type="radio"/>
German		<input type="checkbox"/>	<input type="radio"/>
Spanish		<input type="checkbox"/>	<input type="radio"/>
Italian		<input type="checkbox"/>	<input type="radio"/>
Portuguese		<input type="checkbox"/>	<input type="radio"/>
Swedish		<input type="checkbox"/>	<input type="radio"/>
Dutch		<input type="checkbox"/>	<input type="radio"/>
Russian		<input type="checkbox"/>	<input type="radio"/>

Terms of Use:

Display Terms of Use in Login pages

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

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

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

Due to browser caching, changes may not be visible without clearing the cache and refreshing the page/restarting browser.

* Required

4. Click **Browse** to browse the logo.

*** Note:**

The format of the image should be Graphics Interchange Format (GIF) and width and height of the image should be 160 x 44 pixels.

5. **(Optional)** To configure the Logo as a button, enter the specified URL address in the **Logo URL** field, in the **User Preferences** panel.

If the URL is configured, then clicking on the Logo will open the URL in a new tab.

6. **(Optional)** Select **Display Terms of Use in Login pages** to display the Terms of use information on the Login page. By default, the check box is selected.

*** Note:**

You can edit the default text given in the **Terms of Use** section as its a free form text box.

7. Click **Submit** to change the settings.

Changing Application Name and Page Color

Use the following procedure to change the application name and application page color.

Procedure

1. Go to **Administration > Preferences**.
The **User Preferences** panel appears.
2. In the **Application Name** field, enter the application name that you want to change.
3. To change the **Administrator Page Color**, enter the color code in the **Administrator Page Color** field.
4. To change the **Provisioner Page Color**, enter the color code in the **Provisioner Page Color** field.

The screenshot shows the 'User Preferences' panel with the following fields and values:

- Current Logo:** Extreme (with logo image and tagline 'Connect Beyond the Network')
- New Logo (GIF format, 160 x 44):** Choose File (No file chosen)
- Logo URL:** https://www.google.com
- * Application Name:** Ignition Guest & IoT Manager
- * Administrator Page Color:** #400099
- * Provisioner Page Color:** #400099

5. Click **Submit**.

Changing the Language Preference


Use the following procedure to change the Administrator language preference of the Guest and IoT Manager application.

Procedure

1. Go to **Administration > Preferences**.
The **User Preferences** panel appears.

2. In the **Language Preference** section, select the desired languages check box.

User Preferences

Current Logo:  **Extreme**
Connect Beyond the Network

New Logo (GIF format, 160 x 44): No file chosen










Logo URL:

*** Application Name:**

*** Administrator Page Color:** #400099

*** Provisioner Page Color:** #400099

Language Preference:
(Select maximum of 3 languages and 1 among them as default)

Language	Available to Provisioners	Default
English-US 	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>
French 	<input type="checkbox"/>	<input type="radio"/>
German 	<input type="checkbox"/>	<input type="radio"/>
Spanish 	<input type="checkbox"/>	<input type="radio"/>
Italian 	<input type="checkbox"/>	<input type="radio"/>
Portuguese 	<input type="checkbox"/>	<input type="radio"/>
Swedish 	<input type="checkbox"/>	<input type="radio"/>
Dutch 	<input type="checkbox"/>	<input type="radio"/>
Russian 	<input type="checkbox"/>	<input type="radio"/>

Administrator can select a maximum of three languages including default language.

Administrator can select any one of the three languages as default by selecting the radio button.

3. Click **Submit**.

The configured Flags are displayed on the Guest and IoT Manager Provisioner's Page, Self-Provisioning Portal page and Sponsor Action Page.

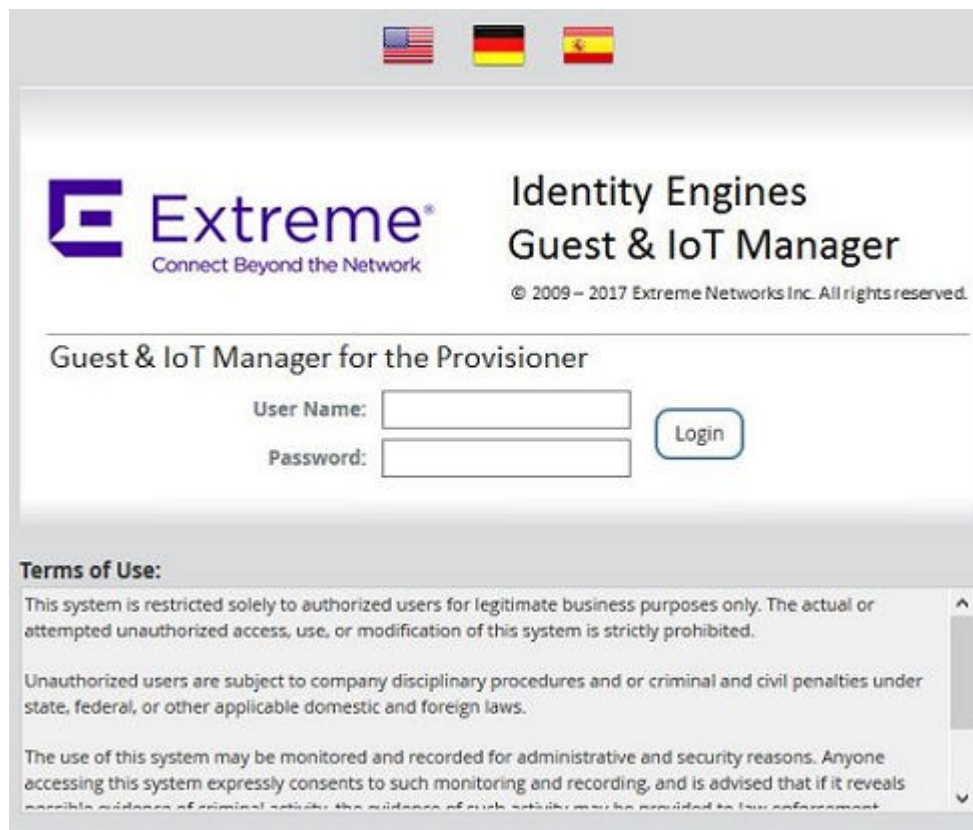
Guest and IoT Manager Provisioner

The first page loads with the **Default** language selected. On clicking a desired language flag, the page reloads with the selected language.

The Provisioner will have the option to select language only in the login page

The Language selected in the login page is used throughout the Provisioner's session.

Provisioner's language preference is stored in his browser as a persistent cookie and used for subsequent sessions. Provisioner can change this by selecting any other flag and this overwrites the cookie.



Self-Provisioning Portals:

The **Self-Provisioning Portals** will have Flags selected by the admin in **Preferences** section.

The Flags are displayed in both Guest User and Device registration page.

Register New Device

* User Name:

* Password:

* MAC Address:

Type: ----- Select One ----- ▾

Sub Type:

Register New Guest User

* First Name:

* Last Name:

* User Name:

* Email:

* Cell Phone:

Carrier: AT&T Wireless ▾

Sponsor

Your access request requires Sponsor approval:

* First Name:

Last Name:

* Email: @extremenetworks.com ▾

Cell Phone:

** Required*

Sponsor Action:

The Sponsor Action page also will have Flags displayed.

Register New Guest User

First Name: Karthik
Last Name: Anand
User Name: anand17
Email: anand17@extreme.com

Message to Guest:

Approve Deny/Lock

Editing E-mail notification settings

You may set up the e-mail notification settings as explained in [Setting up Email notification parameters](#) on page 62.

Editing SMS Notification Settings

Creating SMS Gateways

You can set up SMS notification settings as explained in [Setting up SMS notification parameters](#) on page 65.

Deleting SMS Gateways

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

Procedure

1. Make sure the gateway you will delete is not currently in use by any guest user on the system.
2. Run the Guest and IoT 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 and IoT Manager application sessions automatically disconnect if the period of inactivity exceeds the applicable timeout threshold.

Provisioner Idle Timeout Threshold

The provisioner idle timeout period causes the Guest and IoT 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 132.

Setting Administrator Session Timeout Threshold

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

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

SOAP Client Timeout Threshold

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

Setting the SOAP Client Timeout period

Follow the instructions in [Making SOAP settings on the Ignition Server](#) on page 56.

Restoring a timed out server connection

In most cases Guest and IoT Manager will reconnect automatically. If it does not reconnect, reconnect it manually as explained in [Connecting Guest and IoT Manager to the Ignition Server Appliance](#) on page 78.

Logs

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

Viewing the log files

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

```

Log File: GuestManager.log

2017-08-31 09:25:40,
JDK Version: 24.91-b01
Platform: Linux amd64

2017-08-31 09:25:40, An attempt to connect to appliance is aborted because of incomplete login information.
2017-08-31 09:25:40,
2017-08-31 09:25:40,
2017-08-31 09:25:40, Failed to initialize application configuration.
2017-08-31 09:25:40,
2017-08-31 09:25:40, Ignition Guest & IoT Manager started and ready.
2017-08-31 09:31:17, User=admin, action=Login, record=Guest & IoT Manager administrator, result=Successful
2017-08-31 09:31:28, Could not connect to 10.133.133.221 because: ; nested exception is:
    java.net.ConnectException: Connection refused
2017-08-31 09:31:28, SOAP service might be disabled.
2017-08-31 09:41:33, Connected to 10.133.133.221 by 195.27.104.124
2017-08-31 09:42:12, User=admin, action=Create, record=test_PG, result=Successful
2017-08-31 09:42:12, New provisioning group "test_PG" was successfully created by "admin"
Provisioning Group: test_PG
Access:
2017-08-31 09:44:39, User=admin, action=Update, record=test_PG, result=Successful
2017-08-31 09:44:39, Provisioning Group "test_PG" was successfully updated by "admin"
Provisioning Group: test_PG
Access:
2017-08-31 09:45:09, User=admin, action=Update, record=test_PG, result=Successful
2017-08-31 09:45:09, Provisioning Group "test_PG" was successfully updated by "admin"
Provisioning Group: test_PG
Access:
2017-08-31 09:46:44, User=admin, action=Create, record=test, result=Successful
2017-08-31 09:46:44, New provisioner "test" was successfully created by "admin"
Provisioner: test
First Name: test
Last Name: test
Email Address: test@test.com
Comments:
Provisioning Groups:
    test_PG
2017-08-31 09:47:30, User=, action=Login, record=Guest & IoT Manager provisioner, result=Unsuccessful
2017-08-31 09:47:32, User=as, action=Login, record=Guest & IoT Manager provisioner, result=Unsuccessful
2017-08-31 09:49:27, User=test, action=Login, record=Guest & IoT Manager provisioner, result=Unsuccessful
2017-08-31 09:49:35, User=admin, action=Login, record=Guest & IoT Manager administrator, result=Successful
2017-08-31 09:49:42, ----- Send -----
Class: class net.sf.iradius.packet.AccessRequest

```

Figure 8: Contents of the GuestManager.log File

Chapter 7: Setting guest authorization policies

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

If you are in a hurry to create some guest users, you can skip most of the policy setup procedure. See [Creating a minimal authorization policy](#) on page 116.

Setting authorization policies for guest users

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

Access constraint check boxes on the Create Guest User page

Provisioners use the Create Guest User page of Identity Engines Guest and IoT 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 and IoT Manager Administrator determines which check boxes each provisioner sees.

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

Create Guest User

Associated Provisioning Group:

* **Group Membership:** SunnyvaleFrontDesk ▼

Guest User Info:

* **First Name:** Johnnie

* **Last Name:** Taylor

* **User Name:** jtaylor

* **Password:** F0rmula4D

Email: jtaylor@company.com

Cell Phone: 4155554343 **Carrier:** AT&T Wireless ▼

Delete on Expire: Yes No

Comments:

Guest Details:

* **Activate Account On:** 2015/11/18 10:13:16 AM ▼ GMT+00:00

* **Duration:** 8 hours ▼ (Max 8 hours)

Network Rights: Internet Campus-Internet

Access Zones: Building-1-Public-Areas

Associated Devices:

[Add...](#)
[Remove](#)

Send Notification:

Other Email:

Figure 9: Example Guest User Provisioning Form

Three classes of access constraints are available:

- **Access Type:** The mechanisms of network access the guest user is permitted to use, such as wired, wireless, or secured wireless. To create an access type, create an internal user group in Ignition Dashboard with its type set to **accessType**. The provisioner may tick more than one **Access Type** check box to let the user connect in multiple ways.
- **Network Rights:** The network realm to which the guest user has access, such as the Internet only, or the southeast regional sales department VLAN. To create a network right, create an internal user group in Ignition Dashboard with its type set to **networkRight**. The provisioner

may only tick one **Network Right** check box, because the user must be assigned to one and only one VLAN or segment of the network.

- **Access Zones:** The physical locations at which the guest user can connect to the network. Each is typically the location of a switch or access point. To create an access zone, create an internal user group in Ignition Dashboard with its type set to **accessZone**. The provisioner may tick more than one **Access Zone** check box to let the user connect from multiple locations around the facility.

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

Authorization policies

To set up the guest authorization policies that you will enforce with Guest and IoT Manager, you write authorization policies in Ignition Server just as you would for any other user. Authorization policy decisions are made on the basis of a user's membership in virtual groups. This document explains how to set up an example policy. For additional information, see *Identity Engines Ignition Server Configuration, NN47280-600*.

Mapping internal user groups to virtual groups

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

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

Sample authorization policies

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 and IoT Manager application. The section [Step-by-step configuration in Ignition Dashboard](#) on page 96 shows you how to make these settings in Guest and IoT Manager.

The Example

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

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

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

Access constraint check boxes

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



The constraint check boxes that a provisioner sees in the Create Guest User screen of Guest and IoT Manager are generated from the internal user groups saved on your Ignition Server appliance. Each provisioner sees only those check boxes that the Guest and IoT 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 and IoT Manager 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](#) on page 94.

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

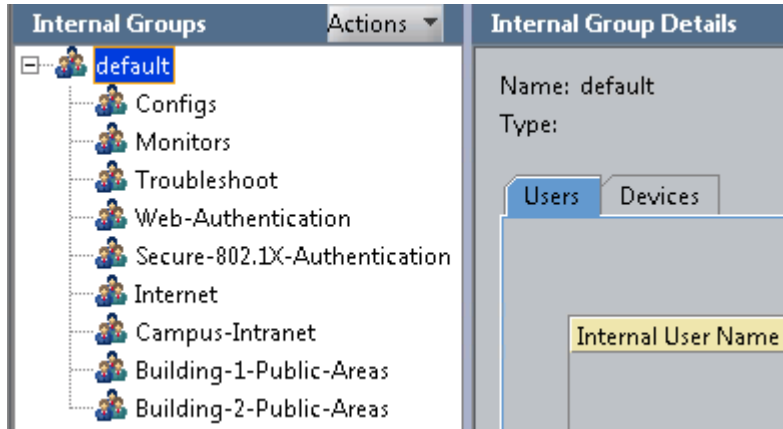
Procedure

1. Run Ignition Dashboard ([Launching Ignition Dashboard](#) on page 245) and log in as the Ignition Server Administrator.
2. Create the new internal user groups as follows.

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

- a. In the Ignition Dashboard main navigation tree, click **Directories: Internal Store: Internal Groups**. The application displays the Internal Groups panel.
- b. In the **Internal Groups** pane, right-click on the root group (usually called “default”) and select **Actions: Add New Internal Group**. The application displays the Add a New Internal Group dialog, where you name the new internal group:
 - Enter the **Internal Group Name**, “Web-Authentication”.
 - In the **Type** field, specify the group type (also known as the access constraint class); this is also the name of the Access Constraint check box that will appear in the Guest and IoT Manager application. For the “Web-Authentication” group, specify a **Type** of “accessType”. This instructs Guest and IoT Manager to display the group in the Access Type section of the Create Guest User page.
 - Tick the **Automatically create** check box. (Note that if you wished to map multiple internal groups to one virtual group, you would leave this check box unticked now and map the groups manually later.)
 - Click **OK**. The Add New Internal Group window closes.

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

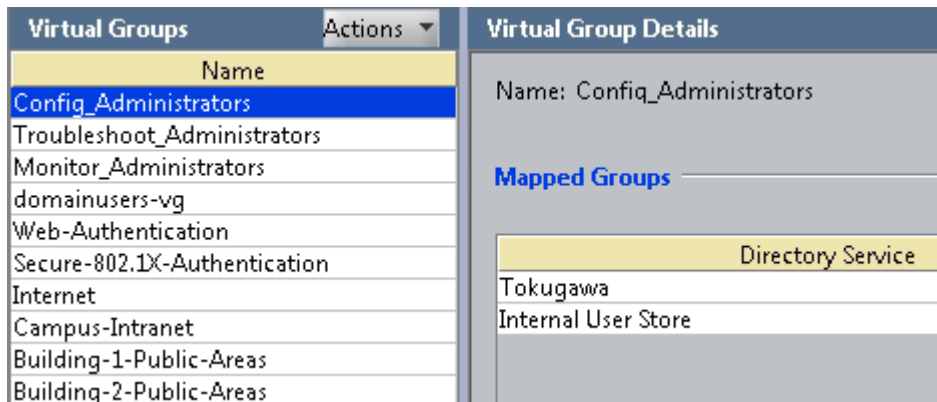


- c. Repeat Step 2 for the remaining internal groups to be created. If you are replicating the example, create all the groups listed in the preceding table.

! Important:

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

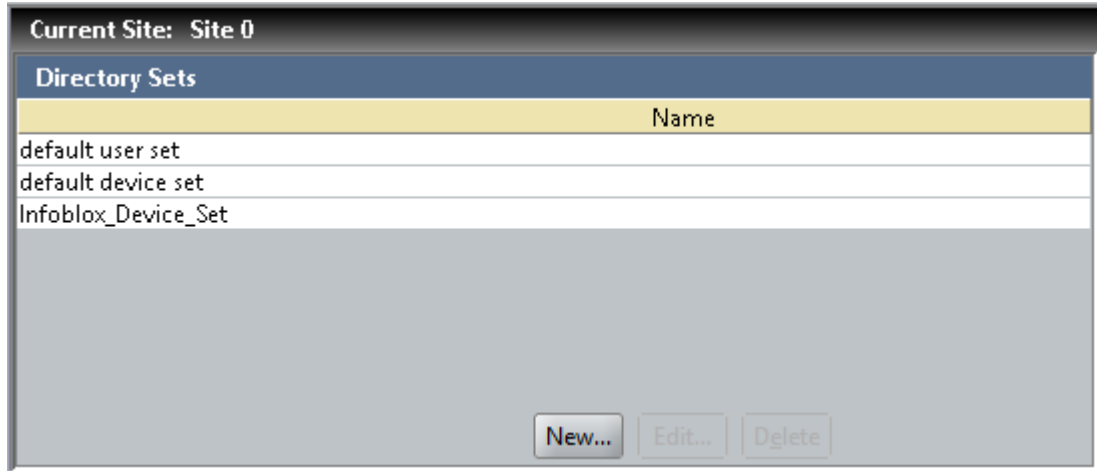
When you have added the final new internal group entry, the Internal Groups panel and the Virtual Groups panel will look similar to the figures.



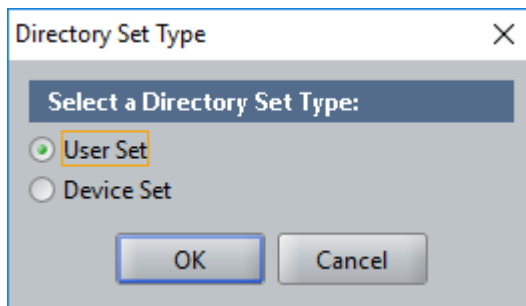
3. Create a Directory Set for the guest users.

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

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

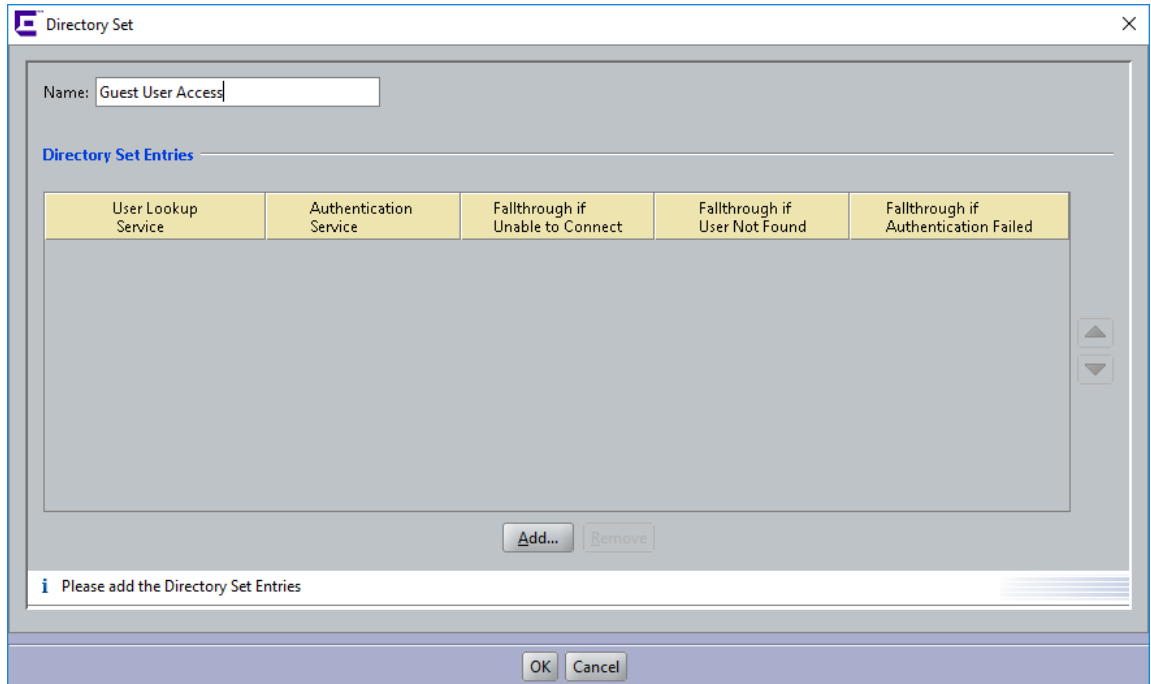


- b. Click the **New** option at the beneath of the window. The *Directory Set Type* window appears.

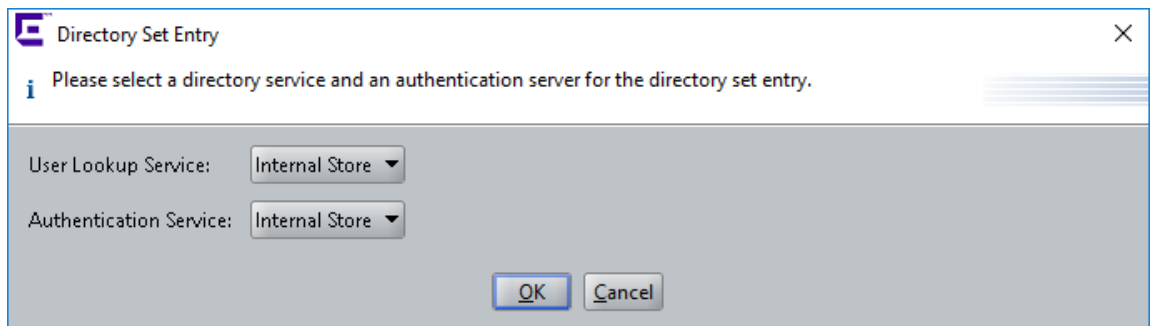


- c. Select the required directory set type option and click **OK**.
The *Director Set* screen is as displayed:

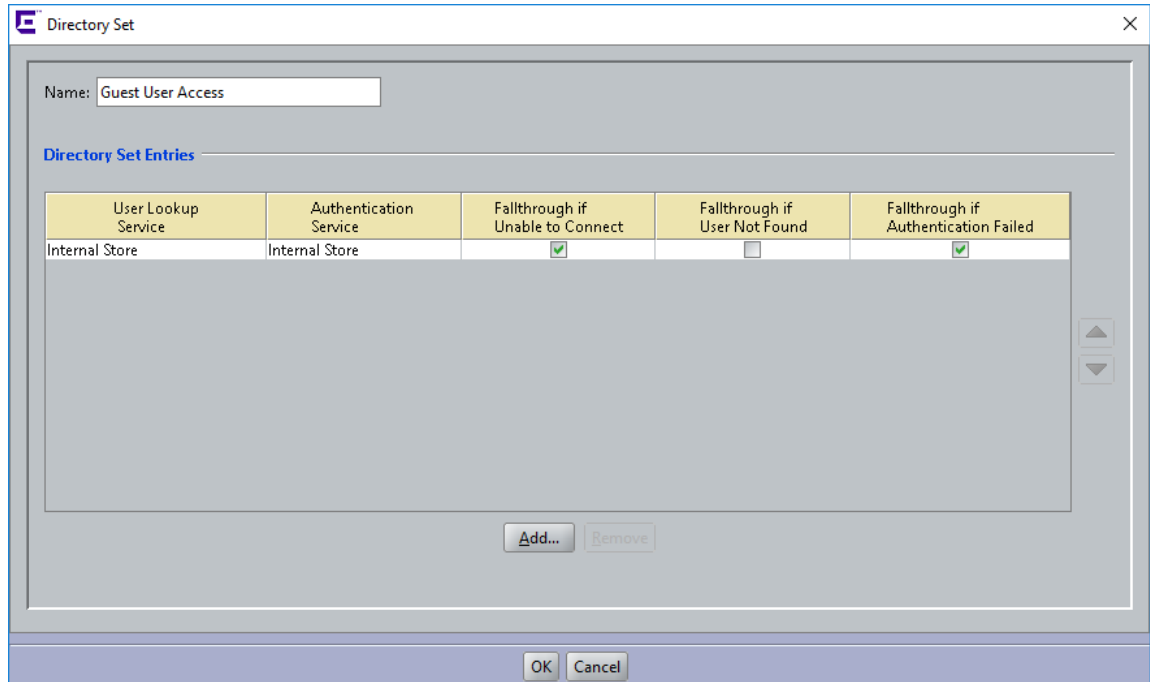
Setting guest authorization policies



- d. Enter the name for the directory set (“Guest User Access” in the example) and click **Add**.
- e. Next, add the guest user directory to the directory set. In the Directory Set Entry window, select “Internal Store” under **User Lookup Service**, and select “Internal Store” under **Authentication Service**. Click **OK**.



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



- f. 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.

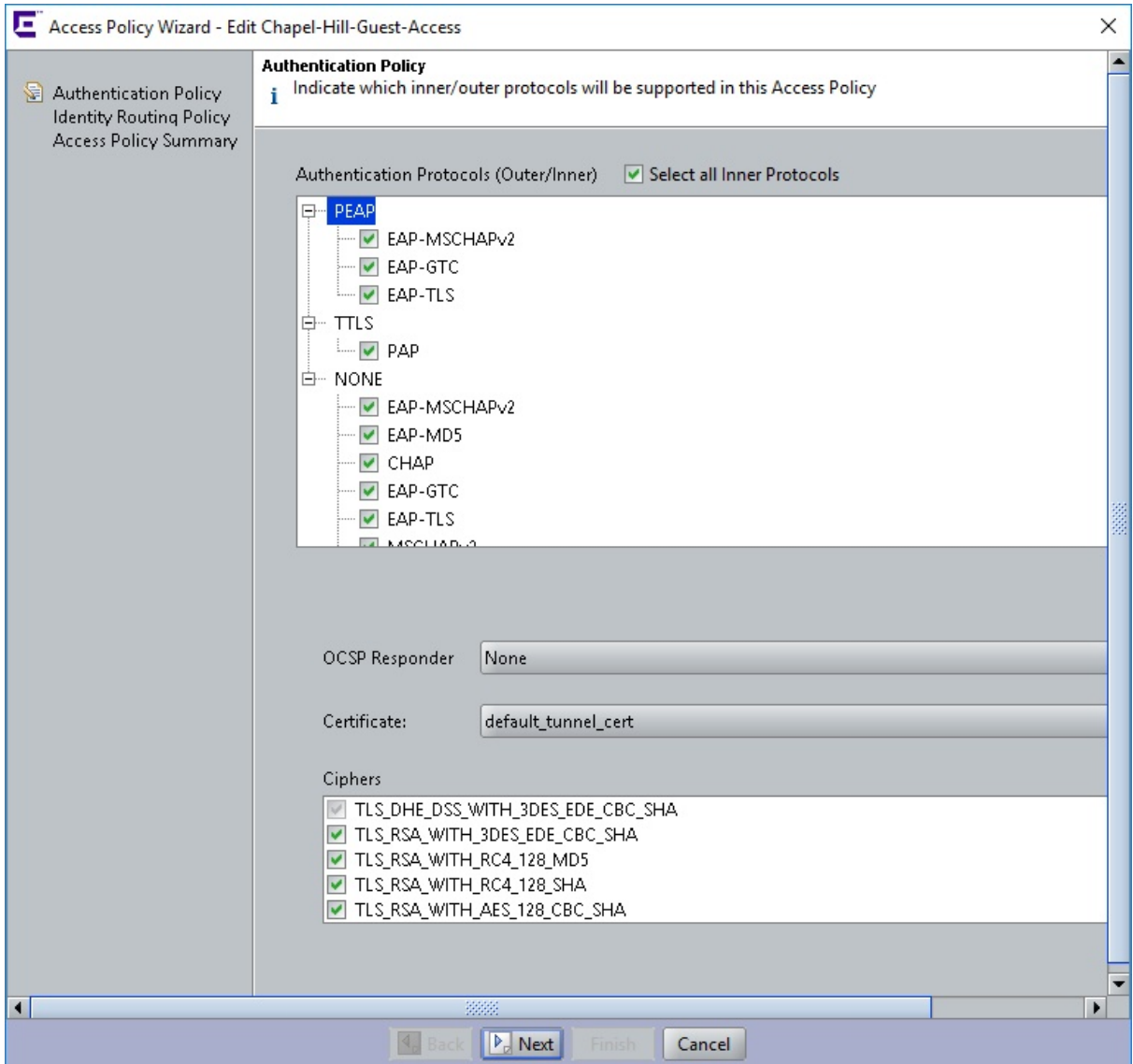
4. Create the Radius Access Policy

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.”

- In Ignition Dashboard main navigation tree, expand **Access Policies** and click on **RADIUS**. At the bottom of the main panel, click **New**.
- In the *New Access Policy* window, type the name, “Chapel-Hill-Guest-Access” and click **OK**.
- In the Access Policies panel, click the name of your new access policy and click the **Edit** button. The application displays the **Access Policy Wizard**.

5. Set up the Allowed Authentication Types.

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



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

- Under PEAP, tick *EAP-MSCHAPv2*
- Under NONE, tick *EAP-MSCHAPv2*, *MSCHAPv2*, and *PAP*
- Select the required Online Certificate Status Protocol responder from the **OCSP** field drop-down list.
- Leave the **Certificate** and **Ciphers** fields set to their defaults.
- Click **Next**.

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

6. Set up Identity Routing.

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

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

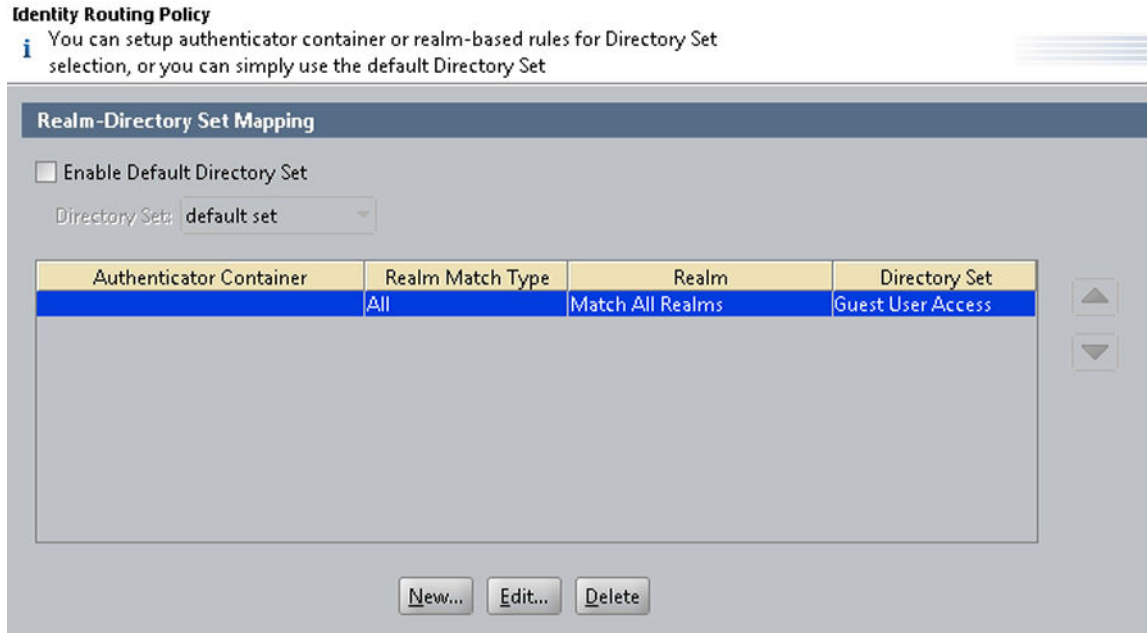
The screenshot shows the 'Realm-Directory Set Map' dialog box. It has a title bar with a close button. The main content is organized into sections:

- Directory Set:** A dropdown menu currently showing 'Guest User Access'.
- Matching Rules:**
 - Match Realm:**
 - Match All Realms (highlighted with a yellow box)
 - Realm Not Specified
 - Match Realm: [text input field]
 - Match Realm in Username: [text input field]
 - Match Realm Containing: [text input field]
 - Match Authenticator Container:**
 - Disable Authenticator Container Matching
- Tree View:** A tree structure showing a 'default' folder containing two sub-items: 'Chapel-Hill-Building-1' and 'Chapel-Hill-Building-2'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

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

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

- c. Click **Next**.
- d. Click **Finish**.



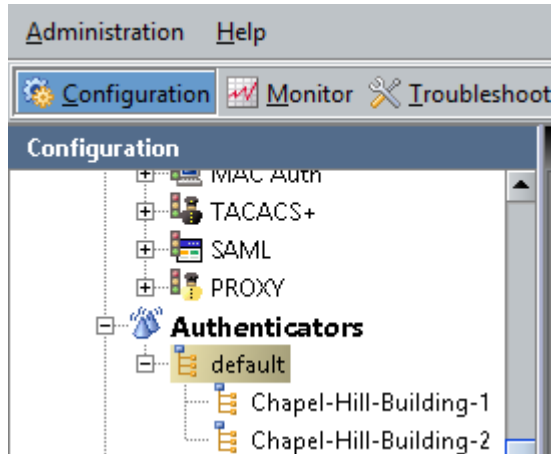
7. Create Your Authenticator Hierarchy to label your locations.

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

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

Set this up as follows:

- a. In Dashboard's main navigation tree, expand the **Authenticators** node. This displays the root node of your **Authenticator Container Hierarchy**.
- b. Select on the root node (usually called, "default") and right click to select **Add Container**.
- c. In the **Container Name** field, type the name of your first location. For this example, the name is "Chapel-Hill-Building-1". Click **OK**.



- d. Now add a container for your second location. In the **Container Hierarchy**, click the root or default node again and right click to select **Add Container**.
 - e. In the **Container Name** field, type “Chapel-Hill-Building-2” (if you are following the example). Click **OK**.
8. Create your Authenticators.

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

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

Follow these steps to create and label the authenticators:

- a. In Dashboard’s navigation tree, under the **Authenticators** node, click on the name of one of the authenticator containers you created.
- b. On the right side of the window, click **New** to add an authenticator.

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

- In the **Access Policy** drop-down list, choose *Chapel-Hill-Guest-Access*.
- Click **OK**.

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

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

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

The preceding section showed how to label authenticators by placing them in authenticator containers. This section will show another way that Ignition Server lets you label authenticators: by applying a custom Ignition Server device template to them. Your policy rules can then read the device template’s name and use it to make access decisions.

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

Set up the device template as follows:

- From the Dashboard main navigation tree, expand **Provisioning > RADIUS > Vendors/VSAs**.
- In the **Vendors** list, scroll down, expand the **IdEngines** node, and click **Device Template**.
- Click **New**.

The *New Device Template* screen is as displayed:

The screenshot shows a dialog box titled "New Device Template" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Device Template Name:** A text input field containing "600S".
- Device Template Vendor:** A text input field containing "IdEngines".
- VLAN Method:** A section with two radio buttons:
 - Use VLAN Label
 - Use VLAN ID
- MAC Authentication:** A section with a dropdown menu showing "Inbound-Calling-Station-Id".
- Buttons:** "OK" and "Cancel" buttons at the bottom.

- d. In the *New Device Template* screen, 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**. The *Edit Device Template* screen is displayed.
- e. In the *Edit Device Template* screen, click **Done** to close the screen or click **New** to repeat the same procedure to add more device templates.

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

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

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

- a. In Dashboard’s navigation tree, under the Authenticators node, click on the name of the authenticator container that will contain your 600S device (in this example, click the container for Chapel-Hill-Building-1).
- b. On the right side of the window, click **New** to add an authenticator.
- c. Create your authenticator record, but with the following changes:
 - Choose an Authenticator Type of **Other**.
 - Set Vendor to **IdEngines**.
 - Select the Device Template, **600S**.
- d. Click **OK**.

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

11. Create outbound values for assigning users to VLANs.

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

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

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

- a. In Dashboard's navigation tree, expand the **Provisioning** node and click Outbound Values. At the bottom of the **Outbound Values** panel, click **New**.
- b. In the Outbound Value Details window, in the **Outbound Value Name** field, type `VLAN Internet`.
- c. Below the **Outbound Attribute** table, click **New**.
- d. The Outbound Value Instance window lets you add the name/value pair that this outbound value will send to the Ignition Server.
 - In **Choose Global Outbound Attribute** drop down box, select **VLAN**.
 - Click the **Fixed Value** radio button.
 - In the **VLAN Label** field or **VLAN ID** field, type the label or number of the VLAN as it is configured in your switch or VLAN concentrator. In this example, we use a sample label of `"VLAN_Internet"` and a sample ID of `"10"`.
 - Click **OK**.
- e. In the Outbound Value Details window, click **OK**. Now your "VLAN Internet" outbound value is ready to use. Next, create the "VLAN Intranet" outbound value.
- f. Create another outbound value, this time calling it `"VLAN Intranet"` instead of `"VLAN Internet"`. Use the same steps you used to create the `"VLAN Internet"` value above. For this example, we use the VLAN Label, `"VLAN_Intranet"`, and the VLAN ID, `"20"`.

Outbound Value Name:

Outbound Attribute	Value
VLAN	VLAN Label = VLAN_Internet, VLAN ID = 10
VLAN	VLAN Label = VLAN_Intranet, VLAN ID = 20

12. Sketch Out Your Guest Authorization policy.

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

- a. **Access types:** The provisioner may give the guest the right to connect via web portal authentication ("Web-Authentication") only; to connect by secure 802.1X authentication ("Secure-802.1X- Authentication") only; or to connect via either method.
- b. **Network rights:** The provisioner may give the guest the right to access the Internet only; or the provisioner may give the guest the right to use the campus intranet (which includes the local campus network and the Internet).
- c. **Access zones:** The provisioner may give the guest the right to connect from Building 1's public areas only; to connect from Building 2's public areas only; or to connect from either location.

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

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

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

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

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

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

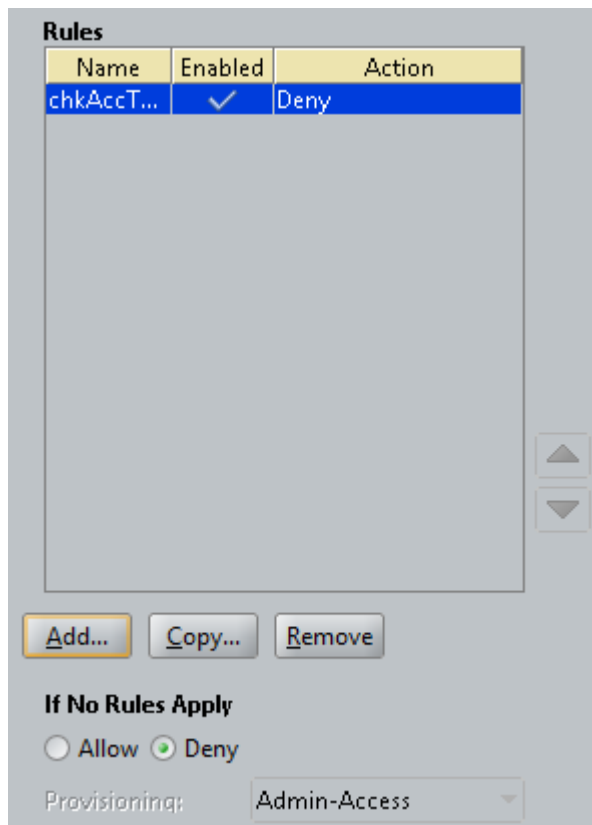
In the Policy Management window, the **chkAccType-Webauth** rule translates as follows: (Note that Ignition Server uses the “!” symbol to mean, “not,” so that in this rule, “!=600S” means “is not 600S”.)

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

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

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

- In Ignition Dashboard main navigation tree, expand Access Policies, expand **RADIUS**, and click the name of the policy your created in [Step-by-step configuration in Ignition Dashboard](#) on page 96.
- In the main part of the window, click the **Authorization Policy** tab.
- 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.
- Begin creating your first rule by clicking the **Add** button under the **Rules** list of the Edit Authorization Policy window.
- In the New Rule window, type a Name for the rule. Call this rule, “chkAccType-Webauth” and click **OK**.



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

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

Your rule consists of *constraints* that can be ANDed and ORed together. It is a good idea to sketch out your desired constraints now. Bearing in mind that the limits applied to a guest user are expressed as “groupmember” attributes, and that the authenticator's model name is expressed as an “Authenticator Device Model” in Ignition, we can express this rule as a phrase of three constraints: “If the User's groupmember is Web-Authentication AND the User's group-member is not Secure-802.1X-Authentication AND the authenticator's Device Model is not 600S, then we should deny his or her access request.”

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

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

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

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

Add the constraint as follows:

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

- In the dropdown list, choose **Secure-802.1X-Authentication**.
 - Click **OK** to close the Add Value window.
 - Click **OK** to close the Constraint Details window.
- j. In the User Authorization Policy window, go to the And/Or column for the just-added constraint and select **AND** from the dropdown list.
- k. Click the **New** button next to the Constraint table to add the last of the three constraints:
- Select an Attribute Category of **Authenticator**.
 - In the list, click **Authenticator Device Template**.
 - In the dropdown list on the right, select **Not Equal To**.
 - Click the **Static Value** radio button.
 - In the dropdown list, choose **600S**.
 - Click **OK** to close the Constraint Details window.
- l. To complete the rule:
- In the Edit Authorization Policy window, click the **Deny** radio button.
 - Click on the first constraint in the table, go to the left parentheses column, and select “(“ from the dropdown list.
 - Click on the last constraint in the table, go to the right parentheses column, and select “)” from the dropdown list.
 - Under the **Action** section, click the **Deny** radio button.
 - Your finished rule will look like the illustration shown below:

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

Selected Rule Details

Rule Name: Rule Enabled

(Constraint)	AND/OR
(User.group-member contains [Web-Authentication])	AND
	User.group-member does not contain [Secure-802.1X-Authentication])	AND
	Authenticator.Authenticator Device Template != 600S)	

Action

Allow
 Deny
 Allow with Actions
 Check Posture
 NAP

Summary

```
IF ( User.group-member contains [Web-Authentication] AND
    User.group-member does not contain [Secure-802.1X-Authentication] AND
    Authenticator.Authenticator Device Template != 600S ) THEN Deny
```

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 *Administering Identity Engines Ignition Server*, NN47280-600.

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

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

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

The is-Empty rule, “chkAccType-isEmpty”: Third, we’ll write a rule that catches and rejects any user who has no access type designation. We can state this rule as follows: If the user bears neither the Secure-802.1XAuthentication flag nor the Web-

Authentication flag, then reject him/her. In the Policy Management window, the `chkAccType-isEmpty` rule translates to:

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

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

To limit the physical locations from which a user can connect, we will write a set of rules that check the authenticator's location in the Ignition Server container hierarchy. Recall that we labelled each switch and access point with a location label, by placing it in the hierarchy when we performed the steps on [Create your authenticators](#) on page 96.

We need three rules for limiting user location:

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

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

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

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

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

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

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

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

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

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

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

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

The final two rules are the *Allow rules*. They assign the user to the appropriate VLAN based on his or her group-member attribute. The attentive reader will notice there is no "AND *User.group-member is not any one of*" phrase as there was in some of the other rules. This

phrase can be left out here because network rights are set via a radio button (as opposed to a series of check boxes which might all be ticked) in the Guest and IoT Manager window, so no user will be a group-member of both groups.

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

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

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

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

16. Sort the rules to create your policy

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

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

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

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

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

Creating a minimal authorization policy

You may elect not to create user groups as explained earlier in this chapter. If you do this, then Guest and IoT Manager 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 *Administering Identity Engines Ignition Server*, NN47280-600.

Chapter 8: Setting Up Self-Provisioning

Identity Engines Guest and IoT 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 and IoT Manager deploys it as an application on the web server where Guest and IoT 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 and IoT 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 196.

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

Creating a Self-Provisioning service

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

Before you begin

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

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

- Set Guest and IoT Manager to send email notifications, as explained in [Setting up Email notification parameters](#) on page 62.
- Set Guest and IoT Manager to send SMS messages, as explained in [Setting up SMS notification parameters](#) on page 65.

Procedure

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

Create Self-Provisioning Service

* **Service Name:**

* **Service Type:**

* **Password:**

* **Confirm Password:**

* **Service Email:**

* **Member of Provisioning Group:**

Terms of use to be displayed on self-provisioning page:

Auto-refresh interval for self-registration page (sec.):

After a self-provisioned guest account was created, perform the following action when auto-refresh interval expired:

Redirect to the self-service registration page

Redirect to this URL:

Don't do anything

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

user name and MAC address as part of the confirmation message. You can add variables to display the start time and end time of the device account in the confirmation message.

Create Self-Provisioning Service

* **Service Name:** Orinthology_Conference

* **Service Type:** Device

* **Password:** [Redacted]

* **Confirm Password:** [Redacted]

* **Service Email:** bbanner@company.com

* **Member of Provisioning Group:** pg2

User acct with provisioning rights must be successfully authenticated to create a device account

Confirmation Template:
 Available variables: \$username, \$macaddress, \$starttime, and \$endtime
 Successfully created a device account:
 \$username
 \$macaddress

Terms of use to be displayed on self-provisioning page:

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

! Important:

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

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

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

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

5. In the **Terms of use to be displayed on self-provisioning page** field, enter the terms to be displayed on the Self Provisioning page.
6. In the **Auto-refresh interval for self-registration page (sec.)** field, enter the value for the refresh interval.

7. In the **After a self-provisioned guest account was created, perform the following action when auto-refresh interval expired** field, select one of the options presented that meet your requirements.
8. Check your entries and click **Submit**. Guest and IoT 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.

Example

The following example displays the successful self-service creation page with service type as Device:

Successful Self-Service Creation

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

Service Name: Orinthology_Conference
Service Type: device
Self-Service URL: https://10.133.140.100/GuestManager/device/Orinthology_Conference/input.jsp
Password: *****
Service Email: bbanner@company.com
Required User: Yes
Authentication:
Confirmation Template: Successfully created a device account:
 \$username
 \$macaddress
Member of Provisioning Group: pg3
Terms of Use:
Auto-refresh Interval (sec.): 10
After a self-provisioned guest account was created, perform the following action when auto-refresh interval expired:
 Redirect to the self-service registration page

Deploying Self Provisioning Service

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

Procedure

1. Find the URL of the self-provisioning service:
 - Log in to the Administrator Application.

- Click **Self-Service** from the main toolbar.
 - Find your portal in the **Self-Provisioning Service** list. The **URL** column shows the URL for the service.
2. In the supported browser, copy and paste the **Self-Provisioning Services** Guest User URL. For example, the Guest User example in the previous section uses the following URL:
`https://<server_name>/Guest&IoTManager/portal/Orinthology_Conference/input.jsp`
- Note that the URLs for Device portals are different from the URLs for Guest User portals. For example, the Device portal example in the previous section uses the following URL:
`https://<server_name>/Guest&IoTManager/device/Orinthology_Conference/input.jsp`
3. Test the page. The Register New Guest User page should appear as follows.

Register New Guest User

* First Name:

* Last Name:

* User Name:

* Email:

* Cell Phone:

Carrier:

Your guest account access details will be provided to you via Email/SMS.
** Required*

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 number. Click **Done** or the page refreshes after few seconds and displays the Register New Guest User page.

The Register New Device page should appear as follows:

Register New Device

* User Name:

* Password:

* MAC Address:

Type:

Sub Type:

4. Guest user can enter his or her username and click on the **resend password** button to receive his or her password via Email / SMS or both depending on the notification options of the Provisioning Group to which the Self Service Portal belongs to.

The following checks are performed depending on which the password is sent:

- a. Notification options has either SMS / Email or both enabled
 - b. The account is not locked/expired
 - c. The Email / SMS Template contains \$password
5. For security, Extreme 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.
 6. Guest and IoT Manager must be connected to the Identity Engines Ignition Server appliance at all times for the self-provisioning portal to operate. To connect, see [Connecting Guest and IoT Manager to the Ignition Server Appliance](#) on page 78.

Guest User Self-Provisioning Portal with Sponsor Approval

When Guest Self-User Provisioning Portal is configured with Sponsor Approval required, Guest User has to enter Sponsor Details along with his details in the Registration page.

The sponsor gets a mail with Guest User's details and option to Approve or Deny Guest User's access request.

Guest User is granted access only after the Sponsor has Approved his access request.

To add sponsor details to the New Self-Provisioning Guest User, do one of the following:

- Entering Sponsor Details Manually. For more information, see [Entering Sponsor details manually](#) on page 123.
- Configuring Sponsor AD Group. For more information, see [Selecting Sponsor details from AD Group](#) on page 125.
- Fixed Sponsor. For more information, see [Fixed Sponsor](#) on page 128

Entering Sponsor details manually

Use the following procedure to add the sponsor details manually in Self-Provisioning Portal.

Before you begin

- Login to the Administrator Application.

- Create a **Guest Self Service with Sponsor Approval** provisioning group and select the **Manually Enter Sponsor Details** to add sponsor details. For more information about configuring sponsor approval, see [Configuring sponsor approval](#) on page 144.
- Create a **New Self-Provisioner** and select the Provisioning Group from **Member of Provisioning Group** drop-down. For more information on creating New Self-Provisioner, see [Creating a Self-Provisioning service](#) on page 118.
- Click **Self Service**, copy and paste the URL of the newly created Self-Provisioner in a supported web browser.

Procedure

1. In the **Register New Guest User** page, enter the Guest User details.
2. Enter the following contact details of your Sponsor:
 - a. **First Name** of the sponsor.
 - b. **Last name** of the sponsor.
 - c. **Email ID** and select the domain from the drop-down beside **Email**.

Only the domains that are added in the **Sponsor > Sponsor Email Domains** are listed in the drop-down.

- d. Enter **Cell Phone** number to send the SMS notification to the sponsor.

Register New Guest User

* **First Name:** Karthik

* **Last Name:** Anand

* **User Name:** 63x336Z2

* **Email:** anand17@extremenetworks.com

* **Cell Phone:** 7788654323

Carrier: AT&T Wireless ▼

Sponsor

Your access request requires Sponsor approval:

* **First Name:** Nehama

Last Name: Shmulik

* **Email:** snehama @extremenetworks.com ▼

Cell Phone: 7766543456

Request Approval Reset Resend Password

* Required

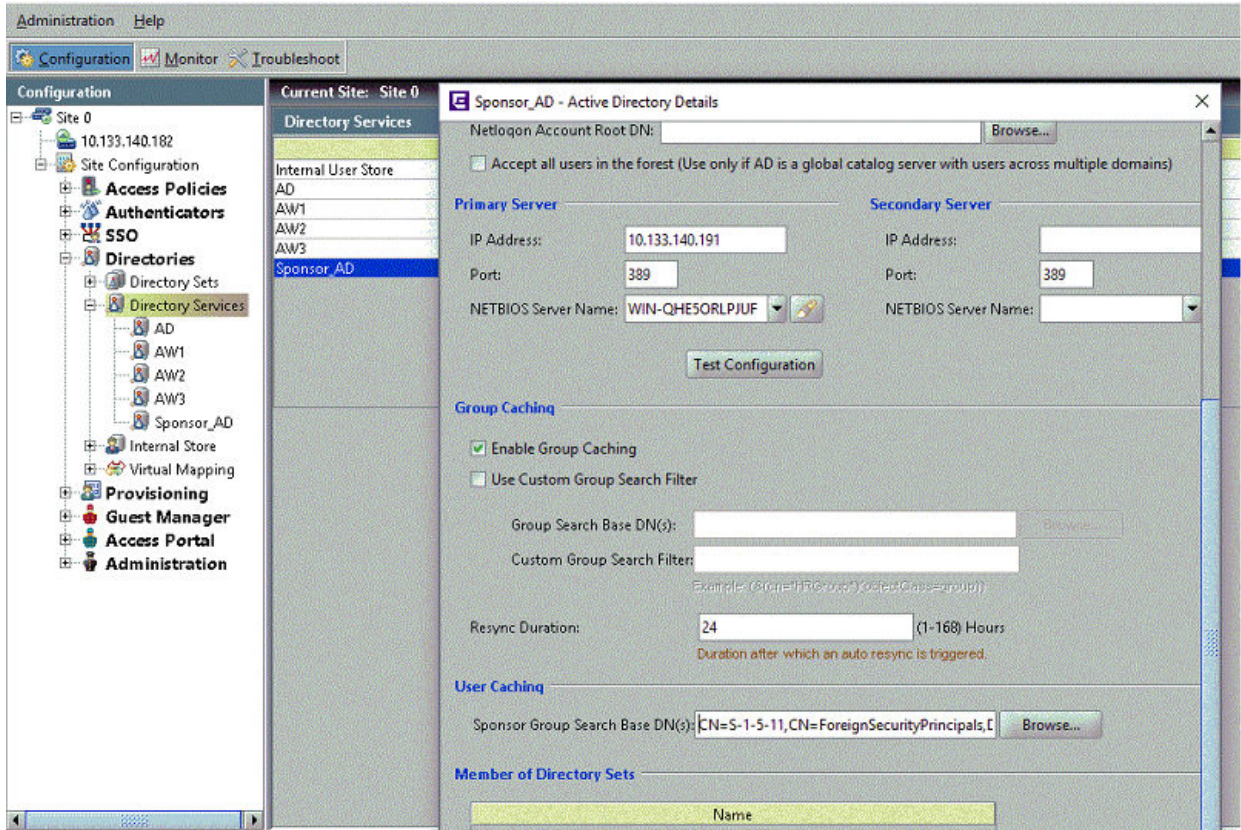
3. Click **Request Approval** to create a Guest User.

Selecting Sponsor details from AD Group

Use the following procedure to configure the sponsor Active Directory group to select the sponsors from pre-populated list in Self-Provisioning Portal.

Before you begin

- In windows Active Directory, create the sponsor groups and assign sponsor users to the groups.
- In Ignition Dashboard, create a **Directory Services** and select the Sponsor Groups under **User Caching**.



The Sponsor Group added under **User Caching** are listed in Guest and IoT Manager Sponsor AD Group drop-down.

- Login to the Administrator Application.
- Create a **Guest Self Service with Sponsor Approval** provisioning group and click the **Configure Sponsor AD Group** to select the sponsor group. For more information about configuring sponsor approval, see [Configuring sponsor approval](#) on page 144.
- Create a **New Self-Provisioner** and select the Provisioning Group from **Member of Provisioning Group** drop-down. For more information on creating New Self-Provisioner, see [Creating a Self-Provisioning service](#) on page 118.
- Click **Self Service**, copy and paste the URL of the newly created Self-Provisioner in a supported web browser.

Procedure

1. In the **Register New Guest User** page, enter the Guest User details.
2. Select your sponsor contact details by clicking the **Select Sponsor**.
Select Sponsor screen appears with list of sponsors for the group.
 You can filter the Sponsor list by selecting **Specify Filter**.

Register New Guest User

First Name:

Last Name:

*** Email:** (Used As User Name)

Cell Phone:

Carrier:

Sponsor
Your access request requires Sponsor approval:

First Name: Samuel

Last Name: Nehama

Email: snehama@extreme.com

** Required*

3. Select the Sponsor from the list and click **Submit**.

Select Sponsor ✕

Sponsor Search Filters

All Sponsors

Specify Filter:

Page size: 1 to 6 of 6 << < > >>

	First Name	Last Name	Email
<input type="radio"/>	C	Sasikanth	sc@extremenetworks.com
<input type="radio"/>	spons		spon@extreme.com
<input type="radio"/>	chinna	tellapati	ctellapati@extremenetworks.com
<input type="radio"/>	Gurudev Singh	Sajwan	gsajwan@extremenetworks.com
<input type="radio"/>	Kamlendra	Singh Shekhawat	ksinghshekhawat@extremenetworks.com
<input type="radio"/>	Shmulik	Nehama	snehama@extremenetworks.com

4. Click **Request Approval** in Register New Guest User screen.
Email notification is sent to the sponsor to approve or reject the user account.

Fixed Sponsor

About this task

Use the following procedure to configure a single sponsor.

Before you begin

- Login to the Administrator Application.
- Create a **Guest Self Service with Sponsor Approval** provisioning group and select the Fixed Sponsor to add sponsor details. For more information, see [Configuring sponsor approval](#) on page 144.
- Create a New Self-Provisioner and select the Provisioning Group from Member of Provisioning Group drop-down. For more information on creating New Self-Provisioner, see [Creating a Self-Provisioning service](#) on page 118.
- Click **Self Service**, copy and paste the URL of the newly created Self-Provisioner in a supported web browser.

Procedure

1. In the Register New Guest User page, enter the Guest User details.
2. Click **Request Approval** to create a Guest User Account.

* Note:

The Sponsor Details are not visible in the Self Service Provisioning Portal. Email notification is sent to the Fixed Sponsor to approve or deny the user account approval request.

Register New Guest User

First Name:

Last Name:

* Email: (Used As User Name)

Cell Phone:

Carrier: AT&T Wireless ▾

Sponsor
Your access request requires Sponsor approval.

* Required

Managing self-provisioned users

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

Procedure

1. Run the Provisioner Application. For instructions, see [Launching the provisioner application](#) on page 200.

2. Log in using the portal provisioner user name and password you received from your Guest and IoT 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 and IoT 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 205 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 and IoT Manager deletes the portal application and its portal provisioner account.

Procedure

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

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

Guest user accounts and device accounts that were created by the deleted provisioning portal remain in the provisioning group of the provisioning portal. For information on retrieving these user accounts, see [Retrieving the guest users owned by a provisioner](#) on page 179.

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

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

Guest and IoT Manager *provisioners*, in contrast to the Guest and IoT Manager *administrator*, exist only to create and manage guest user accounts. Provisioners do not manage other provisioners, nor do they change Guest and IoT Manager settings or policies. For a comparison of user types, see [Types of accounts in your Ignition Server installation](#) on page 16.

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

If you are a provisioner, you may skip this chapter and proceed to [Provisioner application: Managing guests and devices](#) on page 196.

Important:

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

Setting up provisioners

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

As the Guest and IoT Manager administrator, you use the application to create or map provisioner accounts. Each provisioner account is stored either in the 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 and IoT Manager application to Create, Modify, and Delete guest users. The provisioner owns the guest user accounts that he or she creates. If the provisioner's account is deleted, then the guest user accounts it owns are either transferred to other provisioners or deleted.

Creating a provisioning group

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

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

Procedure

1. Run the Administrator Application:
 - Open a browser and navigate to the Administrator Application URL.
 - Type your Guest and IoT Manager administrator `username` and `password`.
 - Guest and IoT Manager must be connected with the Ignition Server appliance. If it is not connected now, see [Connecting Guest and IoT Manager to the Ignition Server Appliance](#) on page 78.
2. Click the **Provisioning Groups** section in the main toolbar. The Provisioning Groups screen appears.
3. Click **Actions > New Provisioning Group**.
4. Configure the provisioning group name and common details for this provisioning group. See [Configuring the common details](#) on page 133.
5. Configure the guest user account details. See [Configuring the Guest User account details](#) on page 135.
6. If self-service guest users must be approved by a sponsor before they are granted access, configure sponsor approval. See [Configuring sponsor approval](#) on page 144.
7. Configure the device records for this provisioning group. See [Configuring the device record details](#) on page 150.

 **Important:**

If you configured sponsor approval, you cannot allow provisioners in this provisioning group to manage devices.

8. Configure the non Guest and IoT Manager devices for the provisioning group. See [Configuring Non Guest and IoT Manager devices](#) on page 152.
9. Configure the contents of the account notification messages sent to guest users. See [Configuring the account notification templates](#) on page 157.

10. If required, configure the advanced details for this provisioning group. See [Configuring advanced details](#) on page 161.
11. Check your entries and click **Submit**. Guest and IoT Manager creates the provisioning group.

Configuring the common details

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

Procedure

1. Enter a **Group Name** for the group.

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

2. Select one of the Provisioning Group type from the **This Provisioning Group will be used for:** section.

Following are the Provisioning Group types.

- **Guest User and Device Provisioning** - This type is used to create a Guest User and Device provisioning. This type is selected by default when you create a Provisioning Group.
- **Guest Self Service with Sponsor Approval** - This type is used to create a Guest User Self Service Provisioning Service with Sponsor Approval.
- **Device Provisioning using Mobile App** - This type is used to create Device provisioning using Mobile Application.
- **Guest User and Device Provisioning using API** - This type is used to create Guest User and Device provisioning using API.

*** Note:**

A new check box option **Provisioners in this group can view all records** is added which makes the Provisioners in the group to view all guest user / device data irrespective of the group they belong to through REST API.

- **Guest User Provisioning using Social Media login** - This type is used to create a Guest User using the social media credentials.

*** Note:**

Provisioner login with Mobile App or REST API provisioning group access cannot create or load new Devices and Guest Users. Only view option will be visible.

3. If the provisioners in this group will collaborate to manage guest users, check the **Provisioners in this group can view and edit each other's records** check box. The **Temporary accounts may be valid for up to filed** is enabled. If you wish to limit each provisioner to view only the guest accounts that they have created, do not check this check box.

4. Set the maximum account life span the group's provisioners can grant to a guest. In the **Temporary accounts may be valid for up to** section, set the maximum life span by selecting the radio button to specify the units (minutes, hours or days) and then entering the number of minutes, hours or days in the preceding field.
5. Set the provisioners' scope of authority. For this, use the check boxes in the lower part of the Create Provisioning Group screen labelled, **Areas to which guest users / devices can be granted access**.

Check the check box for each **Access Types**, **Network Rights**, and **Access Zones** that this group's provisioners may grant to guests. By default, Network Rights check box is selected. For information on these check boxes, see [Access constraint check boxes on the Create Guest User page](#) on page 92.

For example, if you wish to create a Provisioning Group with the **Guest User and Device Provisioning Using API** type, check the check boxes as follows:

Create Provisioning Group

Common | Guest User | Device | Types & Sub Types | Notification | Advanced

Group Name:

This Provisioning Group will be used for:

- Guest User and Device Provisioning
- Guest Self Service with Sponsor Approval
- Device Provisioning using Mobile App
- Guest User and Device Provisioning using API
 - Provisioners in this group can view all records
- Guest User Provisioning using Social Media login

Provisioners in this group can view and edit each other's records

Temporary accounts may be valid for up to:

(1-9999) minutes hours days

Areas to which guest users/devices can be granted access:

Access Types: Network_Access_1

Network Rights: Network_Access_3 network_Access_4

Access Zones: Network_Access_2

Next steps

Go to [Configuring the Guest User account details](#) on page 135.

Configuring the Guest User account details

Use the following procedure to configure the guest user account details for this provisioning group.

Before you begin

To configure the Guest User account details you should select the **Guest User and Device Provisioning** type in **Common** tab.

Create Provisioning Group

Common
Guest User
Device
Types & Sub Types
Notification
Advanced

Group Name:

This Provisioning Group will be used for:

- Guest User and Device Provisioning
- Guest Self Service with Sponsor Approval
- Device Provisioning using Mobile App
- Guest User and Device Provisioning using API
- Guest User Provisioning using Social Media login

Provisioners in this group can view and edit each other's records

Temporary accounts may be valid for up to:

(1-9999)
 minutes
 hours
 days

Areas to which guest users/devices can be granted access:

Access Types: Network_Access_1

Network Rights: Network_Access_3 network_Access_4

Access Zones: Network_Access_2

Procedure

1. Click the **Guest User** tab to configure the guest user account details for this Provisioning Group.

The system displays the Guest User pane.

The screenshot shows the 'Create Provisioning Group' configuration window with the 'Guest User' tab selected. The window has a title bar and several tabs: 'Common', 'Guest User', 'Device', 'Types & Sub Types', 'Notification', and 'Advanced'. The 'Guest User' tab is active, showing the following configuration options:

- Allow or deny provisioners in this provisioning group the right to manage (create, edit, associate) USERS:**
 - Allow Deny
- Guest Notification:** Email SMS Display Password Display User Name
- Auto-generated User Name for Guest Users**
 - Generate User Name with:**
 - Random Generated Username
 - characters (min 1, max 40, single number or range. For example, 6-10) including
 - lower case upper case number
 - FirstnameLastname (e.g., John Smith -> JohnSmith)
 - firstinitiallastname (e.g., John Smith -> jsmith)
 - User Name field editable**
 - Use Email as User Name
 - Use Cell Phone Number as User Name


- Password Complexity Check:**
- characters (min 4, max 30, single number or range. For example, 6-10) including
 - lower case upper case number special characters
- Auto-generated Password for Guest Users**
- Random Generated Password
- Use User Name as Password

At the bottom of the window, there are 'Submit' and 'Cancel' buttons.

*** Note:**

The **Allow or deny provisioners in this provisioning group the right to manage (create, edit, associate) USERS:** will be set to **Allow** by default.

2. In the **Guest Notification** section, select the ways that this group's provisioners will notify guests of their new guest accounts. Select all that apply.
 - **Email** Check this box to notify guest users of their new guest user accounts by way of Email.
 - **SMS** Check this box to notify guest users of their new guest user accounts by way of SMS.
 - **Display Password** Check this box to include the password in the message that is displayed when a guest user account is successfully created (self-service or by provisioner).
 - **Display User Name** Check this box to include the username in the message that is displayed when a guest user account is successfully created (self-service or by provisioner).
3. Check the **Auto-generated User Name for Guest Users** check box to pre-populate a guest username and increase the likelihood that it will be unique. Select any one of the following option:

Choice Option	Choice Description
Generate User Name with	<p>Use the radio buttons below the check box to define the format of the guest user name:</p> <ul style="list-style-type: none"> • Random Generated User name <p>Random generated username consists of a combination of Uppercase letters, Lowercase letters and Numbers. Text box allows the administrator to enter the range or a single value between 1-40 (inclusive) characters in the auto generated username. Depending on the check boxes selected (Lower Case, Upper Case and Number), a random username whose length is within the range specified is generated.</p> <p> Note:</p> <p>Provisioner's create user page and self service portal page will display the randomly generated user name in the username text box.</p> • FirstnameLastname <p>Combination of Firstname and Lastname of the Guest User with an optional suffix/prefix. By default, a suffix of three random numbers is selected.</p> <p>For example, if a provisioner creates a user with first name as "Tom" and last name as "Jones," Guest and IoT Manager will default his username to "TomJonesXYZ" where "XYZ" is a three digit random number.</p> • firstinitiallastname <p>Combination of the initial of the Firstname and Lastname of the Guest User with an optional suffix/prefix. By default, a suffix of three random numbers is selected.</p> <p>For example, if a provisioner creates a user with firstname as "John" and last name "Smith", Guest and IoT Manager will default his username to "jsmithXYZ" where "XYZ" is a three digit random number.</p>

Choice Option	Choice Description
	<p>* Note:</p> <p>User can restrict the Guest User and Provisioner from editing the auto-generated username. Clear the User Name field editable check box to disable editing. By default, this field is selected (enabled).</p>
Use Email as User Name	Select to use the email address as User Name.
Use Cell Phone Number as User Name	Select to use cell phone number as User Name.

- In the **Password Complexity Check** section, select the requirements for passwords.

You can set the password complexity, providing the required number of characters in the text box, and selecting the alphanumeric check boxes : lower case, upper case, number, special character. Allowed special characters are: !, @, #, \$, %, ^, &, *, (,), -, +.

- Check the **Auto-generated Password for Guest Users** field, if you want the provisioner to auto-generate password for the guest users. In this case, Provisioner need not provide the password while creating or editing the Guest User. Select the following type of auto-generated password.
 - **Random Generated Password**
 - **Use User Name as Password**
 - **Static Password**

If you select Random Generated Password, the system generates a random password and send an email to the guest user containing special characters similar to an Admin password while the provisioner creates a guest user.

Random Password Sample Email Format:

Password: E^zf!)V6

First Name: John

Last Name: Smith

Email: johnsmith@extremenetworks.com

Comments: Sample Random Password

Start Time: 2017/09/07 09:39:59 AM GMT+00:00

End Time: 2017/09/07 05:39:59 PM GMT+00:00

Access: Terms of Use

If you select to use the username as the password or enter a static password, the guest user can log in with only a user name. The Access Portal login page must be modified to accept a user name without a password. You must be able to set the password as a fixed string so that a single password can be used for multiple accounts.

6. Self Service portal user can recreate a guest account with same **username** and **E-mail** or same **username** and **Cell phone number** within the duration and number of account recreation limit specified in the provisioning group. Select the check box **Limit the number of Guest Accounts that can be created for a given Email/Cell Phone number**. Guest and IoT Manager Administrator can specify the time limit in text. Enter the number of hours (duration within which the user can recreate an account) and the number of guest accounts.

Create Provisioning Group

Common
Guest User
Device
Types & Sub Types
Notification
Advanced

6-8 characters (min 4, max 30, single number or range. For example, 8-10) including

lower case upper case number special characters

Auto-generated Password for Guest Users

- Random Generated Password
- Use User Name as Password
- Static Password:

Limit the number of Guest Accounts that can be created for a given Email/Cell Phone number within (1-999) hours to .

Customize Printer Friendly Page:

	Accessible to Provisioners	Default Value
Bulk Load Guest Users	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Device Association	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Delete on Expire	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Yes <input type="radio"/> No
Cell Phone	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Email	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Account Activation	<input checked="" type="radio"/> Time Based <input type="radio"/> First Login	
Account Validity Duration	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input checked="" type="radio"/> Max validity duration <input type="radio"/> Permanent
Network Access Rights	<input checked="" type="radio"/> Yes <input type="radio"/> No	All network rights
Guest Details	<input checked="" type="radio"/> Yes <input type="radio"/> No	
First Name and Last Name	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Required <input type="radio"/> Optional
SMS Gateway List	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Resend Password	<input checked="" type="radio"/> Yes <input type="radio"/> No	Applicable only to Self Service
Network Usage	N/A	Static Value: <input style="width: 100px;" type="text"/>

7. **(Optional)** Select **Customize Printer Friendly Page** to enable customization of Guest User information page.
 - a. **Select Uploaded HTML file** from the given drop-down list.

- b. For more details on customizing and uploading a file using File Manager, see [Customizing Printer Friendly Page](#) on page 193.
8. Select the options that are accessible to provisioners and the default value, if appropriate.
 - Bulk Load Guest Users
 - Device Association
 - Delete on Expire
 - Cell Phone
 - Email
 - Account Activation.
 - If you select **Time Based Login**, the account activation will be available to the maximum set time limit. For example, No of minutes, hours or days.
 - If you select **First Login**, the account activation set duration is considered from the time the user logs in for the first instance.
 - Account Validity Duration
 - If you select **Yes**, the account validity duration is set to the value provided by the Provisioner during Guest User account creation.
 - If you select **No**, **Permanent** option is enabled. You can set the account validity duration either to default Provisioning group value (Max Validity Duration) or Permanent. The maximum account life span value the group's provisioners can grant to a guest is specified in units (minutes, hours or days). You can enter the number of minutes, hours or days in the **Provisioners Groups > Common > Temporary accounts may be valid for up to** field.

 **Note:**

If account validity duration is set to Permanent, the **Delete on Expire** and **Account Activation** options will be disabled and the Guest User will gain permanent access.

The Provisioner can view this information during searching Guest User account information. For more information, see [Finding guest user account](#) on page 207.

Create Provisioning Group

Common **Guest User** Device Types & Sub Types Notification Advanced

Customize Printer Friendly Page:

	Accessible to Provisioners	Default Value
Bulk Load Guest Users	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Device Association	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Cell Phone	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Email	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Account Validity Duration	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Max validity duration <input checked="" type="radio"/> Permanent
Network Access Rights	<input checked="" type="radio"/> Yes <input type="radio"/> No	All network rights
Guest Details	<input checked="" type="radio"/> Yes <input type="radio"/> No	
First Name and Last Name	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Required <input type="radio"/> Optional
SMS Gateway List	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Resend Password	<input checked="" type="radio"/> Yes <input type="radio"/> No	Applicable only to Self Service
Network Usage	N/A	Static Value: <input type="text"/>

Submit Cancel

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

! Important:

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

- Resend Password. Depending on the value (Yes / No) of this entity, Resend Password button will be displayed on the Self Service login page.
- Network Usage

Next steps

Do one of the following:

- If sponsor approval is required for the self-service guest users in this provisioning group, go to [Configuring sponsor approval](#) on page 144.
- If this provisioning group manages devices, go to [Configuring the device record details](#) on page 150.

- Otherwise go to [Configuring the account notification templates](#) on page 157.

Creating Guest User Provisioning using Social Media login

About this task

Use this procedure to create a Guest User provisioning using Social Media login. Identity Engines Ignition Access Portal, provides support for Social Media login. Users can now login, using their Google, LinkedIn, or Facebook credentials.

Before you begin

- You should have a complete setup of Identity Engines- Access Portal, Ignition Server and Guest and IoT Manager.
- Configure Social Media Login credentials on third party developer console.
- Configure Social Media Login on Access Portal. For more information on configuring Social Media Login on Access Portal, see *Identity Engines Ignition Server Configuration, NN47280-600*.

Procedure

1. Open a browser and navigate to the Administrator Application URL.
2. Type your Guest and IoT Manager administrator username and password.

 **Note:**

Guest and IoT Manager must be connected with the Ignition Server appliance.

3. On the navigation tree, click **Provisioning Groups**.

The system displays the **Provisioning Groups** window.

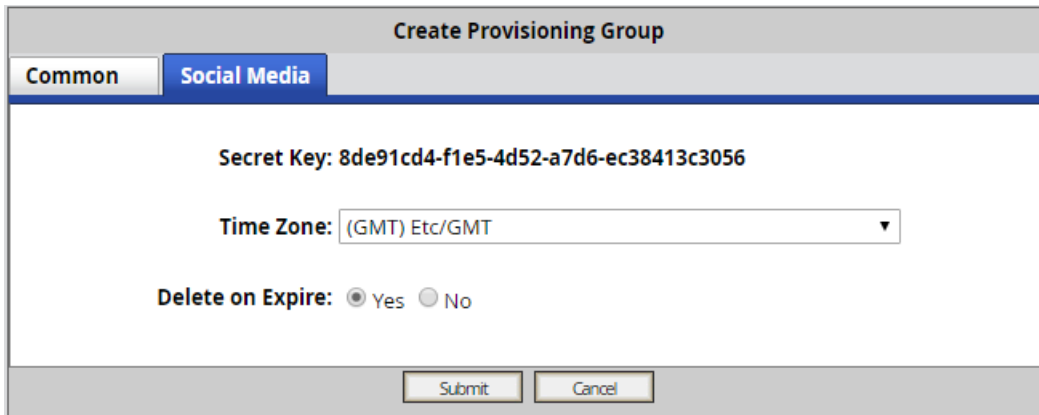
4. On the Provisioning Groups window, click **Actions > New Provisioning Groups**.

The system displays **Create Provisioning Group** page.

5. On the **Common** tab, select **Guest User Provisioning using Social Media login** check box, to create a Guest User in the Ignition Server.

The system enables the **Social Media** tab.

6. On the **Social Media** tab, copy the auto-generated **Secret Key** and click **Submit**.



The screenshot shows a web interface titled "Create Provisioning Group". It has two tabs: "Common" and "Social Media", with "Social Media" selected. The "Secret Key" is displayed as "8de91cd4-f1e5-4d52-a7d6-ec38413c3056". Below it is a "Time Zone" dropdown menu set to "(GMT) Etc/GMT". There are radio buttons for "Delete on Expire": "Yes" (selected) and "No". At the bottom are "Submit" and "Cancel" buttons.

7. Navigate to Identity Engines Ignition Access Portal, and paste the copied **Secret Key** and the **Guest & IoT Manager IP / hostname** in the **Guest & IoT Manager Settings** tab. For more information, see *Administering Identity Engines Ignition Access Portal, NN47280-604*.

Configuring sponsor approval

Use the following procedure to configure sponsor approval if self-service guest users must be approved by a sponsor before they are granted access.

Before you begin

- Open a browser and navigate to the Administrator Application URL.
- Type your Guest and IoT Manager administrator username and password.

*** Note:**

Guest and IoT Manager must be connected with the Ignition Server appliance.

Procedure

1. On the navigation tree, click **Provisioning Groups**.
The system displays the **Provisioning Groups** window.
2. On the **Provisioning Groups** window, click **Actions > New Provisioning Groups**.
The system displays the **Create Provisioning Group** page.
3. To configure Sponsor approval you must select the **Guest Self Service with Sponsor Approval** type in the **Common** tab.
4. Click the **Sponsor** tab to configure sponsor approval for self-service guest users.
5. On the **Sponsor** tab, by default the **Sponsor approval required** check box is selected.
6. To add Sponsor details, do one of the following:
 - a. Select **Manually Enter Sponsor Details** and enter the **Sponsor Email Domains**.

In **Sponsor Email Domains** field, you can add an email domain name up to minimum 2 characters long and maximum 32 characters length. If the entered domain name has the length between 2 and 32 characters, the **Add** button is enabled or be inactive if the length is less than 2 characters or more than 32 characters. For example, the domain name must be : <name>@extremenetworks.travelersinsurance.com

Click **Add** to add the **Sponsor Email Domains** which forces the guest user to have a sponsor in a particular Email domain.

Create Provisioning Group

Common Guest User **Sponsor** Notification Advanced

Sponsor approval workflow cannot be combined with device registration

Sponsor approval required:

Manually Enter Sponsor Details

Sponsor Email Domains @extremenetworks.travelersinsu

Ex. @extremenetworks.com

Repeat to add additional domains as per the specified domain name instructions.

- b. Select **Fixed Sponsor** and enter the **Fixed Sponsor First name, Last Name and the Email ID**. First name and last name of the sponsor are optional fields whereas the email field is mandatory. These details are not visible to the guest.

Create Provisioning Group

Common Guest User **Sponsor** Notification Advanced

Sponsor approval workflow cannot be combined with device registration

Sponsor approval required:

Manually Enter Sponsor Details

Fixed Sponsor

First Name:

Last Name:

*** Email:**

- c. Select **Configure Sponsor AD Group** and select the **AD Group** from the drop-down list.

Edit Provisioning Group: Guest_Access_Bangalore

Common **Guest User** **Sponsor** **Notification** **Advanced**

Sponsor approval workflow cannot be combined with device registration

Sponsor approval required:

Manually Enter Sponsor Details

Fixed Sponsor

Configure Sponsor AD Group

AD Group sponsorAD - Sponsor Approv ▾

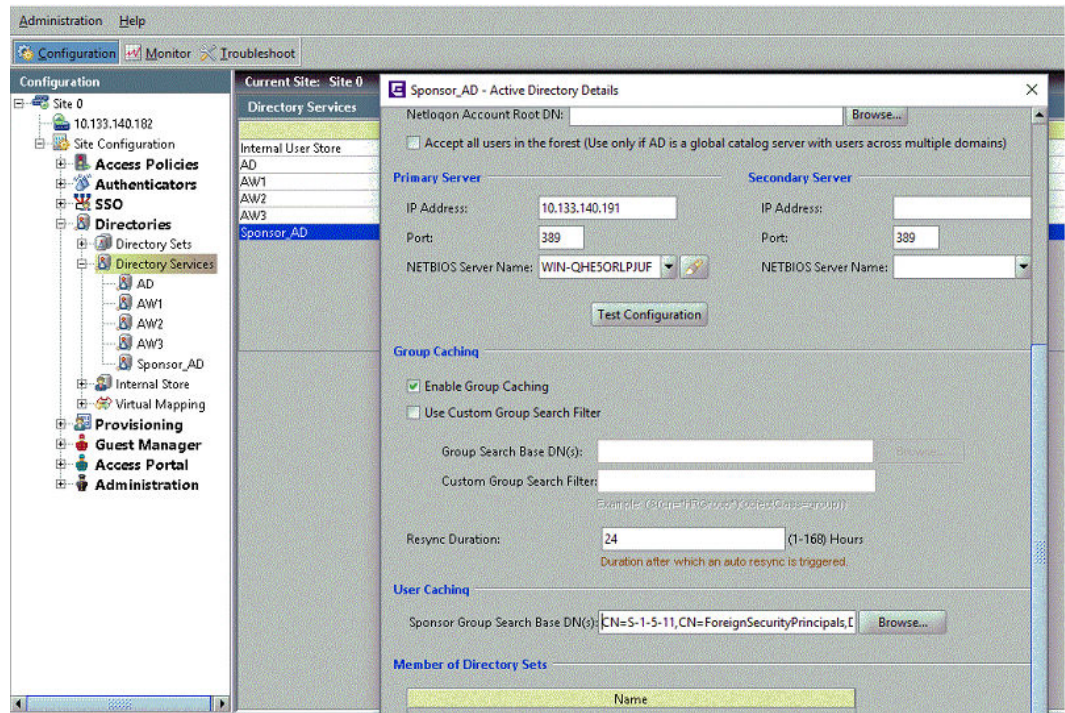
sponsorAD - Sponsor Approvers List

Sponsor response timeout 60 (0-480 min; 0 = Immediate Default Action)

Sponsor Email Notification Template

*** Note:**

- In Ignition Dashboard Directory Services wizard the AD Groups are selected under **User Caching**. Only those AD Groups selected under **User Caching** are reflected in the Guest and IoT Manager Provisioning Group **Configure Sponsor AD Group** drop-down.



- Administrator can configure AD Groups across Multiple Directory Services.
- Each entry in the Drop-down list is formatted as <Directory Service Name> - <AD Group Name>

The Sponsor AD Groups are created in **Active Directory Users and Computer** and associated to Directory Services in Ignition Dashboard. For more information about creating directory services, see *Identity Engines Ignition Server Configuration, NN47280-600*.

- If required, configure a time limit for the sponsor approval and the default action when the time limit passes.
 - Check the **Sponsor response timeout** check box and enter a time in minutes in a range of 0 to 480.

*** Note:**

If the value is 0 it specifies the immediate default approval.

- In the **Default action on timeout** field, select **Approve** or **Deny**.
- In the **Sponsor Email Notification Template** section, enter the contents of the e-mail message to send to the sponsor to approve or deny the request for a guest user account.

! Important:

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

- In the **Select Interface** field, select the required interface to allow a sponsor to have access to a certain network to approve or deny received requests. The options available are: Admin, Service A, Service B. By default, Admin is selected.

For example, If **Service A** interface is selected, the email link that sponsor receives to login will be sent to **Service A** interface IP. This action will affect the *\$sponsoractionlink* variable.

- Choose any one or both the option to send e-mail notification or sponsor response e-mail to a guest:

*** Note:**

These notification options are applicable and available only when self-service requires sponsor action.

Choice Option	Choice Description
Send Initial Notification to Guest	Select the check box if you want guest users to receive an e-mail and SMS notification when they register themselves using self-service.
Send Sponsor Response Notification to Guest	Select the check box if you want guest users to receive an e-mail and SMS notification when sponsor approves or denies guest users access request.

- Click **Submit** to save the configuration.

Example

Common
Guest User
Sponsor
Notification
Advanced

Sponsor approval workflow cannot be combined with device registration

Sponsor approval required:

Manually Enter Sponsor Details

Sponsor Email Domains

Ex. @ extreme.com

Fixed Sponsor

Configure Sponsor AD Group

Sponsor response timeout (0-480 min; 0 = Immediate Default Action)

Sponsor Email Notification Template

Email Template: Subject:

Available variables: \$username, \$password, \$firstname, \$lastname, \$email, \$comment, \$access, \$starttime, \$endtime, \$sponsorname, \$sponsoremail and \$sponsoractionlink

Request for Guest User Account Approval

Message:

Please click [here]($sponsoractionlink) to Approve or Deny the request.

Guest Details:

User Name: \$username
 First Name: \$firstname
 Last Name: \$lastname
 Email: \$email
 Comments: \$comment
 Start Time: \$starttime

Select Interface: Admin

Note: This interface will be used for \$sponsoractionlink

Send Initial Notification to Guest Send Sponsor Response Notification to Guest

Next steps

Go to [Configuring the account notification templates](#) on page 157.

Configuring the device record details

Use the following procedure to configure the device record details for this provisioning group.

Before you begin

To configure the Device record details you must select the **Guest User and Device Provisioning** type in the **Common** tab. Selecting the **Guest User and Device Provisioning** type, disables the **Sponsor** and **Mobile App** tabs.

Procedure

1. Select the **Device** tab to configure the device records details for this Provisioning Group.
2. The **Allow or deny provisioners in this provisioning group the right to manage (create, edit, associate) DEVICES:** must be set to **Allow** to configure the device record details.
3. Select the following device record settings accessible to provisioners in this provisioning group and, if applicable, select a default value.
 - All Non-GM Devices. For more information, see [Configuring Non Guest and IoT Manager devices](#) on page 152.
 - Bulk Load Devices
 - User Association
 - VLAN
 - Custom Attributes
 - Network Access Rights
 - Source
 - Name
 - Type
 - Sub Type
 - Asset Type
 - Delete on Expire
 - Account Activation
 - Account Validity Duration
 - Limit number of enabled devices per provisioner
If **Yes**, enter the maximum number of enabled devices allowed for a provisioner.
 - Display Admin's Comments
If **Yes**, enter the comment to be displayed on the provisioner's Create Device page.
4. Click **Submit** to save the configuration.

Example

Create Provisioning Group

Common
Guest User
Device
Types & Sub Types
Notification
Advanced

Allow or deny provisioners in this provisioning group the right to manage (create, edit, associate) DEVICES:

Allow
 Deny

	Accessible to Provisioners	Default Value
All Non-GM Devices	<input type="radio"/> Yes <input checked="" type="radio"/> No	Static Group(Optional): ----- Select One ----- ▼
Bulk Load Devices	<input checked="" type="radio"/> Yes <input type="radio"/> No	
User Association	<input checked="" type="radio"/> Yes <input type="radio"/> No	
VLAN	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Custom Attributes	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Network Access Rights	<input checked="" type="radio"/> Yes <input type="radio"/> No	All network rights
Source	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Auto populate with GM-[provisioning group] <input type="radio"/> Static: <input style="width: 100px;" type="text"/>
Name	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Required <input checked="" type="radio"/> Optional
Type	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Required <input checked="" type="radio"/> Optional
Sub Type	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Required <input checked="" type="radio"/> Optional
Asset Type	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Permanent <input type="radio"/> Temporary
Delete on Expire	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Yes <input type="radio"/> No
Account Activation	<input checked="" type="radio"/> Time Based <input type="radio"/> First Login	
Account Validity Duration	<input checked="" type="radio"/> Yes <input type="radio"/> No	Max validity duration
Limit number of enabled devices per provisioner	<input checked="" type="radio"/> Yes <input type="radio"/> No	Maximum number of enabled devices: <input style="width: 50px;" type="text"/>
Display Admin's Comments	<input checked="" type="radio"/> Yes <input type="radio"/> No	<div style="border: 1px solid gray; height: 40px; width: 100%;"></div>

Next steps

Go to [Configuring the account notification templates](#) on page 157.

Configuring Non Guest and IoT Manager devices

About this task

Use the following procedure to configure the Non Guest and IoT Manager devices for the provisioning group.

Before you begin

To configure the Non Guest and IoT Manager devices, you must select the **Guest User and Device Provisioning** type in the **Common** tab and select **Provisioners in this group can view and edit each other's records** check box to enable the option to select the Non Guest and IoT Manager devices in the **Device** tab.

To limit the groups that the provisioner can manage, you must select the required groups from **Access Types** and **Access Zones** in the **Areas to which guest users / devices can be granted access** field frame in the **Common** tab.

Procedure

1. Navigate to *Create Provisioning Group* page, click on the **Device** tab and select **Allow to enable provisioner in the specific provision group** to manage devices.
2. Select **Yes in All Non-GIM Devices** to configure the devices. The default value **Static Group (Optional)** field is enabled and lists the Access Types, Network Rights, and Access Zones details to set the provisioners' scope of authority. For more information on setting access rights for each guest user, see [Access constraint check boxes on the Create Guest User page](#) on page 92.

Note:

You need to create Internal Groups on the Dashboard and map them to Access Types, Access Zones, and Network Rights. You also need to assign Internal Groups to the devices created on the Dashboard. For more information, see *Adding a new internal group* section in *Identity Engines Ignition Server Configuration, NN47280-600*.

3. **Optional:** In the **Static Group (Optional)** field, select the required static group to limit the access of a provisioner when managing the Non Guest and IoT Manager devices.

If you select a static group, then the provisioner can view / edit Non Guest and IoT Manager and Guest and IoT Manager devices associated with that particular.

4. Click **Submit** to save the provisioning group configuration and assign this group to provisioners. For more information on assigning groups to provisioner, see [Assigning a provisioner to a provisioning group](#) on page 169.

Example

Edit Provisioning Group: GIM Non GM Devices

Common Guest User **Device** Types & Sub Types Notification Advanced

Allow or deny provisioners in this provisioning group the right to manage (create, edit, associate) DEVICES:

Allow Deny

	Accessible to Provisioners	Default Value
All Non-GIM Devices	<input checked="" type="radio"/> Yes <input type="radio"/> No	Static Group(Optional): ExtremeloTDeviceManage ▾
Bulk Load Devices	<input checked="" type="radio"/> Yes <input type="radio"/> No	----- Select One ----- ExtremeloTDeviceManage
User Association	<input checked="" type="radio"/> Yes <input type="radio"/> No	ExtremeloTDevices
VLAN	<input type="radio"/> Yes <input checked="" type="radio"/> No	ExtremeloTDevices1
Custom Attributes	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Network Access Rights	<input checked="" type="radio"/> Yes <input type="radio"/> No	All network rights
Source	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Auto populate with GIM-[provisioning group] <input type="radio"/> Static: <input type="text"/>
Name	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Required <input checked="" type="radio"/> Optional
Type	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Required <input checked="" type="radio"/> Optional
Sub Type	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Required <input checked="" type="radio"/> Optional
Asset Type	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Permanent <input checked="" type="radio"/> Temporary
Delete on Expire	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Yes <input type="radio"/> No
Account Activation	<input checked="" type="radio"/> Time Based <input type="radio"/> First Login	
Account Validity Duration	<input checked="" type="radio"/> Yes <input type="radio"/> No	Max validity duration
Limit number of enabled devices per provisioner	<input type="radio"/> Yes <input checked="" type="radio"/> No	Maximum number of enabled devices: <input type="text"/>

Submit Cancel

Custom Device Types and Sub Types

About this task

This feature allows an administrator to select a certain set of Device Types and Sub Types created on Ignition server using dashboard, to make available for the Provisioner to select from.

Procedure

1. Navigate to Create Provisioning Group Page, Click on the **Device** tab and select **Allow**

Create Provisioning Group

Common
Guest User
Device
Types & Sub Types
Notification
Advanced

Allow or deny provisioners in this provisioning group the right to manage (create, edit, associate) DEVICES:

Allow **Deny**

	Accessible to Provisioners	Default Value
All Non-GM Devices	<input checked="" type="radio"/> Yes <input type="radio"/> No	Static Group(Optional): ----- Select One ----- ▼
Bulk Load Devices	<input checked="" type="radio"/> Yes <input type="radio"/> No	
User Association	<input checked="" type="radio"/> Yes <input type="radio"/> No	
VLAN	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Custom Attributes	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Network Access Rights	<input checked="" type="radio"/> Yes <input type="radio"/> No	All network rights
Source	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Auto populate with GM-[provisioning group] <input type="radio"/> Static: <input style="width: 100%;" type="text"/>
Name	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Required <input checked="" type="radio"/> Optional
Type	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Required <input checked="" type="radio"/> Optional
Sub Type	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Required <input checked="" type="radio"/> Optional
Asset Type	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Permanent <input type="radio"/> Temporary
Delete on Expire	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Yes <input type="radio"/> No
Account Activation	<input checked="" type="radio"/> Time Based <input type="radio"/> First Login	
Account Validity Duration	<input checked="" type="radio"/> Yes <input type="radio"/> No	Max validity duration
Account Activation	<input checked="" type="radio"/> Time Based <input type="radio"/> First Login	
Account Validity Duration	<input checked="" type="radio"/> Yes <input type="radio"/> No	Max validity duration
Limit number of enabled devices per provisioner	<input type="radio"/> Yes <input checked="" type="radio"/> No	Maximum number of enabled devices: <input style="width: 50px;" type="text"/>
Display Admin's Comments	<input type="radio"/> Yes <input checked="" type="radio"/> No	<div style="border: 1px solid gray; height: 40px; width: 100%;"></div>

By Default, the **Types and Sub Types** tab is disabled since Device Provisioning is disabled by default. Once you Allow Device Provisioning and make **Type** accessible, the **Types and**

Sub Types tab will get enabled. Also, there is an option to make Sub-Type **Required** or **Optional** .

2. Click **Types and Sub Types** tab which will display all the Device Types and Sub Types. By default, all are selected. Deselect the ones that need to be hidden. Click **Submit** button and you can see the list of accessible Types and Sub Types in the confirmation page.

Create Provisioning Group

Common | Guest User | Device | **Types & Sub Types** | Notification | Advanced

Please select the Device Types and Sub Types accessible

Select All Clear All	Types	Sub Types
<input checked="" type="checkbox"/>	FA client	Select All Clear All <input checked="" type="checkbox"/> ONA-SDN <input checked="" type="checkbox"/> ONA-SPBoIP <input type="checkbox"/> ip-camera <input type="checkbox"/> ip-phone <input type="checkbox"/> ip-video <input type="checkbox"/> wlan-9100 <input type="checkbox"/> n/a
<input checked="" type="checkbox"/>	fax machine	<input checked="" type="checkbox"/> n/a
<input checked="" type="checkbox"/>	handheld	<input checked="" type="checkbox"/> n/a
<input checked="" type="checkbox"/>	mobile	Select All Clear All <input type="checkbox"/> android-phone <input checked="" type="checkbox"/> android-tablet <input type="checkbox"/> blackberry <input type="checkbox"/> blackberry-playbook <input checked="" type="checkbox"/> flare <input checked="" type="checkbox"/> generic-android <input type="checkbox"/> generic-ios <input type="checkbox"/> ipad <input type="checkbox"/> iphone <input type="checkbox"/> kindle-fire <input checked="" type="checkbox"/> windows-phone <input checked="" type="checkbox"/> windows-surface-pro <input checked="" type="checkbox"/> windows-surface-rt <input checked="" type="checkbox"/> n/a
<input checked="" type="checkbox"/>	pc	<input checked="" type="checkbox"/> n/a
<input checked="" type="checkbox"/>	printer	<input checked="" type="checkbox"/> n/a
<input checked="" type="checkbox"/>	scanner	<input checked="" type="checkbox"/> n/a

Submit | Cancel

This will limit the device Types and Sub Types accessible to provisioners during device registration.

Create Device

Common

Associated Provisioning Group:

* **Group Membership:** Guest_Access_LosAngeles ▼

Device Info:

* **MAC Address:** 12:32:10:11:56:76

Name: ONA

Type: FA client ▼

Sub Type: ----- Select One ----- ▼

Source: ----- Select One -----

Comments: ONA-SDN
ONA-SPBoIP

Record Enabled: Yes No

*** Note:**

Customizing Device Types and Sub Types applies to self service device registration, provisioner device registration, REST API device registration, and provisioner device bulk load.

Configuring the account notification templates

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

Procedure

1. On the **General** tab, use the **SMS Template** to enter the text message to be sent to the guest user's cell phone when a provisioner saves the guest user's account. For instructions on writing the SMS template, see [Writing SMS and Email templates for account notifications](#) on page 165.

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

2. On the **General** tab, use the **Email Charset** to select HTML or Plain characters for the contents of the guest user email template. For instructions on selecting standard email characters, see [Writing SMS and Email templates for account notifications](#) on page 165.

3. On the **General** tab, use the **Email Template** to enter the contents of the confirmation email to be sent to the guest user when a provisioner saves the guest user's account. For instructions on writing the email template, see [Writing SMS and Email templates for account notifications](#) on page 165.

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

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

The text entered in the **Terms of Use and /or Additional information to be included as part of guest account confirmation page** field is by default appended as part of email confirmation sent to the user. In addition to this, to include a message in the confirmation email to the guest, add the *\$comment* variable to the **Email Template** (see [Creating a provisioning group](#) on page 132) and have your provisioners type the message in the **Comment** field when creating the Guest User.

Create Provisioning Group

Common Guest User Sponsor **Notification** Advanced

General Sponsor Action

This Email/SMS template will be used for provisioner Guest user and Self-Service Guest user registration
Note: Message needs to be update if sponsor approval required.

SMS Template: Message:
Available variables: \$username, \$password, \$sponsorname and \$sponsoremail

New guest user was successfully created.
User Name: \$username
Password: \$password

81 SMS characters

Email Charset: HTML Character set
 Plain Character set

Font: sans-serif
Color: Blue
Font Size: 12

Email Template: Subject:
Available variables: \$username, \$password, \$firstname, \$lastname, \$email, \$comment, \$access, \$starttime, \$endtime, \$sponsorname, \$sponsoremail and \$terms

Guest user account

Message:
User Name: \$username
Password: \$password
First Name: \$firstname
Last Name: \$lastname
Email: \$email
Comments: \$comment
Start Time: \$starttime
End Time: \$endtime
Access: \$access
Terms of Use
\$terms

Terms of Use and/or Additional information to be included as part of guest account confirmation page:

Submit Cancel

5. On the **Sponsor Action** tab, use the **SMS Template** to enter the text message to be sent to the guest user's cell phone when a sponsor approves or denies the guest user's account. For instructions on writing the SMS template, see [Writing SMS and Email templates for account notifications](#) on page 165.
6. On the **Sponsor Action** tab, use the **Email Template** to enter the email message to be sent to the guest user when a sponsor approves or denies the guest user's account. For instructions on writing the email template, see [Writing SMS and Email templates for account notifications](#) on page 165.

Create Provisioning Group

Common Guest User Sponsor **Notification** Advanced

General **Sponsor Action**

This Email/SMS template will be used for sponsor response
\$sponsoraction value will be either Approved or denied based on sponsor response

SMS Template: Message:
Available variables: \$username, \$password, \$sponsorname, \$sponsoremail and \$sponsoraction
Your guest user account request has been \$sponsoraction.
User Name: \$username
Password: \$password

97 SMS characters

Email Template: Subject:
Available variables: \$username, \$password, \$firstname, \$lastname, \$email, \$comment, \$access, \$starttime, \$endtime, \$sponsorname, \$sponsoremail, \$sponsoraction and \$sponsortext
Guest user account

Message:
Your guest user account request has been \$sponsoraction.
User Name: \$username
Password: \$password
First Name: \$firstname
Last Name: \$lastname
Email: \$email
Comments: \$comment
Start Time: \$starttime
End Time: \$endtime
Access: \$access
\$sponsortext

Submit Cancel

Next steps

If advanced details are required for this provisioning group, go to [Configuring advanced details](#) on page 161. Otherwise, go to [Creating a provisioning group](#) on page 132.

Configuring advanced details

Use the **Advanced** tab to

- Limit the locations from which provisioners can log into the Provisioner Application and manage users.
- Select a time zone.
- Configure the period of inactivity after which a provisioner's session in the Provisioner Application automatically disconnects. After the session disconnects, the provisioner must log in again.

Procedure

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

Format: `<Host>.<Domain>.<suffix>`

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

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

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

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

Next steps

Go to [Creating a provisioning group](#) on page 132.

Creating a provisioner in the internal store

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

To authenticate provisioners against LDAP or AD, see [Creating a provisioner from an account in an LDAP or AD store](#) on page 163. To bulk-import provisioners, see [Bulk importing provisioner accounts from a file](#) on page 163.

Before you begin

Before you create a provisioner account, make sure you have created the provisioning group to which the new provisioner will belong. If you do not have an appropriate provisioning group, see [Creating a provisioning group](#) on page 132.

Procedure

1. Run the Administrator Application (note that you cannot use Ignition Dashboard for this):
 - Open a browser and navigate to the Administrator Application URL.
 - Type your Guest and IoT Manager administrator `username` and `password`.
 - Guest and IoT Manager must be connected with the Ignition Server appliance. If it is not connected now, see [Connecting Guest and IoT Manager to the Ignition Server Appliance](#) on page 78.
2. Select **Provisioner** in the main toolbar. The Internal Provisioners screen appears.
3. Select **Actions > New Internal Provisioner**. The Create Provisioner screen appears.

The screenshot shows the 'Create Provisioner' form with the following fields and options:

- * User Name:** lblack
- * First Name:** Lewis
- * Last Name:** Black
- * Password:** [masked]
- * Confirm Password:** [masked]
- * Email:** lblack@idengines.com
- Comments:** [empty text area]
- * Member of Provisioning Group(s):**
 - default
 - pg_device
 - sponsor_group
 - test10
 - test1_gudgud
 - test2_gugd
 - test3_gu
 - test4_gu
 - test5_gd
 - test6_gd
 - test8_gd
 - test_gugd

Buttons: Submit, Cancel

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

! Important:

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

 - **Email:** Enter the email address of the provisioner.
 - In **Comments**, enter any notes you wish to make. These comments are not sent to the provisioner.
5. In the **Member of Provisioning Group** check boxes, check the provisioning group(s) that this user belongs to.
6. Check your entries and click **Submit**. Guest and IoT Manager creates the provisioner.
7. **(Optional)** Click **Cancel** to cancel the changes.
8. Notify the provisioner of his or her new provisioner username and password, and provide the URL of the provisioner application, which is


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

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

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

You have the option of allowing existing users in your LDAP or Active Directory store to act as provisioners. See [Creating a Provisioner access policy](#) on page 48 or [Creating an Advanced Provisioner access policy](#) on page 52 for instructions.

Bulk importing provisioner accounts from a file

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

If your provisioners exist in an LDAP or AD store, then you might not have to import them at all. Instead, you can set Guest and IoT 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 163.

Use these steps to bulk-import provisioner accounts:

Procedure

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

The format consists of one user per line:

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

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

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

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

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

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

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

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

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

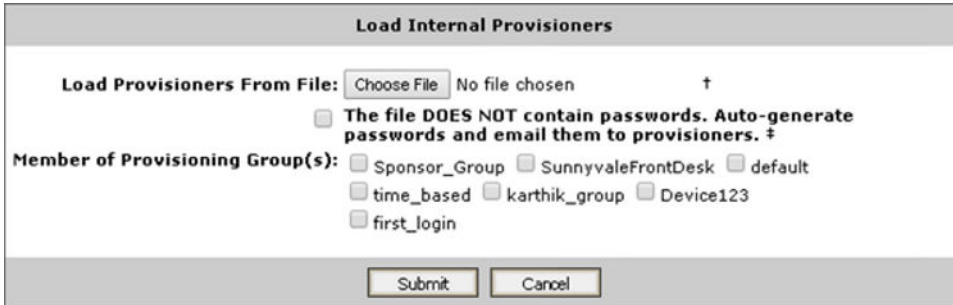
! Important:

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

! Important:

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

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



4. To the right of the **Load Provisioners From File** field, click the **Browse** button and browse to find your CSV file. Click **Open**.

5. If you wish to import passwords from the file, clear the **File DOES NOT contain passwords** check box. With this check box selected, Guest and IoT Manager automatically chooses a password for each provisioner you import.
6. In the **Member of Provisioning Group(s)** section, select the check box(es) of the groups to which the imported provisioners will belong. Membership in a provisioning group establishes the provisioners' rights and settings.
7. Click **Submit**. Guest and IoT Manager displays a progress bar while it imports the users. Under some conditions, the bulk loading may take several minutes to complete.

Once the provisioner accounts have been created, you may view them by clicking **Provisioners** in the command bar on the left of the window. To see a record of the success or failure of each account creation attempt, check your Guest and IoT Manager logs as explained in [Viewing the log files](#) on page 90.

Checklist: Before your provisioners start working

Before your provisioners can start working, you (as Guest and IoT 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 and IoT Manager Provisioner Application: Each provisioner must be able to connect to the Guest and IoT Manager Provisioner Application via his or her browser.
- Connection to an Ignition Server appliance: The Guest and IoT 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 and IoT Manager to send email notifications to new guest users. See [Setting up Email notification parameters](#) on page 62. If desired, make sure you have configured Guest and IoT Manager to send SMS messages. See [Setting up SMS notification parameters](#) on page 65.

If you have created your guest authorization policies and set up your provisioner accounts, you should now train the provisioners to use the Guest and IoT Manager Provisioner Application. As the basis for this training, use [Provisioner application: Managing guests and devices](#) on page 196.

Writing SMS and Email templates for account notifications

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

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

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

Before you begin

Make sure you have set up your email and/or SMS gateways as shown in [Setting up Email notification parameters](#) on page 62 and [Setting up SMS notification parameters](#) on page 65.

Procedure

1. Run the Administrator Application, and click on the **Provisioning Groups** section in the main toolbar.
2. From the **Provisioning Groups** list, click on the group whose template(s) you wish to edit.
3. Click the **Notification > General** tab in the *Edit Provisioning Group* screen. You will see the **SMS Template**, **Email Charset** and the **Email Template**. The text boxes and options to the right of these fields display the current account notification messages being sent to new users.
4. Edit the **SMS**, **Email Charset**, or **Email Template**.
 - **SMS Template:** In this 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.
 - **Email Charset** You can use **HTML Character set** or **Plain Character set** option for the contents of the guest user email template. HTML Character set option allows you to select Font family, Color and Font size. Plain Character set option allows you to set plain characters without any standards in the email template. By default, HTML Character set option is selected.
 - **Email Template:** 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. *\$sponsortext* variable reflects the message entered by the sponsor while Approving or Denying the guest user account access request and the *\$terms* variable is included to add the "Terms of Use" confidential information in the email template.
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 and IoT Manager administrator to access the Provisioner Application (for example, if you want to create guest user accounts to test your policies), you must have a provisioner account for your own use.

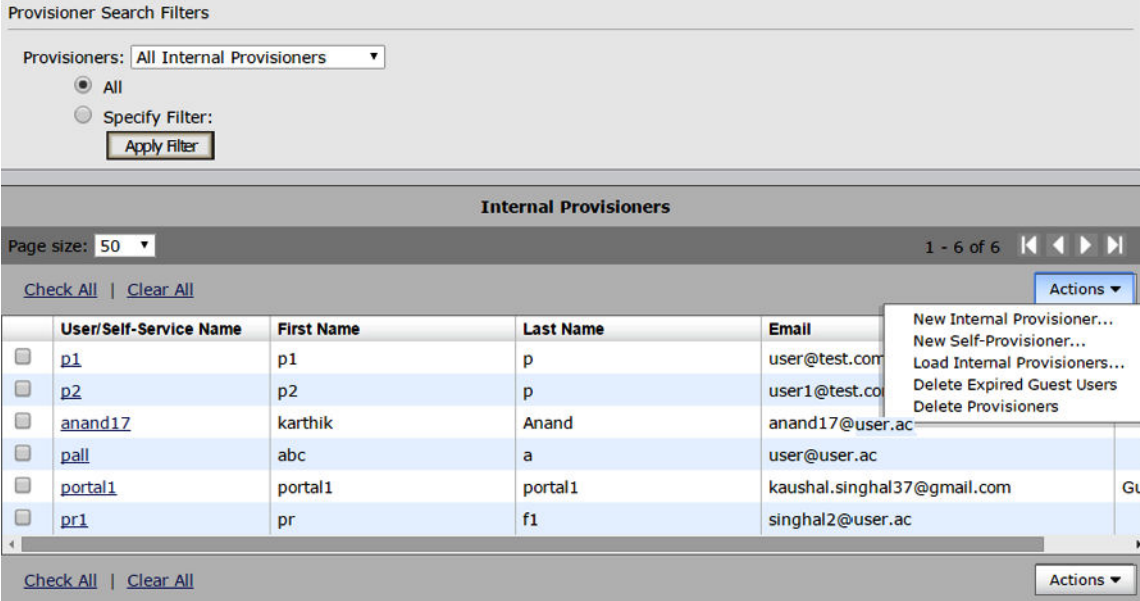
Managing provisioners

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

Your site may also use provisioner accounts that are stored externally in your corporate LDAP or Active Directory store. You cannot edit these users in Guest and IoT Manager, but you can set up rules that place them in the appropriate provisioning groups. See [Creating a Provisioner access policy](#) on page 48.

Viewing the internal provisioners list

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



The screenshot shows the 'Provisioner Search Filters' window. At the top, there is a dropdown menu for 'Provisioners' set to 'All Internal Provisioners'. Below it are radio buttons for 'All' (selected) and 'Specify Filter:'. An 'Apply Filter' button is present. The main area is titled 'Internal Provisioners' and shows a table of provisioners. The table has columns for 'User/Self-Service Name', 'First Name', 'Last Name', and 'Email'. There are 6 rows of data. A context menu is open over the table, showing options like 'New Internal Provisioner...', 'New Self-Provisioner...', 'Load Internal Provisioners...', 'Delete Expired Guest Users', and 'Delete Provisioners'. At the bottom, there are 'Check All' and 'Clear All' links, and an 'Actions' dropdown menu.

User/Self-Service Name	First Name	Last Name	Email
p1	p1	p	user@test.com
p2	p2	p	user1@test.co
anand17	karthik	Anand	anand17@user.ac
pall	abc	a	user@user.ac
portal1	portal1	portal1	kaushal.singhal37@gmail.com
pr1	pr	f1	singhal2@user.ac

Figure 10: Provisioner search filter window

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

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

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

The **Actions** drop-down menu allows you to carry out the following actions:

 **Note:**

You can also perform bulk actions that apply to all the provisioners whose check boxes you have selected.

- **New Internal Provisioner** displays Create Provisioner page to create a new internal provisioner.
- **New Self-Provisioner** displays Create Self-Provisioning Service page to create a new self-provisioner.
- **Load Internal Provisioner** displays Load Internal Provisioners page to upload provisioners the information from the selected file.
- **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 187.
- **Delete Provisioners** deletes the selected provisioner(s). See [Deleting a provisioner account](#) on page 169.

Modifying a provisioner account

Procedure

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

The Edit Provisioner screen appears. This screen contains the same fields as the Create Provisioner screen. See [Creating a provisioner in the internal store](#) on page 162 for an explanation of each field.

4. Edit the fields as desired. If you wish to change the provisioner's password, click the "change" link in the **Password** field.
5. Click **Submit**.

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

6. (Optional) Click **Cancel** to cancel the changes.

Assigning a provisioner to a provisioning group

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

This procedure works only for *internal provisioners* stored in Ignition. If your provisioners are stored in LDAP or AD, turn instead to [Creating a Provisioner access policy](#) on page 48.

Procedure

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

The Edit Provisioner screen appears

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

Deleting a provisioner account

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

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

Procedure

1. Click **Provisioners** in the main toolbar of the Administrator Application. The Internal Provisioners screen appears displaying the list of provisioners.
2. If the provisioner you plan to delete owns guest and device accounts and you wish to keep those accounts, then reassign them as explained in [Reassigning a provisioner's guest user accounts and devices to another provisioner](#) on page 177.
3. From the Internal Provisioners list, select the check box of the provisioner account(s) you wish to delete.
4. In the **Actions** menu, choose the **Delete Provisioners** command. In the confirmation dialog, click **OK**.

 **Warning:**

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

Changing a provisioners password

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

Procedure

1. Click **Provisioners** in the main toolbar of the Administrator Application. The Internal Provisioners screen appears displaying the list of provisioners.
2. Click the **User/Self-Service Name** of the provisioner whose password you wish to change. The Edit Provisioner window appears.
3. In the **Password** field, select the **Change** link.
4. Type the new `password` in the **New Password** field.
5. Retype the `password` in the **Confirm Password** field.
6. Click **Submit**.

Setting the provisioner time-out period

See [Provisioner Idle Timeout Threshold](#) on page 89.

Monitoring provisioner and guest logins

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

Procedure

1. Run Ignition Dashboard (see [Launching Ignition Dashboard](#) on page 245) 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. For more information, see *Identity Engines Ignition Server Configuration, NN47280-600*.

You can also filter the set of records. For more information, see *Identity Engines Ignition Network Analytics, NN47280-605*.

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 and IoT Manager application settings.

The most common tasks are described in the following sections:

- [Modifying a provisioning group](#) on page 175
- [Setting provisioner groups for provisioners stored in LDAP and AD](#) on page 177

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.

Provisioning Groups		
Check All Clear All		Actions ▼
	Name	Access Rights
<input type="checkbox"/>	cxv	Guest User
<input type="checkbox"/>	default	Guest User
<input type="checkbox"/>	Guest Standard	Guest User, Device
<input type="checkbox"/>	mobile	Mobile App
<input type="checkbox"/>	mobile1	Mobile App
<input type="checkbox"/>	pg-api-user-device	API Guest User, API Device
<input type="checkbox"/>	pg-fl	Guest User
<input type="checkbox"/>	pg1	API Guest User
<input type="checkbox"/>	pg2	Guest User, Device
<input type="checkbox"/>	social-media	Social Media Guest User
<input type="checkbox"/>	social-media1	Social Media Guest User
<input type="checkbox"/>	t2	Guest User
<input type="checkbox"/>	Techathon2015-Customers	API Guest User
<input type="checkbox"/>	Techathon2015-Partners	API Guest User
<input type="checkbox"/>	test	Guest User
<input type="checkbox"/>	test1	Guest User
Check All Clear All		Actions ▼

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

The **Actions** menu allows you to carry out bulk actions that apply to all the groups whose check boxes you have selected. The following table lists and describes the **Action** menu options available for Provisioning Groups:

Table 1: Action Menu — Provisioning Groups

Action Menu	Description
New Provisioning Group	Creates a new provisioning group.
Copy Provisioning Group	Creates a copy of the existing provisioning group. For more information, see Copying a provisioning group on page 173.
Reassign Provisioning Group Membership	Displays the Reassignment window to let you move the selected groups internal provisioners, users, or devices to a different provisioning group.
Delete Provisioning Group Members	Allows you to delete all the internal provisioners, guest users, or devices in the group you have selected. When you choose this command, Guest

Table continues...

Action Menu	Description
	Manager displays a dialogue window that allows you to choose the type of records to delete.
View Provisioning Group	Displays the Provisioning Group summary. For more information, see Viewing Provisioning Group Summary on page 176.
Delete Expired Guest Users	Deletes all the expired guest accounts owned by the provisioner(s) you have selected. For more information, see Deleting expired guest users on page 187.
Delete Provisioning Groups	Deletes the selected group(s).

Copying a provisioning group

Use the following procedure to create a copy of an existing provisioning group.

*** Note:**

Copy Provisioning Group option will only create a new Provisioning Group. The Provisioners, Guest Users, or Devices associated with the source Provisioning Group will not be added to the copied Provisioning Group.

Before you begin

- Open a browser and navigate to the Administrator Application URL.
- Type your Guest and IoT Manager administrator username and password.

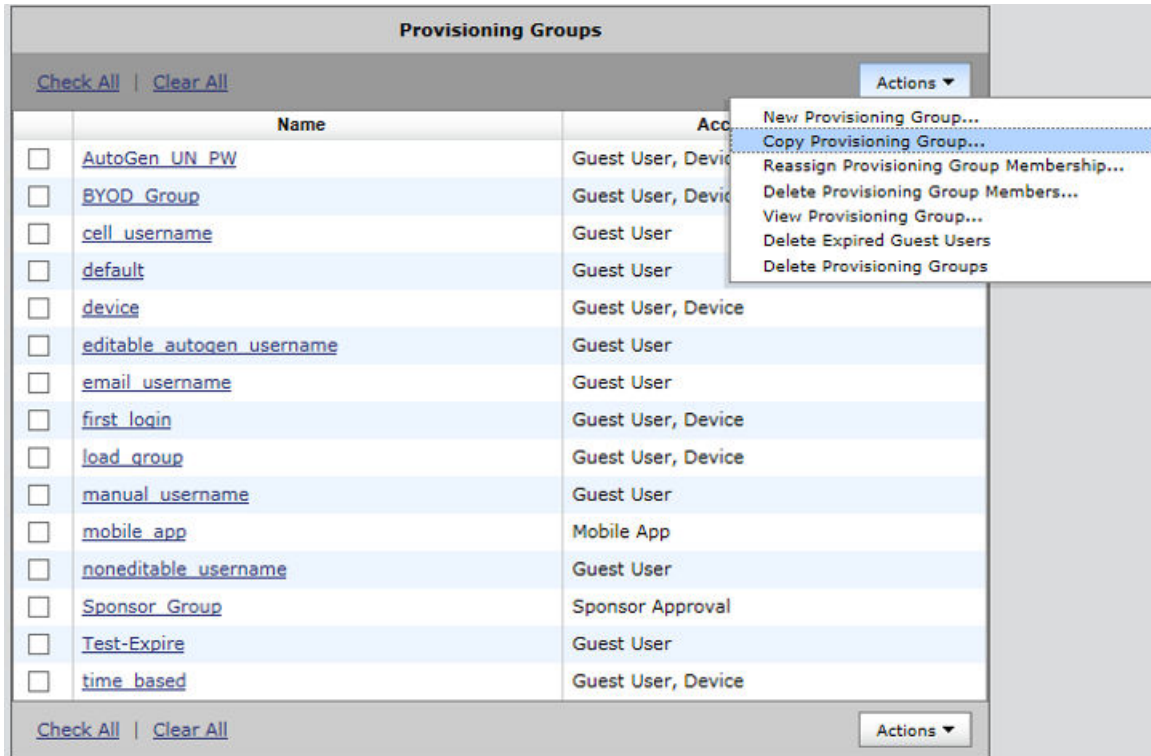
*** Note:**

Ensure that the Guest and IoT Manager is connected to the Ignition Server appliance.

Procedure

1. Click **Provisioning Groups** in the main toolbar of the Administrator Application.
2. Check one provisioning group in the **Provisioning Groups** table.

The system displays the following page.



3. Select **Copy Provisioning Group** from the **Actions** drop-down.

The system displays the **Copy Provisioning Group** page.

Figure 11: Copy Provisioning Group page

You must enter the name of the new Provisioning Group. The provisioning group configuration will be same as the selected (source) Provisioning Group. However, before submitting, you can make the required changes to the new Provisioning Group.

4. Click **Submit**.

Modifying a provisioning group

Procedure

1. Click **Provisioning Groups** in the main toolbar of the Administrator Application.
2. In the table, click the name of the provisioning group that you wish to modify.

3. In the Edit Provisioning Group window, make your edits and click **Submit**.

Viewing Provisioning Group Summary

Use the following procedure to view the provisioning group summary.

Procedure

1. Click **Provisioning Groups** in the main toolbar of the Administrator Application.
2. In the **Provisioning Groups** table, select the check box of the **Provisioning Group** that you wish to view summary.

*** Note:**

You can view only one **Provisioning Group** summary at a time.

3. Click **Actions** drop-down and click **View Provisioning Group**.

Provisioning Groups	
Name	Access Rights
<input type="checkbox"/> AutoGen_UN_PW	Guest User, Device
<input type="checkbox"/> BYOD_Group	Guest User, Device
<input type="checkbox"/> cell_username	Guest User
<input type="checkbox"/> default	Guest User
<input type="checkbox"/> device	Guest User, Device
<input type="checkbox"/> editable_autoquen_username	Guest User
<input type="checkbox"/> email_username	Guest User
<input type="checkbox"/> first_login	Guest User, Device
<input type="checkbox"/> load_group	Guest User, Device
<input type="checkbox"/> manual_username	Guest User
<input type="checkbox"/> mobile_app	Mobile App
<input type="checkbox"/> noneditable_username	Guest User
<input type="checkbox"/> Sponsor_Group	Sponsor Approval
<input type="checkbox"/> Test-Expire	Guest User
<input type="checkbox"/> time_based	Guest User, Device

The system displays the **View Provisioning Group: <Provisioning Group Name>** details.

Setting provisioner groups for provisioners stored in LDAP and AD

If your provisioner accounts are stored in LDAP or Active Directory, you must set up rules to associate each provisioner account with a provisioning group. The provisioning group provides the provisioner's rules of operation. See this setup as shown in [Creating a Provisioner access policy](#) on page 48 or [Creating an Advanced Provisioner access policy](#) on page 52.

Managing group memberships

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

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Provisioning Groups** from the main toolbar.
2. Select the check box of the name of the provisioning group of the provisioner whose guests and/or devices you wish to reassign.
3. Click **Actions** > **Reassign Provisioning Group Membership**.
4. In the *middle part* of the window, check **Reassign members of**.
5. Check the **Guest Users** and/or **Devices** check boxes, as applicable.
6. In the **being managed by provisioner** field, type the name of the provisioner who currently owns the users or device records.

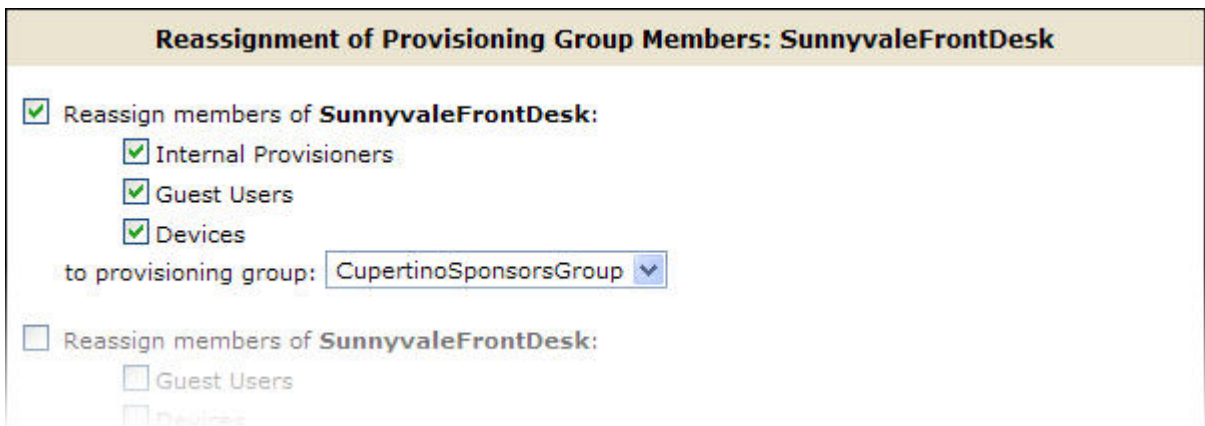
The screenshot shows a configuration window for reassigning group membership. At the top, there is a dropdown menu for 'to provisioning group:' with 'CupertinoSponsorsGroup' selected. Below this, a checked checkbox 'Reassign members of SunnyvaleFrontDesk:' is followed by two sub-checkboxes, 'Guest Users' and 'Devices', both of which are also checked. Underneath, there are two text input fields: 'being managed by provisioner:' containing 'lblack' and 'to provisioner:' containing 'hazaria'. To the right of the 'to provisioner:' field are two radio buttons: 'Internal Provisioner' (which is selected) and 'LDAP Provisioner'. At the bottom, there is an unchecked checkbox labeled 'Assign SunnyvaleFrontDesk members not being managed by a provisioner:'.

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

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

Procedure

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



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

Assigning unmanaged guests or devices to a provisioner

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Provisioning Groups** on the main toolbar.

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

Internal Provisioner LDAP Provisioner
 Assign **Sunnyvale-Sponsors** members not being managed by a provisioner:
 Guest Users
 Devices
 to provisioner:
 Internal Provisioner LDAP Provisioner

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

Operations on Guest Users

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

Retrieving the guest users owned by a provisioner

Procedure

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

Example

Guest User Search Filters

All Guests
 Specify Filter: Provisioner Contains Apply Filter

Guest Users

Page size: 50 1 - 2 of 2

[Select All](#) | [Clear All](#)

[Extend Expiration](#)
[Resend Password](#)
[Export](#)
[Delete](#)

	User Name	First Name:	Last Name:	Email	SMS Address	Start Time	End Time
<input type="checkbox"/>	FH3z5WHC	Karthik	Anand	anand17@extreme.com	2233456789@txt.att.net	2017/04/26 05:19:31 PM GMT+00:00	2017/04/27 01:15:00 PM GMT+00:00
<input type="checkbox"/>	prasad25	Lakshmi	Prasad	prasad25@extreme.com	9898989898@txt.att.net	2017/04/26 05:58:37 PM GMT+00:00	2017/04/27 01:15:00 PM GMT+00:00

Figure 12: Guest User search filter- Provisioner

Retrieving the guest users that belong to a provisioning group

Procedure

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

Retrieving the guest users first login pending accounts

About this task

Perform this procedure to retrieve the list of all the first login pending accounts created before the specific date. You can use this procedure to delete those inactive accounts.

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Guest Users** from the left-hand navigation tree.
The system displays the list of all the guest users provisioned.
2. Select **Specify Filter** and select **First Login Pending and Created Before** from the drop-down menu.
 - a. Enter the date in YYYY/MM/DD format or optionally click the calendar icon to choose a date.
 - b. Enter the time and select AM or PM from the drop-down menu.

- c. Select the time zone from the drop-down menu.
3. Click **Apply Filter**.
The system displays the list of all the first login pending accounts created before the specific date as entered in the time field.
4. **(Optional)** Click the following options button on the Guest Users section to perform the below-stated action:

Option	Description
Export	Exports to a CSV-formatted file the account details of all the pending guest accounts displayed.
Delete	Deletes the account details of all the pending guest accounts.

Example

Figure 13: Guest User search filter- First login pending and created before

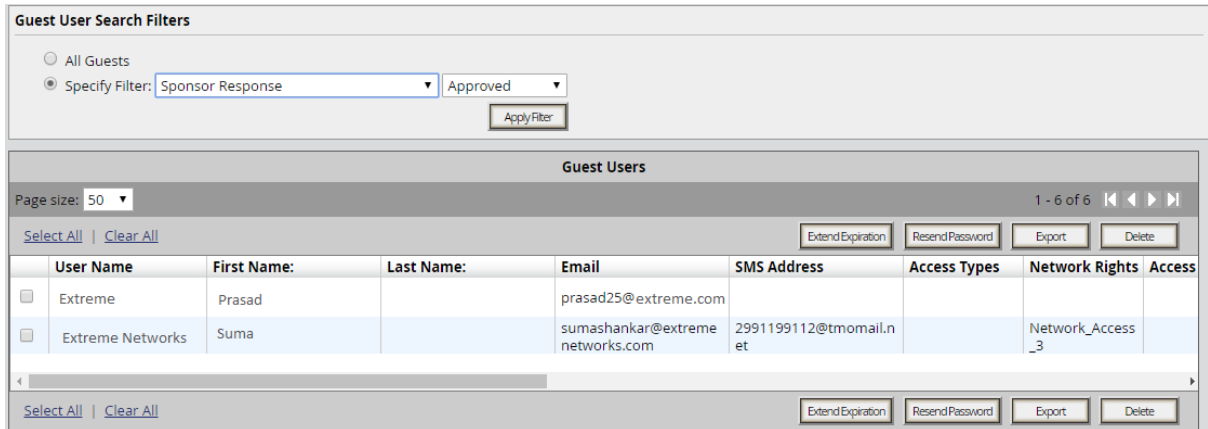
Retrieving Guest Users based on sponsor response

About this task

Perform this procedure to retrieve the list of all the guest users based on Sponsor's Response.

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Guest Users** from the left-hand navigation tree.
The system displays the list of all the guest users provisioned.
2. Select **Specify Filter** and select **Sponsor Response** and select one of the values among:
 - Approved
 - Denied
 - Pending
 - Auto-Approved
 - Auto-Denied
 - Not Applicable
3. Click **Apply Filter**.
The system displays the list of all the guest users which have the selected Sponsor Response.



Retrieving the guest users activated in last X hours

About this task

Perform this procedure to retrieve the list of all the guest users activated in last X hours.

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Guest Users** from the left-hand navigation tree.

The system displays the list of all the guest users provisioned.

2. Select **Specify Filter** and select **Guest Users activated in the last** and enter number of hours in the **hours** field.

3. Click **Apply Filter**.

The system displays the list of all the guest users activated in last X hours. Here, X represents the number of hours as entered in **hours** field.

Example

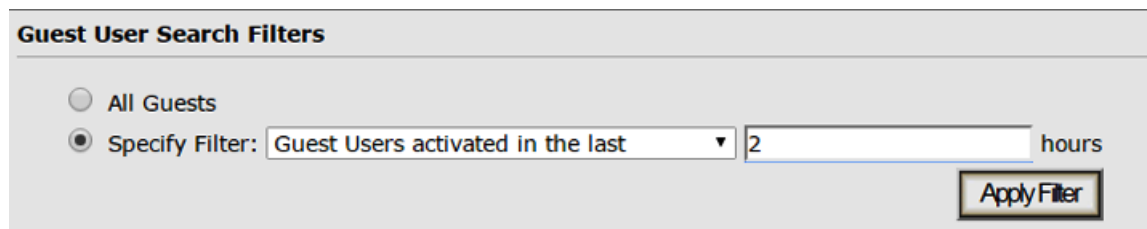


Figure 14: Guest User search filter- Guest users activated in the last

Viewing expired guest users accounts

About this task

Perform this procedure to view the list of all the expired guest user accounts. When guest accounts are expired, the affected guest users cannot access the network. You can also use this procedure to delete all the expired guest user accounts.

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Guest Users** from the left-hand navigation tree.

The system displays the list of all the guest users provisioned.

2. Select **Specify Filter** and select **Expired Guest Users** from the drop-down menu.
3. Click **Apply Filter**.

The system displays the list of all the expired guest user accounts.

Extending expiry of a guest user account

Extend Expiration enables you to extend the duration of expiry of a guest user account(s) at one click. **Extend Expiration** includes the following two enhancements:

1. A new filter `Guest Users expiring in the next 'X' days` – It calculates and fetches the users according to:

$$\text{CURRENT_TIME} < \text{END_TIME} < \text{CURRENT_TIME} + X \text{ days}$$

'X' is a variable here. So, if you want to filter all Guest Users expiring tomorrow, you can select the filter `Guest Users Expiring in the next 1 days`.

 **Note:**

This filter is available to the Guest and IoT Manager administrator also.

2. A new button **Extend Expiration** in the **Provisioner > Guest User > View** page. For each selected Guest User, the duration of expiry will be calculated as:

$$\text{DURATION} = \text{END_TIME} - \text{START_TIME}$$

Then, the account will be modified to:

$$\text{START_TIME} = \text{OLD_END_TIME}$$

$$\text{END_TIME} = \text{OLD_END_TIME} + \text{DURATION}$$

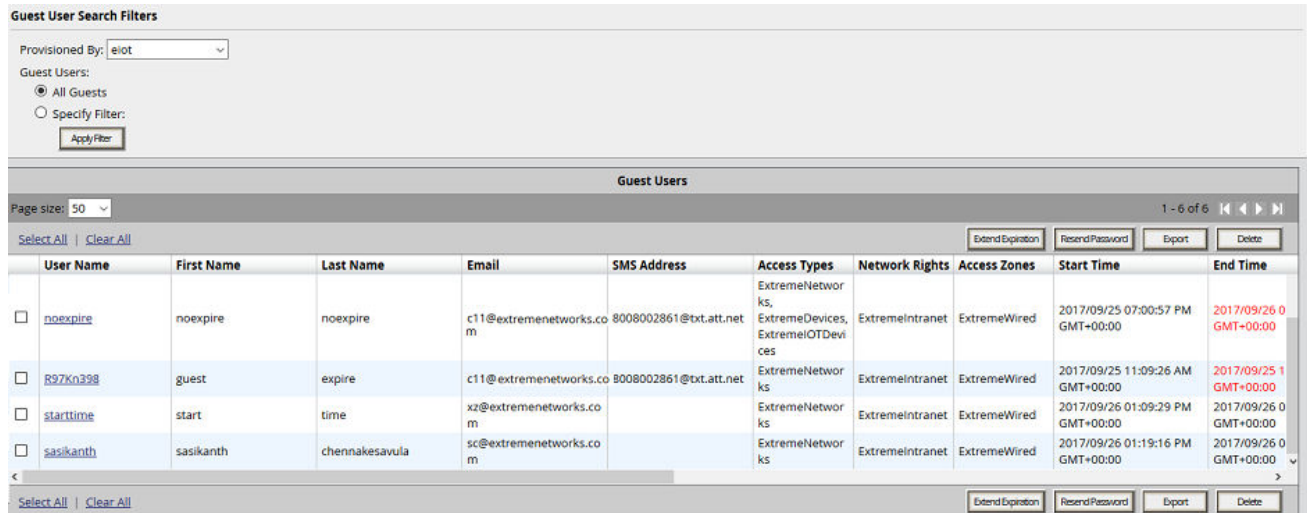


Figure 15: New filter and Extend Expiration button in Provisioner's Guest User View page

Example

Consider two guest users, User 1 valid for a duration of one month and User 2 valid for a duration of two months, both are expiring at 02:00 P.M. tomorrow. When you select these two accounts and click **Extend Expiration** button, their expiry is extended as follows:

- User 1 is extended as Start Time = 02:00 P.M. tomorrow and End Time = 02:00 P.M. tomorrow + 1 month.
- User 2 is extended as Start Time = 02:00 P.M. tomorrow and End Time = 02:00 P.M. tomorrow + 2 months.

* Note:

- Provisioners can use Extend Expiration to extend the duration of expiry for expired Guest User account(s) also.
- Expiry of First Login Pending Guest Accounts cannot be extended.

Resending Password to Guest User(s)

Resend password enables you to resend the password to Guest User(s). When one or more users are selected and the **Resend Password** button is clicked, then the following checks are performed depending on which the password is sent via Email or SMS or both:

1. Notification options has either SMS / Email or both enabled
2. The account is not locked / expired
3. The Email / SMS Template contains \$password

Guest Users										
User Name	First Name	Last Name	Email	SMS Address	Access Types	Network Rights	Access Zones	Start Time	End Time	
<input type="checkbox"/> noexpire	noexpire	noexpire	c11@extremenetworks.com	8008002861@txt.att.net	ExtremeNetworks, ExtremeDevices, ExtremeIoTDevices	ExtremeIntranet	ExtremeWired	2017/09/25 07:00:57 PM GMT+00:00	2017/09/26 0 GMT+00:00	
<input type="checkbox"/> R97Kn398	guest	expire	c11@extremenetworks.com	3008002861@txt.att.net	ExtremeNetworks	ExtremeIntranet	ExtremeWired	2017/09/25 11:09:26 AM GMT+00:00	2017/09/25 11:09:26 AM GMT+00:00	
<input type="checkbox"/> starttime	start	time	xz@extremenetworks.com		ExtremeNetworks	ExtremeIntranet	ExtremeWired	2017/09/26 01:09:29 PM GMT+00:00	2017/09/26 0 GMT+00:00	
<input type="checkbox"/> sasikanth	sasikanth	chennakesavula	sc@extremenetworks.com		ExtremeNetworks	ExtremeIntranet	ExtremeWired	2017/09/26 01:19:16 PM GMT+00:00	2017/09/26 0 GMT+00:00	

Retrieving guest users based on sponsor E-mail

About this task

Perform this procedure to filter guest users based on their sponsor e-mail. This procedure displays all guest users created by each sponsor using the filter criteria.

Procedure

- From the Guest and IoT Manager Administrator Application, click **Guest Users** from the left-hand navigation tree.

The system displays the list of all the guest users provisioned.

- Select **Specify Filter** and select **Sponsor Email** and enter the desired search criteria as given below using the drop-down menu:

- Start With
- Equal
- Not Equal
- Contains
- Ends With

- Click **Apply Filter**.

The system displays the list of guest user based on the sponsor Email filter criteria

Example

Guest User Search Filters

All Guests
 Specify Filter:
 Sponsor Email
Contains
extreme.com

Apply Filter

Figure 16: Guest User search filter- sponsor Email with <Contains - extreme.com> as selected filter

Viewing and Printing Guest User account details

To view and optionally print an account summary of a Guest User account, do the following:

Procedure

1. On the left-hand navigation pane of the Guest and IoT Manager Administrator Application, click **Guest Users**.

The system displays the Guest User screen.

2. On the Guest Users screen, locate the row containing the Guest User whose account details you wish to print.
3. Click on the Guest User entry under the **Username** column.
4. Click **View**.

The system displays the selected Guest User Information page.

Guest User Info: sasikanth

User Name: sasikanth
First Name: sasikanth
Last Name: chennakesavula
Password: h9f4QvUY
Email: sc@extremenetworks.com
Cell Phone:
Comments:

Guest Details:
Activate Account On: 2017/09/26 01:19:16 PM GMT+00:00
Expire Time: 2017/09/26 09:19:16 PM GMT+00:00
Delete on Expire: Yes
Group Membership: GuestManagerIoT
Provisioner: Internal/eiot
Access: ExtremeNetworks
ExtremeWired
ExtremeIntranet
Access Types: ExtremeNetworks
Network Rights: ExtremeIntranet
Access Zones: ExtremeWired

[Edit Guest User](#)

[Printer Friendly Version](#)

5. (Optional) Click **Printer Friendly Version** to print the Guest User information.

*** Note:**

To customize the Printer Friendly page see, [Customizing Printer Friendly Page](#) on page 193 .

Deleting the guest users of a provisioner or provisioning group

Procedure

1. Load the users as explained in [Retrieving the guest users owned by a provisioner](#) on page 179 or as explained in [Retrieving the guest users that belong to a provisioning group](#) on page 180.
2. Select the check box of each user you want to delete.
3. Click **Delete**.

Deleting expired guest users

Procedure

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

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

Exporting guest user records to a file

About this task

Perform this procedure to export guest user records to a file. You can use this procedure to delete those inactive accounts.

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Guest Users** from the left-hand navigation tree.
The system displays the list of all the guest users provisioned.
2. Select **Specify Filter** and select the desired entry from the drop-down menu.
3. Click **Apply Filter**.

The system displays the filtered result in the Guest Users window.

4. Click the following button on the Guest Users section to perform the export:

Button	Description
Export	Exports the account details of all the guest accounts displayed on a CSV-formatted file.

Operations on Devices

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

Retrieving the devices owned by a provisioner

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Devices** from the left-hand navigation tree.
By default, all Guest and IoT Manager device records are displayed in the frame.
2. Select **Specify Filter** and select **Provisioner** from the drop-down menu.
3. Enter the operation (Start with, Equal, Not Equal, Contains, Ends With) and the name of the provisioner.
4. Select Guest and IoT Manager and Non Guest and IoT Manager in **From** field.
5. Click **ApplyFilterandRefresh**. A list of devices provisioned by the selected provisioner appears.

Retrieving the devices owned by a provisioning group

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Devices** from the left-hand navigation tree.
The system displays the device record screen.
2. Select **Specify Filter** and select **Provisioning Group** from the drop-down list.
3. Select the provisioning group from the drop-down menu of provisioning groups.
4. Select Guest and IoT Manager and Non Guest and IoT Manager in **From** field.
5. Click **ApplyFilterandRefresh**. A list of devices owned by the selected provisioning group appears.

Retrieving the devices activated in last X hours

About this task

Perform this procedure to retrieve the list of all the devices activated in last X hours.

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Devices** from the left-hand navigation tree.

By default, all Guest and IoT Manager device records are displayed in the frame.

2. Select **Specify Filter** and select **Devices activated in the last** and enter number of hours in the **Hours** field. You can also select Guest and IoT Manager and Non Guest and IoT Manager in **From** field.
3. Click **ApplyFilterandRefresh**.

The system displays the list of all the selected devices activated in last X hours. Here, X represents the number of hours as entered in **Hours** field.

Viewing a device record summary

About this task

Use the following procedure to view the device record summary.

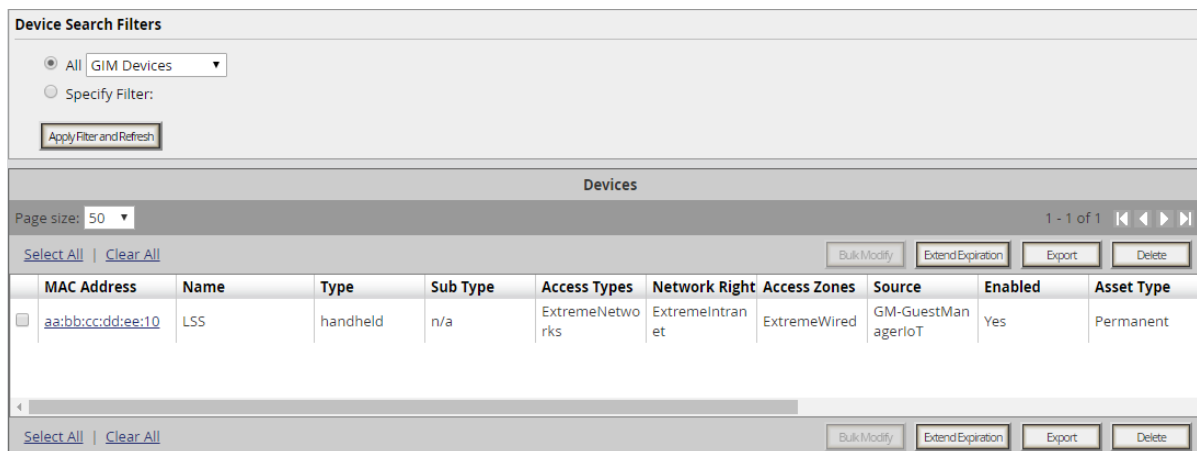
Before you begin

- Log in to the Guest and IoT Manager Administrator Application.

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Devices** from the left-hand navigation tree.

The system displays the device record screen.



By default, all Guest and IoT Manager device records are displayed in the frame.

2. Select **All** option and select Guest and IoT Manager or Non Guest and IoT Manager devices from the drop-down list.
3. **Optional:** Select **Specify Filter** option to select specific device attributes from the drop-down list. For example, you can provide explicit operations such as Start with, Equal, Not Equal, Contains, Ends With and the name of the search value. You can also select Guest and IoT Manager and Non Guest and IoT Manager in **From** field.
4. Click **ApplyFilterandRefresh** to view the selected device records displayed in the frame.
5. On the Device screen frame, locate the row containing the device record whose details you wish to view.
6. Click on the device entry beneath the **MAC Address** column.
7. Click **View**.

The system displays the selected device record details page.

Device Info: 22:22:22:22:22:22	
MAC Address:	22:22:22:22:22:22
Name:	Device
Type:	fax machine
Sub Type:	n/a
Source:	GIM-ExtremeloTManagement
Comments:	
Record Enabled:	Yes
Asset Type:	Temporary
Activate Account On:	2017/10/24 05:45:25 AM GMT+00:00
Expire Time:	2017/10/24 01:45:25 PM GMT+00:00
Delete on Expire:	Yes
Group Membership:	ExtremeloTManagement
Provisioner:	Internal/eiot
Access Types:	ExtremeloTManage ExtremeloTDevice
Network Rights:	ExtremeloTWired
Access Zones:	ExtremeloTFirstFloor
Guest Users:	

Viewing the pending devices list

About this task

Perform this procedure to view the list of all the pending device accounts created before the specific date. You can use this procedure to delete those inactive accounts.

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Devices** from the left-hand navigation tree.
By default, all Guest and IoT Manager device records are displayed in the frame.
2. Select **Specify Filter** and select **First Login Pending and Created Before** from the drop-down list.
 - a. Enter the date in YYYY/MM/DD format or optionally click the calendar icon to select a date.
 - b. Enter the time and select AM or PM from the drop-down list.

- c. Select the time zone from the drop-down list.
 - d. Select Guest and IoT Manager and Non Guest and IoT Manager in **From** field.
3. Click **ApplyFilterandResearch**.

The system displays the list of all the first login pending device accounts created before the specific date as entered in the time field.

Viewing expired device accounts

About this task

Perform this procedure to view the list of all the expired device accounts. You can also use this procedure to delete all the expired device accounts.

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Devices** from the left-hand navigation tree.
By default, all Guest and IoT Manager device records are displayed in the frame.
2. Select **Specify Filter** and select **Expired Devices** from the drop-down list.
3. Click **ApplyFilterandRefresh**.

The system displays the list of all the expired device accounts.

Exporting device records to a file

Procedure

1. From the Guest and IoT Manager Administrator Application, click **Devices** from the left-hand navigation tree.
By default, all Guest and IoT Manager device records are displayed in the frame.
2. Select **Specify Filter** and select the desired entry from the drop-down list.
3. Select Guest and IoT Manager and Non Guest and IoT Manager in **From** field.
4. Click **ApplyFilterandRefresh**.

The system displays the filtered result in the Devices screen.

5. Select the all / required device and click **Export**, to export the account details of the devices available in a CSV-formatted file.

Customizing End User Web Portals

The Identity Engines Guest and IoT Manager allows you to make global customization changing the look and feel of the web pages user see and print in the Guest and IoT Manager Portal.

- [Customizing the IDE Ignition Guest and IoT Manager Logo and Login Page](#) on page 80.

File Manager

File Manager allows you to manage files that you need for customizing the following feature on the Guest and IoT Manager portal:

- [Customizing Printer Friendly Page](#) on page 193.

Customizing Printer Friendly Page

About this task

You can use this procedure to customize the Printer friendly page using the newly introduced **File Manager** option. By default system is pre-installed with the following four sample files:

- `sample_print.css`
- `sample_print_page.html`
- `sample_style.css`
- `sample_logo.gif`

Before you begin

- Open a browser and navigate to the Administrator Guest and IoT Manager Application URL.
- Type your Guest and IoT Manager administrator `username` and `password`.

* Note:

Guest and IoT Manager must be connected with the Ignition Server appliance.

Procedure

1. Navigate to the left-hand navigation pane and click **Administration > File Manager**.

The system displays the following screen on the right-hand pane.

Files		
	Name	Size
<input type="checkbox"/>	sample_print.css	38 B
<input type="checkbox"/>	sample_print_page.html	1.8 KB
<input type="checkbox"/>	sample_style.css	1.6 KB
<input type="checkbox"/>	sample_logo.gif	2.1 KB

Check All | Clear All

Upload Download Delete

2. Click **Upload**.

The system displays the **Upload** window.

- Click **Browse** to upload the files to customize the Printer Friendly page.

! **Important:**

- Ensure that the file size is less than 10 MB.
- There is no restriction on number of files or file extension.
- You can choose Guest User attributes that you want to display in the page by adding following appropriate variables in the HTML file:

Attributes	Definition
<i>\$username</i>	Displays the guest username.
<i>\$password</i>	Displays the guest account password.
<i>\$firstname</i>	Displays the guest first name.
<i>\$lastname</i>	Displays the guest last name.
<i>\$email</i>	Displays the guest email address.
<i>\$cellphone</i>	Displays the guest cellphone number.
<i>\$starttime</i>	Displays the start time when the guest account becomes usable.
<i>\$endtime</i>	Displays the end time of the guest account.
<i>\$comment</i>	Displays any comments entered by Provisioner for the Guest User.
<i>\$termsofuse</i>	Displays the terms of use text. For more information, see Configuring the account notification templates on page 157.

- You can retrieve the uploaded External images/css files from the File Manager by using the URL in the following format and by entering the actual file name in place of the file name variable:

`/Guest&IoTManager/uploads/<file_name>.`

Sample: ``

- Click **Submit** to upload the file.
- (Optional)** You can select the desired file name from the given list and click **Download** to download a file.
- (Optional)** Select a desired file name from the given list and click **Delete** to delete any existing file name.

! **Caution:**

- You cannot delete files that are used by any Provisioning Groups.
- It is recommended to retain all the files that are used by any Provisioning Groups.

***** **Note:**

You cannot delete the pre-installed four sample files.

Next steps

Navigate to **Provisioning Groups** and select **Customize Printer Friendly Page** to enable customizing option. For more information, see [Configuring the Guest UserTab](#) on page 135.

Chapter 10: Provisioner application: Managing guests and devices

As an Identity Engines Guest and IoT 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 and IoT Manager Provisioner Application to perform these actions.

Introduction to guest user accounts

A guest user is a visitor, or other temporary user, to whom you grant specific, limited rights to use your network. Guest user accounts expire automatically after a specified period of time. Creation of guest user accounts is done in the Guest and IoT Manager application by a provisioner. For a comparison of user types, see [Types of accounts in your Ignition Server installation](#) on page 16.

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 and IoT Manager. The table below explains the attributes that define a guest user account. Note that the available access types, network rights, and access zones are customized for your site; your Ignition Server Administrator will have set up these fields in Ignition Dashboard.

Field	Description
Group Membership	The provisioning group of which this user is a member. You must choose the provisioning group before you begin creating a user, because the provisioning group limits what rights can be granted to the user.
First Name	First or given name of the guest user
Last Name	Family name of the guest user
User Name	Login name of the guest. Cannot contain spaces. User name entered should be unique. If the provisioning group is configured to auto-generate the user name, the User Name field is auto-filled after the provisioner enters the first and last names.
Password	The password for the guest user account. If the provisioning group is configured to auto-generate the password, the Password field does not appear.
Email	Email address of the guest user. When this account is created, you can instruct Guest and IoT Manager to send a notification to this or another address. (See Send Notification below.)
Cell Phone (digits only)	The cell phone number (digits only) of the guest user. This is the number to which Guest and IoT 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 and IoT 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 and IoT Manager administrator must add the "\$comment" variable to the Email Template of the provisioning group in order to allow this value to be sent to the guest user. See Writing SMS and Email templates for account notifications on page 165.
Guest Details	Use this section to add details about the guest user, such as company name.
Activate Account on	The date and time at which the guest user account becomes active. The value in these fields defaults to the current date and time on the Ignition Server appliance. Date: Enter the start date for activating guest user account. The date should be in yyyy/mm/dd format.

Table continues...

Field	Description
	<p>Time: Enter the time in hours and minutes based on a 12-hour setting. The time should be in hh:mm format.</p> <p>AM/PM: Select AM for morning; PM for afternoon.</p>
Activate on First Login	<p>This displays as “Yes” when the Guest has been assigned the activate on first login. The Activate account information on a non-assigned guest is replaced by this information.</p>
Duration	<p>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 and IoT Manager application sets the entry to 8 hours. Type the period as an integer and set the units by selecting minutes, hours, or days from the drop-down list. See Guest user account validity period on page 199 for more details.</p>
Access Types	<p>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.</p> <p>The Guest and IoT Manager Administrator determines which Access Type check boxes are available to you.</p> <p>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.”</p>
Network Rights	<p>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.</p> <p>The Guest and IoT Manager Administrator determines which Network Rights check boxes are available to you.</p> <p>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.”</p>
Access Zones	<p>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.</p> <p>The Guest and IoT Manager Administrator determines which Access Zones check boxes are available to you.</p> <p>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.”</p>

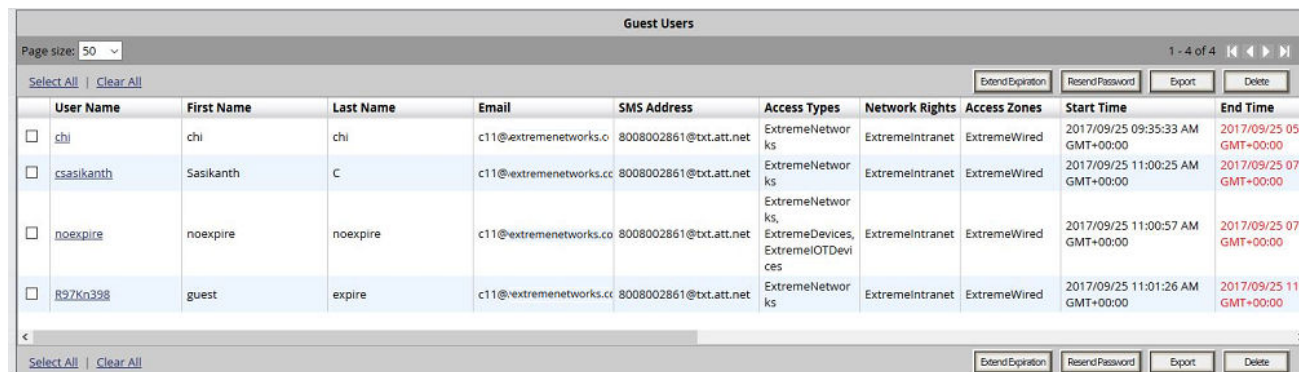
Table continues...

Field	Description
Associated Devices	To assign a laptop or other device to a user, so that the user can only log in using his own device, use the Associated Devices: Add button and assign the device to the user you are editing. This is possible only if the provisioning group allows device provisioning.
Send Notification	In this section, tick a check box for each address or number to which you wish to send an account notification. Guest and IoT Manager sends notifications via email or via SMS messaging. See Sending guest account notifications on page 204 for details.

Guest user account validity period

A user account you create in Guest and IoT 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.



User Name	First Name	Last Name	Email	SMS Address	Access Types	Network Rights	Access Zones	Start Time	End Time
<input type="checkbox"/> chi	chi	chi	c11@extremenetworks.o	8008002861@txt.att.net	ExtremeNetworks	ExtremeIntranet	ExtremeWired	2017/09/25 09:25:33 AM GMT+00:00	2017/09/25 05:00:00 GMT+00:00
<input type="checkbox"/> csasikanth	Sasikanth	C	c11@extremenetworks.cc	8008002861@txt.att.net	ExtremeNetworks	ExtremeIntranet	ExtremeWired	2017/09/25 11:00:25 AM GMT+00:00	2017/09/25 07:00:00 GMT+00:00
<input type="checkbox"/> noexpire	noexpire	noexpire	c11@extremenetworks.co	8008002861@txt.att.net	ExtremeNetworks, ExtremeDevices, ExtremeIoTDevices	ExtremeIntranet	ExtremeWired	2017/09/25 11:00:57 AM GMT+00:00	2017/09/25 07:00:00 GMT+00:00
<input type="checkbox"/> R97Kn398	guest	expire	c11@extremenetworks.cc	8008002861@txt.att.net	ExtremeNetworks	ExtremeIntranet	ExtremeWired	2017/09/25 11:01:26 AM GMT+00:00	2017/09/25 11:00:00 GMT+00:00

Figure 17: Guest user account validity period example

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

- [Checking validity of guest user account](#) on page 208
- [Renewing a guest user account](#) on page 210

How a guest user logs in

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

1. **Standard login:** In most networks, the guest user plugs his or her laptop into the wired network or connects to an open wireless access point. The networking client (known as the

“supplicant”) on the user’s laptop brings up a login dialog. The user types his or her credentials, clicks a button, and, in the typical configuration, is given a session on the appropriate VLAN or secure SSID/VLAN.

2. **Captive portal:** If you use a captive portal tool, the user plugs his laptop into the wired network, or connects to an open wireless access point and launches his browser. The captive portal intercepts the user’s web traffic and displays a login page in the browser. The user types his or her credentials, clicks a button, and, in the typical configuration, is given a session on the appropriate VLAN or secure SSID/VLAN.

Launching the provisioner application

Procedure

1. Open your web browser and type the URL of the Provisioner Application:
http://<Guest Manager machine>/GuestManager/provisioner/
OR
https://<Guest Manager machine>/GuestManager/provisioner/
where “Guest Manager machine” is the name of your Guest and IoT Manager server.
2. In the Login screen, enter your provisioner **Username** and **Password**. If you do not have a provisioner account, contact your Guest and IoT Manager Administrator.
3. Click **Login**. If your login attempt succeeds, the following message appears:
You have successfully signed in as <UserName>.

 **Important:**

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

If your login attempt fails see [Failed connection](#) on page 200.

Failed connection

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

Ignition Guest Manager is not connected to the Ignition™ Server. Please contact the Administrator.

Application time-out

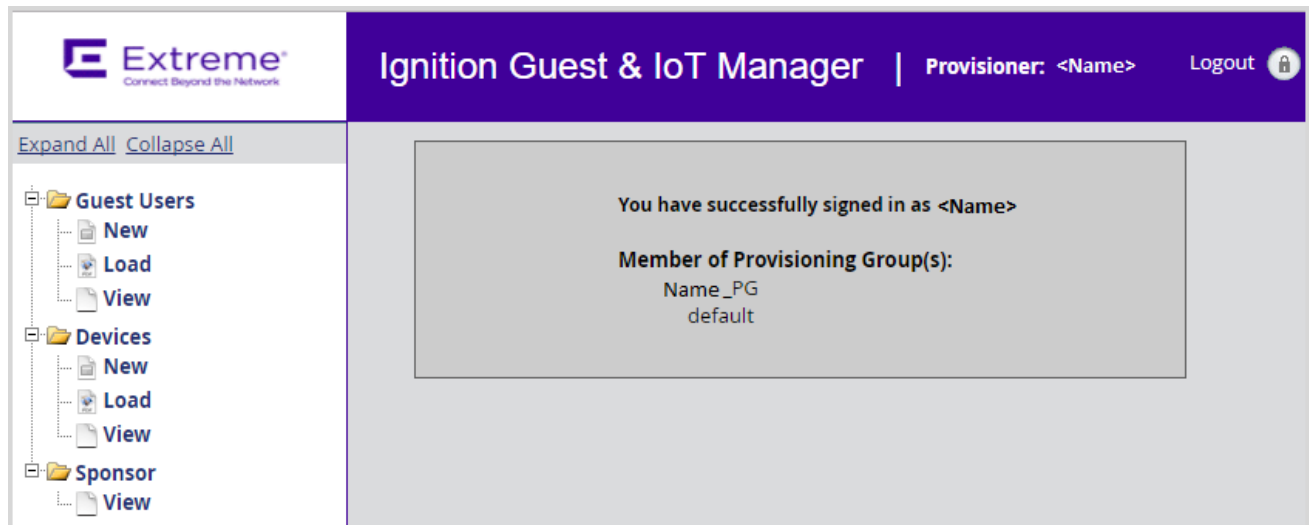
Your Provisioner Application session will disconnect if you leave it inactive for a period of time. The Guest and IoT Manager Administrator sets this timeout threshold. When you attempt to use the Provisioner Application after it has disconnected, it prompts you to log in again. Re-enter your username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



Note:

Provisioner login with Mobile App or REST API provisioning group access cannot create or load new Devices and Guest Users. Only view option will be visible.

Managing guests

Creating guest user accounts

To create many accounts at once, use the **Load Guest Users** command, instead, as explained on [Bulk importing guest user accounts from a file](#) on page 203.

Use the steps below to create a guest user account.

Procedure

1. Log in to the Provisioner Application. See [Launching the provisioner application](#) on page 200.
2. Click **Guest Users** > **New** in the toolbar on the main page of the Provisioner Application.
3. In the Create Guest User screen, provide the account details. Do the following:
 - a. In the **Group Membership** drop-down list, choose the provisioning group this guest will belong to.

Each provisioning group imposes certain account guidelines (for example, auto-generation of the user name, auto-generation of the password, max. validity period, allowable access zones, and so on), according to how the administrator configured the guest user account details for this provisioning group. As a result, the fields and defaults of the window can change after you choose a provisioning group.
 - b. Enter the account details. See [Guest user account attributes](#) on page 197 for an explanation of the rest of the fields.
 - c. If you have login instructions for the user, type them in the **Comments** field. Later when you send the user a notification email, or print the user's login information sheet, the comments are included.
 - d. **(Optional)** To cancel the changes that you have made, click **Cancel**.
4. Click **Submit**. The Guest and IoT Manager application creates the guest user account and sends email notifications to the people you specified in the Send Notifications section. See [Sending guest account notifications](#) on page 204 for details. Guest and IoT Manager displays the **Successful Guest Creation** page to confirm the account was saved.
5. You can print the users 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 199.

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

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

Bulk importing guest user accounts from a file

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

Procedure

1. Save your user data to a text file in comma-separated value (CSV) format. The format consists of one user per line.

- *If you wish to import passwords*, then format the file as follows:

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

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

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

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

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

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

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

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

Important:

Observe the following guidelines when bulk loading guest users:

- The maximum number of guest users you can import from a file is 1000.
- It is recommended 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 and IoT Manager application running, open a web browser and navigate to the Provisioner Application URL.
 - Type your provisioner `Username` and `Password`.
3. In the toolbar on the left, click **Guest Users > Load**. The Load Guest Users screen appears.
4. In the **Group Membership** drop-down list, choose the provisioning group that will own the accounts.
5. To the right of the **Load Guest Users From File** field, click the **Browse** button and browse to find your CSV file. Click **Open** to select it.

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

Once the users have been created, click **Guest Users > View** to view the users. To see a record of the success or failure of each user creation attempt, check your Guest and IoT Manager logs as explained in [Viewing the log files](#) on page 90.

Sending guest account notifications

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

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

These check boxes are present only if the Guest and IoT Manager Administrator has configured the application to send messages. For set-up instructions, see [Setting up Email notification parameters](#) on page 62 and [Setting up SMS notification parameters](#) on page 65.

Procedure

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

To set up your templates see, [Writing SMS and Email templates for account notifications](#) on page 165.

Viewing guest user accounts

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

Each provisioner owns the guest user accounts that he or she creates; however, the Guest and IoT Manager Administrator can use the Administrator Application to view all guest users. The following figure shows the overall sections of the Guest Users screen:

The screenshot shows the 'Guest User Search Filters' section with 'Provisioned By' set to 'eliot'. Under 'Guest Users', 'All Guests' is selected. Below this is the 'Guest Users' table with columns: User Name, First Name, Last Name, Email, SMS Address, Access Types, Network Rights, Access Zones, Start Time, and End Time. The table contains four rows of guest user data.

User Name	First Name	Last Name	Email	SMS Address	Access Types	Network Rights	Access Zones	Start Time	End Time
chi	chi	chi	c11@extremene:wo:ks.com	8008002861@txt.att.net	ExtremeNetworkks	ExtremeIntranet	ExtremeWired	2017/09/25 09:35:33 AM GMT+00:00	2017/09/25 05:00:00 GMT+00:00
csasikanth	Sasikanth	C	c11@extremene:wo:ks.com	8008002861@txt.att.net	ExtremeNetworkks	ExtremeIntranet	ExtremeWired	2017/09/25 11:00:25 AM GMT+00:00	2017/09/25 07:00:00 GMT+00:00
noexpire	noexpire	noexpire	c11@extremene:wo:ks.com	8008002861@txt.att.net	ExtremeNetworkks, ExtremeDevices, ExtremeIoTDevices	ExtremeIntranet	ExtremeWired	2017/09/25 11:00:57 AM GMT+00:00	2017/09/25 07:00:00 GMT+00:00
R37kn398	guest	expire	c11@extremene:wo:ks.com	8008002861@txt.att.net	ExtremeNetworkks	ExtremeIntranet	ExtremeWired	2017/09/25 11:01:26 AM GMT+00:00	2017/09/25 11:00:00 GMT+00:00

Figure 18: Guest Users screen

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

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

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

Guest User field description

The **Guest Users** screen contains the following fields and buttons. Use the data in the following table to use the Guest User screen.



Name	Description
Username	Displays the username created for the user. You can click to edit the guest user account.
Password	Displays the guest user password. The password is visible only if the Guest and IoT Manager Administrator has given you permission to view it.
First Name	Displays the first name of the guest.
Last Name	Displays the last name of the guest.
Email	Displays the E-mail address of the guest.
SMS Address	Displays the SMS Address of the guest with the combination of cell-phone and gateway provider.
Start Time	Displays the start time when the account becomes usable.  Note: The text displays in red color if the account is not yet active. Edit the guest account if you need to activate it sooner.
End Time	Displays the end time of the account.  Note: The text displays in red color for the expired accounts. Edit the guest account if you need to reactivate it.
Provisioning Group	Displays the provisioning group information.
Provisioner	Displays the provisioner information.
Sponsor Name	Displays the sponsor name.
Sponsor Email	Displays the sponsor e-mail address
Sponsor Response	Displays the sponsor response as <i>approve</i> , <i>Pending</i> , <i>Deny</i> or <i>N/A</i> .
Guest Details	Displays the guest details.
Check All	To select all the user rows, use the Check All link.
Clear All	To clear all the user rows, use the Clear All link.
Delete	Deletes all guest user account(s) whose check box(es) are selected.
Export	Exports a CSV file of the guest user records that match the filter.

Table continues...

Name	Description
Extend Expiration	Extends the duration of expiry of guest accounts or devices.
Bulk Modify	Enabled only when non Guest and IoT Manager devices are displayed in the <i>Device Search Filter</i> page. Allows the provisioner to modify the device information in bulk.

Finding guest user account

Procedure

1. Click the **Guest Users > View** button in the main toolbar of the Provisioner Application. The Guest Users screen appears, displaying the list of guest user accounts currently authorized to gain guest access and also the users who hold permanent access.
2. In the **Guest User Search Filters** section, in the **Provisioned By** field, 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 display all users, click **All Guests** and click **Apply Filter**.

4. To view the permanent access user accounts, select the required guest user name checkbox and scroll towards left. The **End Time** column status is displayed blank (-).

Modifying guest user accounts

Procedure

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

The screenshot shows the 'Reactivate Account' section of the Edit Guest User screen. It includes the following fields and options:

- Reactivate Account:** Radio buttons for 'Yes' and 'No'. The 'No' option is selected.
- Activate on First Login:** A dropdown menu set to 'No'.
- * Duration:** A text input field containing '1', followed by a dropdown menu set to 'minutes', and the text '(Max 1 minutes)'.
- Access Types:** A checked checkbox followed by the text 'mt-access-grp'.

- Click **Submit**. Guest and IoT Manager updates the guest user account and sends email notifications to the people that you specified in the **Send Notifications** section. See [Sending guest account notifications](#) on page 204 for details. Guest and IoT Manager displays the updated guest user account information in the Successful Guest Update page to confirm the account changes were saved.
- You can print the user’s account details. In the **Successful Guest Update** page, click the **Printer Friendly Version** button. In the **Guest User Account** page that appears, click the **Print** button.

Checking validity of guest user account

Procedure

- Run the Provisioner Application.
- From the Guest and IoT Manager Provisioner Application, click **Guest Users > View** from the left-hand navigation tree.

The system displays the list of the guest users provisioned.

- 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:

Access Zones	Start Time	End Time	Provisioning Group	Provisioner	Sponsor Name	Sponsor Email	Sponsor Response	Guest Details
ExtremeWired	2017/09/26 03:00:57 AM GMT+00:00	2017/09/26 11:00:57 AM GMT+00:00	GuestManagerIoT	Internal/eiot			NA	
ExtremeWired	2017/09/25 11:17:26 AM GMT+00:00	2017/09/25 11:25:26 AM GMT+00:00	GuestManagerIoT	Internal/eiot			NA	
ExtremeWired	2017/09/26 02:09:29 PM GMT+00:00	2017/09/26 03:09:29 PM GMT+00:00	GuestManagerIoT	Internal/eiot			NA	
ExtremeWired	2017/09/26 09:19:16 PM GMT+00:00	2017/09/27 05:19:16 AM GMT+00:00	GuestManagerIoT	Internal/eiot			NA	

Figure 19: Guest User account validity

No.	Description
1	Red text indicates an account start time in the future. The account becomes active at the start time.
2	Red text indicates the account is expired.

- If an account is currently not usable because its period of validity is in the future or past, you can make the account usable.
 - To make a not-yet-valid account usable now, open the user record and change the **Activate Account On** field to a time at or before the current time.
 - To renew an expired account, see [Renewing a guest user account](#) on page 210.

Viewing and Printing Provisioner Guest User account details

To view and optionally print an account summary of a Guest User account, do the following:

Before you begin

- Run the Provisioner Application.

Procedure

1. On the left-hand navigation pane of the Guest and IoT Manager Provisioner Application, click **Guest Users > View**.

The system displays the Guest User screen.

The screenshot shows the 'Guest User Search Filters' section at the top, with 'Provisioned By' set to 'eiot' and 'Guest Users' set to 'All Guests'. Below this is the 'Guest Users' table with the following data:

Last Name	Email	SMS Address	Access Types	Network Rights	Access Zones	Start Time	End Time	Provisioning Group	Provisioner
noexpire	c11@avaya.com	8008002861@txt.att.net	ExtremeNetworks, ExtremeDevices, ExtremeIOTDevices	ExtremeIntranet	ExtremeWired	2017/09/26 03:00:57 AM GMT+00:00	2017/09/26 11:00:57 AM GMT+00:00	GuestManagerIoT	Internal/eiot
expire	c11@avaya.com	8008002861@txt.att.net	ExtremeNetworks	ExtremeIntranet	ExtremeWired	2017/09/25 11:17:26 AM GMT+00:00	2017/09/25 11:25:26 AM GMT+00:00	GuestManagerIoT	Internal/eiot
time	xz@extremenetworks.com		ExtremeNetworks	ExtremeIntranet	ExtremeWired	2017/09/26 02:09:29 PM GMT+00:00	2017/09/26 03:09:29 PM GMT+00:00	GuestManagerIoT	Internal/eiot
chennakesavula	sc@extremenetworks.com		ExtremeNetworks	ExtremeIntranet	ExtremeWired	2017/09/26 09:19:16 PM GMT+00:00	2017/09/27 05:19:16 AM GMT+00:00	GuestManagerIoT	Internal/eiot

2. On the Guest Users screen, locate the row containing the Guest User whose account details you wish to view or print.
3. Click on the Guest User entry under the **Username** column.
4. Click **View**.

The system displays the selected Guest User Information page.

Guest User Info: sasikanth

User Name: sasikanth
First Name: sasikanth
Last Name: chennakesavula
Password: h9f4QvUY
Email: sc@extremenetworks.com
Cell Phone:
Comments:

Guest Details:
Activate Account On: 2017/09/26 01:19:16 PM GMT+00:00
Expire Time: 2017/09/26 09:19:16 PM GMT+00:00
Delete on Expire: Yes
Group Membership: GuestManagerIoT
Provisioner: Internal/eiot
Access: ExtremeNetworks
ExtremeWired
ExtremeIntranet
Access Types: ExtremeNetworks
Network Rights: ExtremeIntranet
Access Zones: ExtremeWired

5. (Optional) Click **Printer Friendly Version** to print the Guest User information.

*** Note:**

To customize the Printer Friendly page see, [Customizing Printer Friendly Page](#) on page 193 .

Renewing a guest user account

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

Procedure

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

5. Click **Submit**.

Deleting guest user accounts

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

Procedure

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

Guest and IoT Manager deletes the selected guest user accounts.

Extending expiry of a guest user account

Extend Expiration enables you to extend the duration of expiry of a guest user account(s) at one click. **Extend Expiration** includes the following two enhancements:

1. A new filter `Guest Users expiring in the next 'X' days` – It calculates and fetches the users according to:

$$\text{CURRENT_TIME} < \text{END_TIME} < \text{CURRENT_TIME} + X \text{ days}$$

'X' is a variable here. So, if you want to filter all Guest Users expiring tomorrow, you can select the filter `Guest Users Expiring in the next 1 days`.

 **Note:**

This filter is available to the Guest and IoT Manager administrator also.

2. A new button **Extend Expiration** in the **Provisioner > Guest User > View** page. For each selected Guest User, the duration of expiry will be calculated as:

$$\text{DURATION} = \text{END_TIME} - \text{START_TIME}$$

Then, the account will be modified to:

$$\text{START_TIME} = \text{OLD_END_TIME}$$

$$\text{END_TIME} = \text{OLD_END_TIME} + \text{DURATION}$$

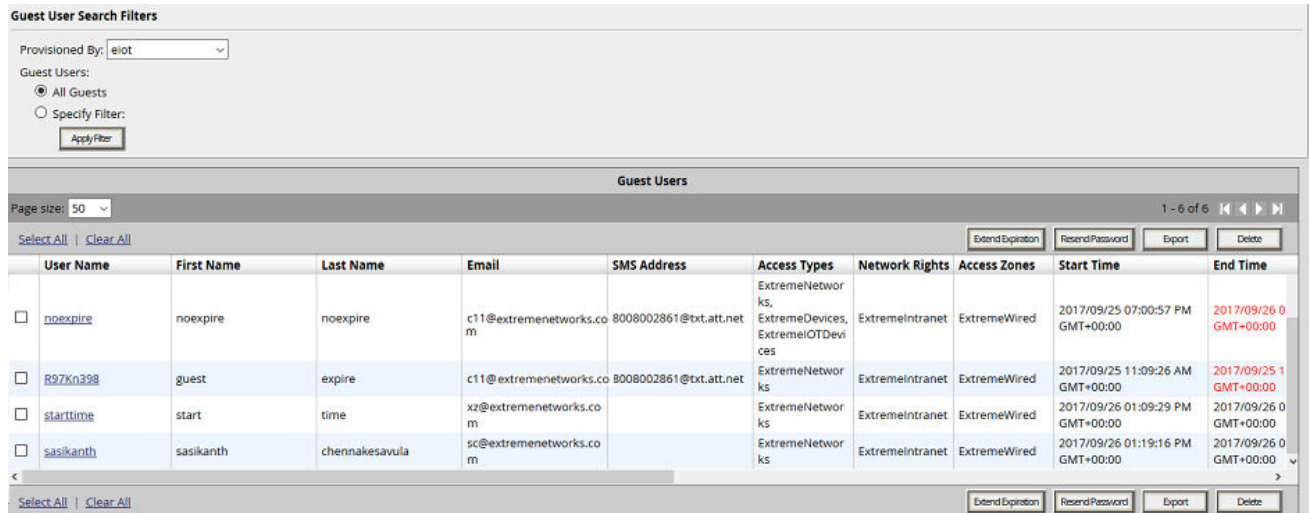


Figure 20: New filter and Extend Expiration button in Provisioner's Guest User View page

Example

Consider two guest users, User 1 valid for a duration of one month and User 2 valid for a duration of two months, both are expiring at 02:00 P.M. tomorrow. When you select these two accounts and click **Extend Expiration** button, their expiry is extended as follows:

- User 1 is extended as Start Time = 02:00 P.M. tomorrow and End Time = 02:00 P.M. tomorrow + 1 month.
- User 2 is extended as Start Time = 02:00 P.M. tomorrow and End Time = 02:00 P.M. tomorrow + 2 months.

* Note:

- Provisioners can use Extend Expiration to extend the duration of expiry for expired Guest User account(s) also.
- Expiry of First Login Pending Guest Accounts cannot be extended.

Resending Password to Guest User(s)

Resend password enables you to resend the password to Guest User(s). When one or more users are selected and the **Resend Password** button is clicked, then the following checks are performed depending on which the password is sent via Email or SMS or both:

1. Notification options has either SMS / Email or both enabled
2. The account is not locked / expired
3. The Email / SMS Template contains \$password

Guest Users										
User Name	First Name	Last Name	Email	SMS Address	Access Types	Network Rights	Access Zones	Start Time	End Time	
<input type="checkbox"/> noexpire	noexpire	noexpire	c11@extremenetworks.com	8008002861@txt.att.net	ExtremeNetworks, ExtremeDevices, ExtremeIoTDevices	ExtremeIntranet	ExtremeWired	2017/09/25 07:00:57 PM GMT+00:00	2017/09/26 0 GMT+00:00	
<input type="checkbox"/> R97Kn398	guest	expire	c11@extremenetworks.com	3008002861@txt.att.net	ExtremeNetworks	ExtremeIntranet	ExtremeWired	2017/09/25 11:09:26 AM GMT+00:00	2017/09/25 11:09:26 AM GMT+00:00	
<input type="checkbox"/> starttime	start	time	xz@extremenetworks.com		ExtremeNetworks	ExtremeIntranet	ExtremeWired	2017/09/26 01:09:29 PM GMT+00:00	2017/09/26 0 GMT+00:00	
<input type="checkbox"/> sasikanth	sasikanth	chennakesavula	sc@extremenetworks.com		ExtremeNetworks	ExtremeIntranet	ExtremeWired	2017/09/26 01:19:16 PM GMT+00:00	2017/09/26 0 GMT+00:00	

Managing devices

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

Creating a device record

Ignition Server can enforce rules that allow a guest to connect only using his or her own device.

For more information, see [Device example](#) on page 20.

To create multiple devices at once, click **Devices > Load**.

Procedure

1. Log in to the Provisioner Application.
2. Click the **Devices > New**.

The system displays the Create device window with default **Common** tab.

The screenshot shows the 'Common' tab of a configuration interface. It contains several sections:

- Associated Provisioning Group:** A dropdown menu with 'Guest_Standard' selected.
- Device Info:**
 - * MAC Address:** An empty text input field.
 - Name:** An empty text input field.
 - Type:** A dropdown menu with '----- Select One -----' selected.
 - Sub Type:** A dropdown menu.
 - Source:** A text input field containing 'GM-Guest_Standard'.
 - Comments:** An empty text input field.
 - Record Enabled:** Radio buttons for 'Yes' (selected) and 'No'.
 - Asset Type:** Radio buttons for 'Permanent' and 'Temporary' (selected).
 - Delete on Expire:** Radio buttons for 'Yes' (selected) and 'No'.
 - * Activate Account On:** Three input fields: '2015/12/07', '08:42:14', and 'AM', followed by 'GMT+00:00'.
 - * Duration:** An input field with '8', a dropdown with 'hours', and '(Max 8 hours)'.
- Associated Users:** A list area with 'Add...' and 'Remove' links and an empty list box.

Figure 21: Create Device as Provisioner

3. On the **Common** tab in the **MAC Address** field, specify the MAC address of the device.
Format of MAC address: xx:xx:xx:xx:xx:xx.
For example: 10:00:01:02:21:10.
4. In the **Name** field, type a name for the device. This name identifies the device in logs and when you associate it with a group or user.
5. Select the device **Type** of the device from the drop-down list.
On selecting the Device **Type** the Device **Sub Type** drop-down is loaded.
6. Select the appropriate device **Sub Type** from the drop-down list.
The Device Type and Sub Type are fetched from the Ignition Dashboard Device Types.
7. The **Record Enabled** is selected **Yes** by default.
Selecting **Record Enabled** to **No** discards the device from connecting to the network.
8. To select **Asset Type**, do one of the following:
 - To create a permanent record for the device, click **Permanent**.

- To create a temporary record for the device, click **Temporary** and **specify the Activate Account On** date and time and the **Duration** of the validity. If the **Activate on First Login** is assigned, then the **Activate Account On** is replaced by **Activate on First Login: Yes**. If the device record should be deleted when it expires, select the **Delete on Expire to Yes**.
9. Specify where and how the device can be used by clicking the appropriate **Access Type**, **Network Rights**, and **Access Zone** check boxes.
 10. To assign the device to a user, click **Add** in the **Associated Users** section.
 11. Click **Submit**.

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

MAC Address	Name	Type	Sub Type	Access Types	Network Right	Access Zones	Source	Enabled	Asset Type	Start Time	End Time
aa:bb:cc:dd:ee:10	LSS_Extreme	fax machine	n/a	ExtremeNetworks, ExtremeDevices	ExtremeIntranet	ExtremeWired	GM-GuestManager IoT	Yes	Permanent	2017/09/20 10:39:20 AM GMT+00:00	-
10:10:10:10:10:10		FA client	ONA-SDN	ExtremeNetworks, ExtremeDevices, ExtremeIoTDevices, AvayaDevices, AvayaIoTDevice	TreeRights	ExtremeWired, ExtremeWireless, TreeZone	GM-GuestManager IoT	Yes	Permanent	2017/09/26 04:45:58 AM GMT+00:00	-

If the **Asset Type** is selected as **Permanent**, the End Time column displays “-”.

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:

If Network Access Group assignment is from GUI:

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

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

If Network Access Group is from CSV:

```
MAC Address,Name,Type, Sub-Type, Attribute 1,Attribute 2,
Attribute 3,Attribute 4,Attribute 5,Comments,
VLAN Label,VLAN ID,Account Disabled, "Access Type 1, Access Type2", Network
Rights, "Access Zone 1, Access Zone 2"
```

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

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. Fields containing multiple values should be enclosed within double quotes.

 **Important:**

Observe the following guidelines when bulk loading:

- The maximum number of device records you can import from a file is 1000.
- Extreme Networks 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 and IoT Manager application running, open a web browser and navigate to the Provisioner Application URL.
- Type your provisioners `Username` and `Password`.

3. In the toolbar on the left, click **Devices** > **Load**. The system displays *Load Devices* screen.

4. In the **Group Membership** drop-down list, select the provisioning group.

5. To the right of the **Load Devices From File** field, click the **Browse / Choose File** option and browse to find the CSV file in your local drive. Click **Open** to select it.

6. In the **Source** field, enter a name as a reminder of the information source you used for this particular bulk import.

7. **Optional:** Select **Override Duplicate Records** check box to override existing MAC entries in the system. By default, it is enabled.

 **Note:**

If you clear **Override Duplicate Records** check box and import the device records, the system displays unsuccessful Device MAC entries along with “Duplicate Record” message for duplicate MAC entries in the *Device Uploading Results* screen.

8. Specify whether the Asset Type will be temporary or permanent. Do one of the following:

- To create permanent records for the devices, click **Permanent**.
- To create temporary records for the devices, click **Temporary** and specify the **Activate Account On** date and the **Duration** of validity. If the Guest has been assigned to **Activate on First Login**, the Activate Account is replaced with a Yes for the first login. If the device record should be deleted when it expires, select **Yes** for the **Delete on Expire** field.

9. If the Provisioner has access to modify Network Access Rights of a device, then the Provisioner can either import the groups from the GUI or from the CSV. In the **Group**

Assignment (Input from) field, to Import the Groups from GUI / CSV, do one of the following:

- Select **CSV** to import Network Access Rights (Types, Zones, Rights) from the CSV File. All the check boxes pertaining to Network Access rights are greyed out on the GUI.

Load Devices Screen — CSV

Load Devices

Associated Provisioning Group:

* **Group Membership:**

Device Info:

* **Load Devices From File:** No file chosen

Source:

Override Duplicate Records

Asset Type: Permanent Temporary

Delete on Expire: Yes No

Activate on First Login: Yes

* **Activate Account On:** GMT+00:00

* **Duration:** (Max 8 hours)

Group Assignment (Input from): CSV GUI

Access Types: Network_Access_1 Network_Access_5

Network Rights: network_Access_4

Access Zones: Network_Access_6

Note: Any row in the CSV file that begins with character "#" will be ignored for processing
Expected CSV file format with field order as below:
MAC Address,Name,Type,Sub Type,Custom 1,Custom 2,Custom 3,Custom 4,Custom 5,Comments,VLAN Label,VLAN ID,Account Disabled*,"Access Type 1, Access Type 2",Network Right,"Access Zone 1, Access Zone 2"
* Account Disabled is either 'yes' or 'no'. Default is enabled.
** Required*

If Access Types and Access Zones have multiple values, it has to be indicated in double quotes in the CSV. Network Rights can take only one value.

Network Access Rights (Types, Zones, Rights) must contain values that belongs to the Provisioning group selected from the drop-down list. While Access Types and Access Zones can take multiple values that needs to be indicated in double quotes, Network rights can take only one value.

If the device record does not contain any value / more than one value for Network Rights or the values mentioned for Access Types and Access Zones does not belong to the selected Provisioning Group, then the system displays unsuccessful device information along with details in the *Device Uploading Results* screen.

If **Asset Type** is **Permanent**, then **Expire Time: NA** is displayed in *Device Uploading Results* screen.

- Select **GUI**, to select Network Access Rights (Types, Zones and Rights) by enabling the check boxes provided on the GUI. By default, GUI is selected.

Load Devices Screen — GUI

Load Devices

Associated Provisioning Group: _____

*** Group Membership:** ▾

Device Info: _____

*** Load Devices From File:** No file selected.

Source:

Override Duplicate Records

Asset Type: Permanent Temporary

Activate on First Login: Yes

Group Assignment (Input from): CSV GUI

Access Types: ExtremeNetworks ExtremeDevices ExtremeIoTDevices
 TreeIoTDevices Extreme_IoT_Manage_Devices
 Extreme_Networks_IoT_Devices_Group

Network Rights: ExtremeIntranet ExtremeInternet TreeRights

Access Zones: ExtremeWired ExtremeWireless TreeZone

Note: Any row in the CSV file that begins with character "#" will be ignored for processing
 Expected CSV file format with field order as below:
 MAC Address,Name,Type,Sub Type,Custom 1,Custom 2,Custom 3,Custom 4,Custom 5,Comments,VLAN Label,VLAN ID,Account Disabled*
 * Account Disabled is either 'yes' or 'no'. Default is enabled.
* Required

*** Note:**

If the Provisioning group has static group enabled, then the Access Type or Zone corresponding to the static group is selected by default and grayed out in case of Group Assignment from GUI View.

If the Provisioning group has a static group enabled, then the static group is added to all the imported devices.

10. Click **Submit**. Guest and IoT Manager displays a progress bar while it imports the records. Under some conditions, bulk loading may take several minutes.

Once the devices have been created, you may view them by clicking **Devices > View** in the main toolbar on the left of the window. To see a record of the success or failure of each record creation attempt, check your Guest and IoT Manager logs as explained in [Viewing the log files](#) on page 90.

Assigning a device to a guest user

Ignition Server can enforce rules that allow a guest to connect only using his or her own device. See [Device example](#) on page 20.

Procedure

1. Click the **Guest Users > View** button in the main toolbar of the Provisioner Application. The Guest Users screen appears, displaying the list of guest user accounts currently authorized to gain guest access.
2. Locate the row containing the guest user whose account you wish to modify, and click on the entry in the **User Name** column. The Edit Guest User screen appears.
3. In the Associated Devices section of the window, click **Add**. A list of devices appears.
4. Locate the user's laptop or device record in the list. If it is not there, see [Creating a device record](#) on page 213. Click the check box of the desired device and click **Add Devices to User**.
5. In the Edit Guest User screen, click **Submit**.

Viewing a device record summary

About this task

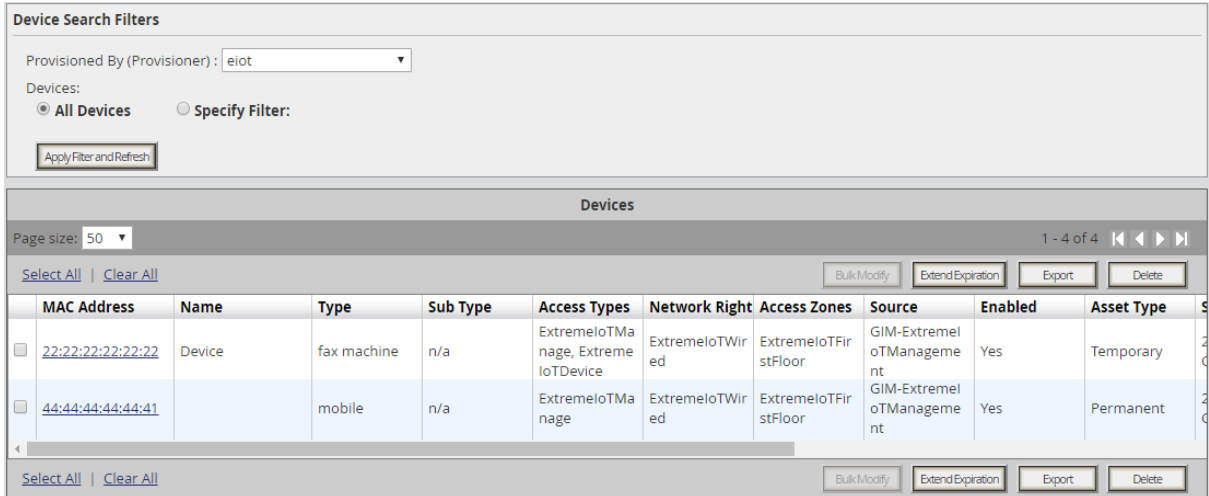
Use the following procedure to view the record summary of Guest and IoT Manager and NonGuest and IoT Manager.

Before you begin

- Log in to the Provisioner Application.

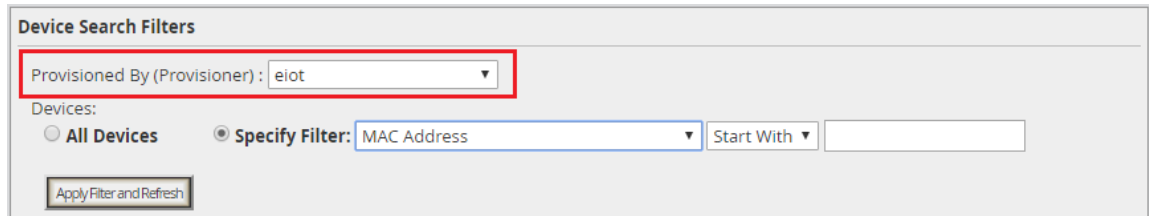
Procedure

1. From the Guest and IoT Manager Provisioners Application, click **Devices > View**.
The system displays the *Device Search Filters* screen.



By default, all the devices created by the Provisioner are displayed in the frame.

2. To view Guest and IoT Manager devices, do the following:
 - a. In the **Provisioned By (Provisioner)** field, select the Guest and IoT Manager Provisioning device from the drop-down list.



- b. Click **All Devices** to view all the devices provisioned in the system. By default, this option is selected.
- c. **Optional:** Select **Specify Filter** option to select specific device attributes from the drop-down list. For example, you can provide explicit operations such as Start with, Equal, Not Equal, Contains, Ends With and the name of the search value.
- d. Click **ApplyFilterandRefresh** to view the selected device records displayed in the frame.
- e. On the *Device* screen frame, locate the row containing the device record whose details you wish to view.
- f. Click on the device entry under the **MAC Address** column

The system displays the *Device Info* screen along with the selected device record details.

Device Info: 22:22:22:22:22:22

MAC Address: 22:22:22:22:22:22

Name: Device

Type: fax machine

Sub Type: n/a

Source: GIM-ExtremeloTManagement

Comments:

Record Enabled: Yes

Asset Type: Temporary

Activate Account On: 2017/10/24 05:45:25 AM GMT+00:00

Expire Time: 2017/10/24 01:45:25 PM GMT+00:00

Delete on Expire: Yes

Group Membership: ExtremeloTManagement

Provisioner: Internal/eiot

Access Types: ExtremeloTManage
ExtremeloTDevice

Network Rights: ExtremeloTWired

Access Zones: ExtremeloTFirstFloor

Guest Users:

- g. Click on the device entry under the **MAC Address** column.
 - h. In the **Device Info** page, click **EditDevice** to edit device information if required.
3. To view the Non Guest and IoT Manager devices, do the following:
- a. In the **Provisioned By (Provisioner)** field, select the Provisioning group that has view / edit Non Guest and IoT Manager devices from the drop-down list.

The field changes from **Provisioned By (Provisioner)** to **Provisioned By (Provisioner Group)**.

Device Search Filters

Provisioned By (Provisioning Group): ExtremeloTManagement OR All Devices of * ExtremeloTManage

Devices:

All Devices Specify Filter: MAC Address Start With

If the selected Provisioning group has static enabled, then the **All Devices of** field is enabled. If the selected Provisioning group does not have a static group enabled, then the **All Devices of** field is disabled.

- b. If the Provisioning group contains a static group, select the **All Devices of** check box and select the required access from the drop-down to have another level of filter for the selected parent group. This is optional.
- c. If the Provisioning group does not contain a static group, select the **All Devices of** check box and select the required access from the drop-down. This is mandatory.
- d. Click **All Devices** to view all the devices provisioned in the system. By default, this option is selected.
- e. **Optional:** Select **Specify Filter** option to select specific device attributes from the drop-down list. For example, you can provide explicit operations such as Start with, Equal, Not Equal, Contains, Ends With and the name of the search value.
- f. Click **ApplyFilterandRefresh** to view the list of Non Guest and IoT Manager devices in the frame.
- g. Click on the device entry under the **MAC Address** column.

The system displays the *Device Info* screen along with the selected device record details. The Non Guest and IoT Manager can only be edited using Bulk Modify option. For more information, see [Bulk modifying the Non Guest and IoT Manager devices](#) on page 222.

Bulk modifying the Non Guest and IoT Manager devices

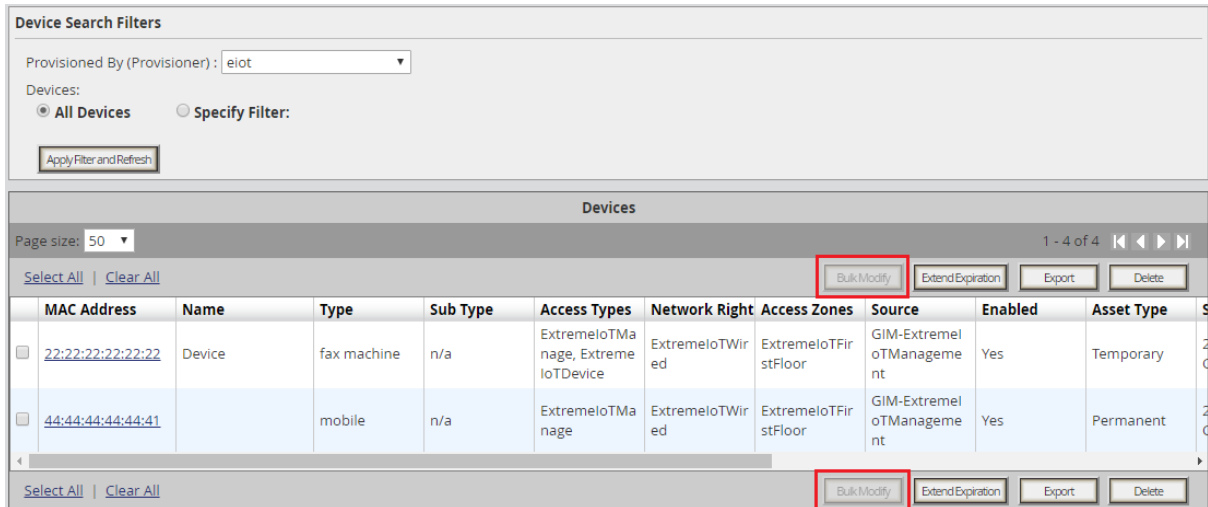
About this task

Use the following procedure to manage the Non Guest and IoT Manager devices for a provisioning group that has “**All Non GIM Devices**” enabled.

Procedure

1. Log in to the Provisioner Application. For more information, see [Launching the provisioner application](#) on page 200 .
2. Click **Devices** > **View** in the toolbar on the main page of the Provisioner Application.

The system displays *Device Search Filters* screen.



By default, the **Bulk Modify** option is disabled and devices that belong to the particular Provisioner is displayed in the frame. The **Access Types**, **Network Rights**, and **Access Zones** columns in the frame display all the access rights assigned for the devices separated with commas.

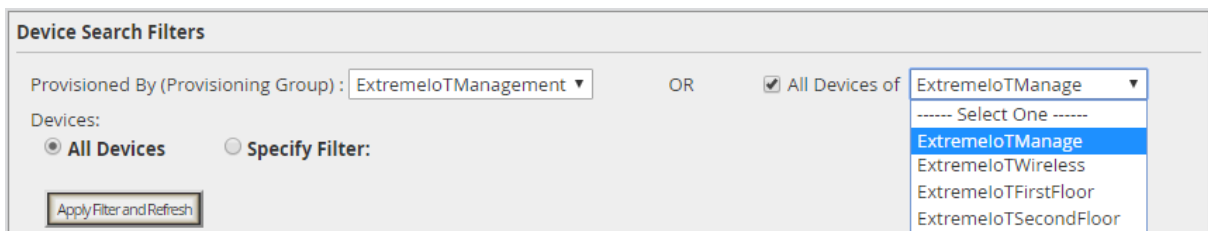
- In the **Provisioned By (Provisioner)** field, select the Provisioning group that has access to view / edit Non Guest and IoT Manager devices.

If the selected Provisioning group has static enabled, then the **All Devices of** field is enabled with the list of selected User Groups. If the selected Provisioning group does not have a static group enabled, then the **All Devices of** field is disabled.

*** Note:**

If the Administrator has not selected a Static Group while configuring the device record details, then the provisioner must select a Network Access Rights from the drop-down to view Non Guest and IoT Manager devices. The Access Rights displayed in the drop down depend on the Access Rights set by the Administrator while creating the Provisioning group. It is mandatory to select one group and there is no option to select multiple groups.

Non Guest and IoT Manager Device — Without Static Group Selection Screen

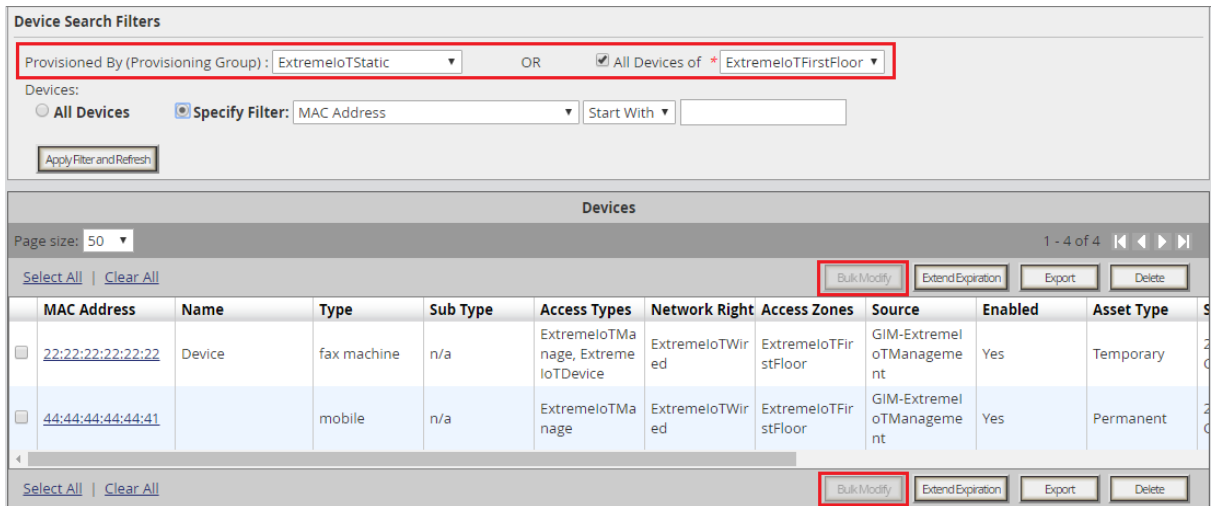


*** Note:**

If the Administrator has selected a Static Group while configuring the device record details, then the system displays the selected User Groups in the **All Devices of** field.

Now the provisioner is forced to view only devices that are part of the selected displayed group.

Non Guest and IoT Manager Device — Static Group Selected Screen



4. Select the **All Devices** of check box and select the required access group from the drop-down to have another level of filter for the selected parent group.
5. **Optional:** Select **Specify Filter** to select specific device attributes from the drop-down list. For example, you can provide explicit operations such as Start with, Equal, Not Equal, Contains, Ends With and the name of the search value.
6. Click **ApplyFilterandRefresh**. A list of Non Guest and IoT Manager devices are displayed. The **Bulk Modify** option is enabled and the **Extended Expiration** option is hidden. Extended Expiration functionality will be available in the *Bulk Modify* screen.
7. Select all / required Non Guest and IoT Manager devices and click **Bulk Modify** to edit the attributes.

The system displays *Bulk Modify* screen.

- a. Modify the details as tabulated:

Attribute	Description
Name	Name of the device.

Table continues...

	<p>Choose Attribute to Modify:</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> Name: <input type="radio"/> Type/Sub Type <input type="radio"/> Records Enable <input type="radio"/> Network Access Rights <input type="radio"/> Extend Expiration <p>Name: <input type="text"/></p> <p style="text-align: right;"><input type="button" value="Submit"/> <input type="button" value="Close"/></p>
<p>Type / Subtype</p>	<p>Select the Type and Subtype from the drop down for the selected Provisioning Group.</p> <p>Choose Attribute to Modify:</p> <ul style="list-style-type: none"> <input type="radio"/> Name: <input checked="" type="radio"/> Type/Sub Type <input type="radio"/> Records Enable <input type="radio"/> Network Access Rights <input type="radio"/> Extend Expiration <p>Type: <input type="text" value="----- Select One -----"/></p> <p>Sub Type: <input type="text"/></p> <p style="text-align: right;"><input type="button" value="Submit"/> <input type="button" value="Close"/></p>
<p>Records Enable</p>	<p>Select Yes OR No.</p> <p>Choose Attribute to Modify:</p> <ul style="list-style-type: none"> <input type="radio"/> Name: <input type="radio"/> Type/Sub Type <input checked="" type="radio"/> Records Enable <input type="radio"/> Network Access Rights <input type="radio"/> Extend Expiration <p>Records Enable <input checked="" type="radio"/> Yes <input type="radio"/> No</p> <p style="text-align: right;"><input type="button" value="Submit"/> <input type="button" value="Close"/></p>
<p>Network Access Rights</p>	<p>Modify Access Types, Network Rights, and Access Zones.</p> <p>* Note:</p> <p>If the Admin has specified a Static Group, then that particular Access Type / Access Zone pertaining to the static group is selected by default (greyed out) and the provisioner does not have access to remove or modify the device from that group.</p>

Table continues...

	<p>Choose Attribute to Modify:</p> <p><input type="radio"/> Name:</p> <p><input type="radio"/> Type/Sub Type</p> <p><input type="radio"/> Records Enable</p> <p><input checked="" type="radio"/> Network Access Rights</p> <p><input type="radio"/> Extend Expiration</p> <p>Access Types: <input checked="" type="checkbox"/> ExtremeNetworks <input checked="" type="checkbox"/> ExtremeDevices</p> <p><input checked="" type="checkbox"/> ExtremeIoTDevices</p> <p>Network Rights: <input checked="" type="radio"/> ExtremeIntranet</p> <p>Access Zones: <input checked="" type="checkbox"/> ExtremeWired</p> <p style="text-align: right;"> <input type="button" value="Submit"/> <input type="button" value="Close"/> </p>
Extend Expiration	<p>Extends the duration of expiry. The device start time is extended and displayed in <i>Device Search Filter</i> screen in Start Time column in RED color.</p>

- b. Click **Submit** to save the device modification details or click **Close** to close the *Bulk Modify* screen.

*** Note:**

You can now confirm the modified device information in the Dashboard. For more information, see "Finding an internal device" section in *Identity Engines Ignition Server Configuration, NN47280-600*. You can also modify the Non Guest and IoT Manager devices in Dashboard, Internal Stores and the same is reflected back in Guest and IoT Manager devices.

8. To export Non Guest and IoT Manager devices, select all and click **Export** to export the device information to a CSV file.
9. Select the required device and click **Delete** to delete the selected device in Ignition Server.

+ Tip:

If the Administrator has not selected the Static Group while configuring the device record details, you can follow the same procedure listed above to manage Non Guest and IoT Manager devices. In this case, the system forces you to select one group from the **All Device of** drop-down and then **ApplyFilterandRefresh** to modify the given attributes.

Extending expiry of a device

Extend Expiration extends the duration of expiry of device(s) by "X" days at one click . **Extend Expiration** includes the following two enhancements:

1. A new filter `Devices expiring in the next 'X' days` – It calculates and fetches the devices according to:

$$\text{CURRENT_TIME} < \text{END_TIME} < \text{CURRENT_TIME} + X \text{ days}$$

'X' is a variable here. So, if you want to filter all Devices expiring tomorrow, you can select the filter `Devices Expiring in the next 1 days`.

*** Note:**

This filter is available to the Guest and IoT Manager administrator also.

2. A new button **Extend Expiration** in the **Provisioner > Devices > View** page. For each selected Device, the duration of expiry will be calculated as:

$$\text{DURATION} = \text{END_TIME} - \text{START_TIME}$$

Then, the account will be modified to:

$$\text{START_TIME} = \text{OLD_END_TIME}$$

$$\text{END_TIME} = \text{OLD_END_TIME} + \text{DURATION}$$

*** Note:**

Extend Expiration is available to the Guest and IoT Manager Administrator also.

The screenshot shows a web interface titled "Devices" with a table of device information. The table has columns for MAC Address, Name, Type, Sub Type, Access Types, Network Right, Access Zones, Source, Enabled, and Asset Type. A single device is listed with MAC Address 10:10:10:10:10:10, Type FA client, Sub Type ONA-SDN, Access Types ExtremeNetworks, ExtremeDevices, ExtremeIoTDevices, Network Right TreeRights, Access Zones ExtremeWired, ExtremeWireless, TreeZone, Source GM-GuestManager IoT, Enabled Yes, and Asset Type Permanent. Above the table are buttons for Bulk Modify, Extend Expiration, Export, and Delete. Below the table are buttons for Select All, Clear All, Bulk Modify, Extend Expiration, Export, and Delete. The page size is set to 50 and it shows 1 - 2 of 2 items.

MAC Address	Name	Type	Sub Type	Access Types	Network Right	Access Zones	Source	Enabled	Asset Type
<input type="checkbox"/> 10:10:10:10:10:10		FA client	ONA-SDN	ExtremeNetworks, ExtremeDevices, ExtremeIoTDevices	TreeRights	ExtremeWired, ExtremeWireless, TreeZone	GM-GuestManager IoT	Yes	Permanent

Figure 22: New filter and Extend Expiration button in Provisioner's Device View page

Example

Consider two devices, Device 1 valid for a duration of one month and Device 2 valid for a duration of two months, both are expiring at 02:00 P.M. tomorrow. When you select these two devices and click **Extend Expiration** button, their expiry is extended as follows:

- Device 1 is extended as Start Time = 02:00 P.M. tomorrow and End Time = 02:00 P.M. tomorrow + 1 month.
- Device 2 is extended as Start Time = 02:00 P.M. tomorrow and End Time = 02:00 P.M. tomorrow + 2 months.

*** Note:**

- Provisioners can extend the duration of expiry for expired device(s) also.
- Expiry of First Login Pending devices cannot be extended.

- Expiry of permanent devices cannot be extended.

Managing Sponsored Guests

Guest and IoT Manager allows a Sponsor to manage guest accounts that require Sponsor's attention. A sponsor can either be an internal store Provisioner or a Provisioner belonging to a Sponsor AD group.

About this task

Use this procedure to view all sponsored guest users and allow actions such as extend expiration, send email, bulk approve, bulk deny/lock.

Procedure

1. Log in to the Provisioner application.
2. Navigate to **Sponsor > View**.

The system displays the Guest Users list window :

The screenshot shows the 'Guest Users' interface. At the top, there are 'Guest User Search Filters' with options for 'All Guests' (selected) and 'Specify Filter'. Below this is a table with columns: User Name, First Name, Last Name, Sponsor Response, Email, SMS Address, and Start Time. A single row is visible with the following data: Name, sample, approve, Approved, c11@extreme.com, 8008002861@in.airtel.com, 2017/09/22 11:48:30 AM GMT+00:00. The interface includes 'Page size: 50', '1 - 1 of 1', and buttons for 'Approve', 'DenyLock', 'Extend Expiration', and 'Send Email'.

User Name	First Name:	Last Name:	Sponsor Response	Email	SMS Address	Start Time
Name	sample	approve	Approved	c11@extreme.com	8008002861@in.airtel.com	2017/09/22 11:48:30 AM GMT+00:00

Fetches all the list of guests for which the Provisioner is a Sponsor. Displays nothing if no requests to particular Sponsor.

* Note:

The view functionality is available only if the following conditions are met:

- If a valid email is present for the Sponsor.
- AD sponsor username should be mentioned along with the complete domain. Though GM - AD authentication is not case sensitive, the sponsor view functionality is case sensitive. For e.g. If the Provisioner username in AD is Holle and the domain is

test.local, then the sponsor managing guest users view will work only if the Provisioner logs in as Holle@test.local.

3. User can perform the below actions:

Action Name	Description
Bulk Approve	Allow selection of multiple guest users and approve their requests.
Bulk Deny/Lock	Allow selection of multiple guest users and deny their requests.
Bulk Extend Expiration	Allow extend expiration of multiple guest user accounts.
Send Email	Allow to send email with text to Guest Users.

Bulk Approve: Sponsor can select multiple Guest User accounts and Click **Approve** button to approve the access to the selected Guest accounts. Sponsor can also optionally include a message that needs to be sent as part of the approval Email.



Message to Guest(s):

Approve Close

Bulk Deny/Lock: Sponsor can select multiple Guest User accounts and Click **Deny/Lock** button to Deny/lock the access to the selected Guest accounts. Sponsor can also optionally include a message that needs to be sent as part of the denial Email.



Message to Guest(s):

Deny/Lock Close

Bulk Extend Expiration: Extend Expiration enables you to extend the duration of expiry of a guest user account(s) at one click. **Extend Expiration** includes the following two enhancements:

- a. A new filter `Guest Users expiring in the next 'X' days` – It calculates and fetches the users according to:

$$\text{CURRENT_TIME} < \text{END_TIME} < \text{CURRENT_TIME} + X \text{ days}$$

'X' is a variable here. So, if you want to filter all Guest Users expiring tomorrow, you can select the filter `Guest Users Expiring in the next 1 days`.

*** Note:**

This filter is available to the Guest and IoT Manager administrator also.

- b. A new button **Extend Expiration** in the **Provisioner > Guest User > View** page. For each selected Guest User, the duration of expiry will be calculated as:

$$\text{DURATION} = \text{END_TIME} - \text{START_TIME}$$

Then, the account will be modified to:

$$\text{START_TIME} = \text{OLD_END_TIME}$$

$$\text{END_TIME} = \text{OLD_END_TIME} + \text{DURATION}$$

Send Email : Sponsor can select multiple Guest User accounts and Click **Send Email** button to send mails to the selected Guest users.



Message to Guest(s):

Send Email

Close

Chapter 11: Identity Engines Ignition Device Registration Android App

Identity Engines (IDE) introduces an Android Smartphone Application which simplifies the device registration for the provisioner.

Guest and IoT Manager defines the minimum configuration fields to Android App that are required to register a guest device with a specified provisioner group.

Installing Identity Engines IDR Android App

Use the following procedure to install the Identity Engines IDR Android App in your smartphone.

Procedure

1. In your android smartphone, click **Play Store**.

The **Google Play Store** launches.

2. In the search text box, enter the application name and click **Search** button.

The search result is displayed. Select the Identity Engines IDR Android App icon to open the install page.

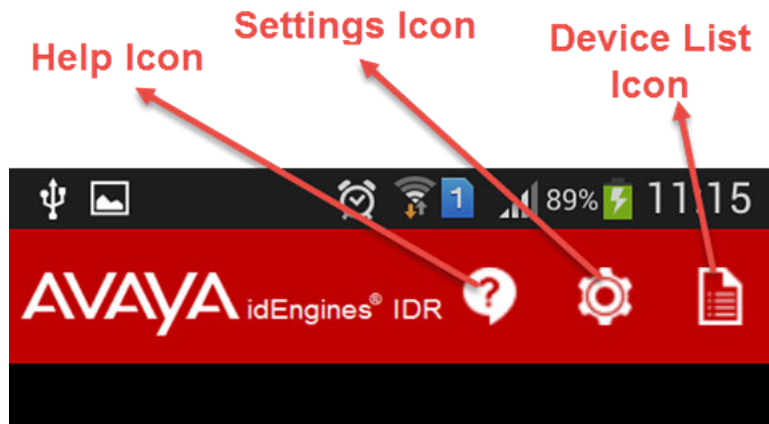
3. Click **Install**.

The application get installed to android smartphone and App shortcut icon appears on home screen and App list screen.

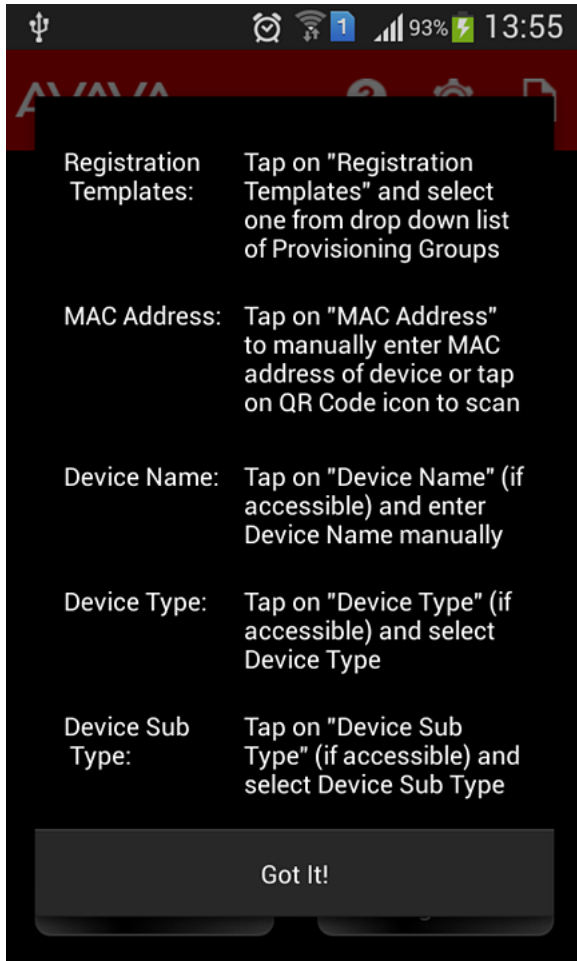


Identity Engines IDR App Icons

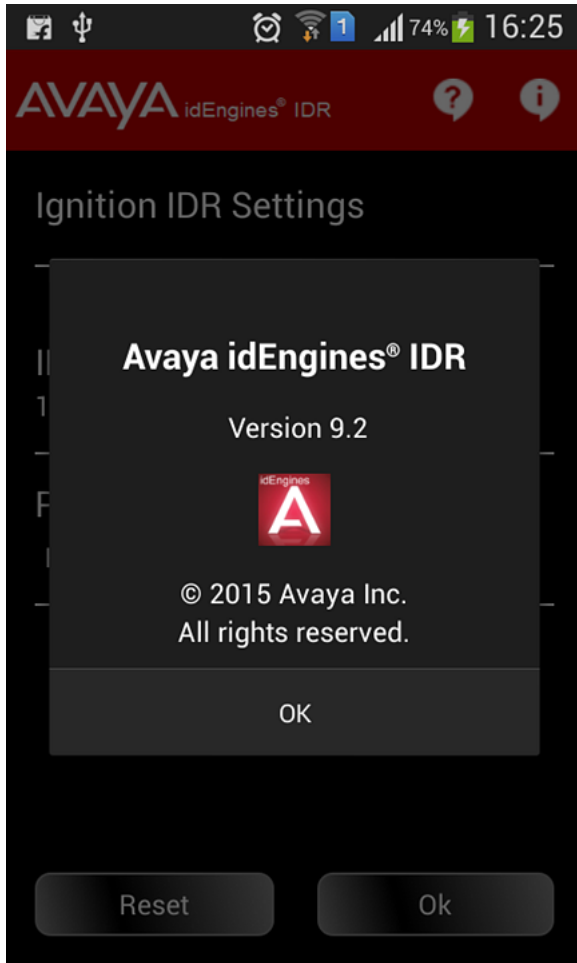
Following are the icons that are used in Identity Engines IDR App.



- **Help Icon** - Displays appropriate help messages for the current page.
For example, the field description is displayed as help message in Device Registration page.



- **Settings Icon** - Settings icon is used to change the **IP/HostName** and **Protocol**.
- **Device List Icon** - Displays the device list that are added using IDR app.
- **About IDR App Icon** - Displays details about the application. The About App icon are found in the settings page.

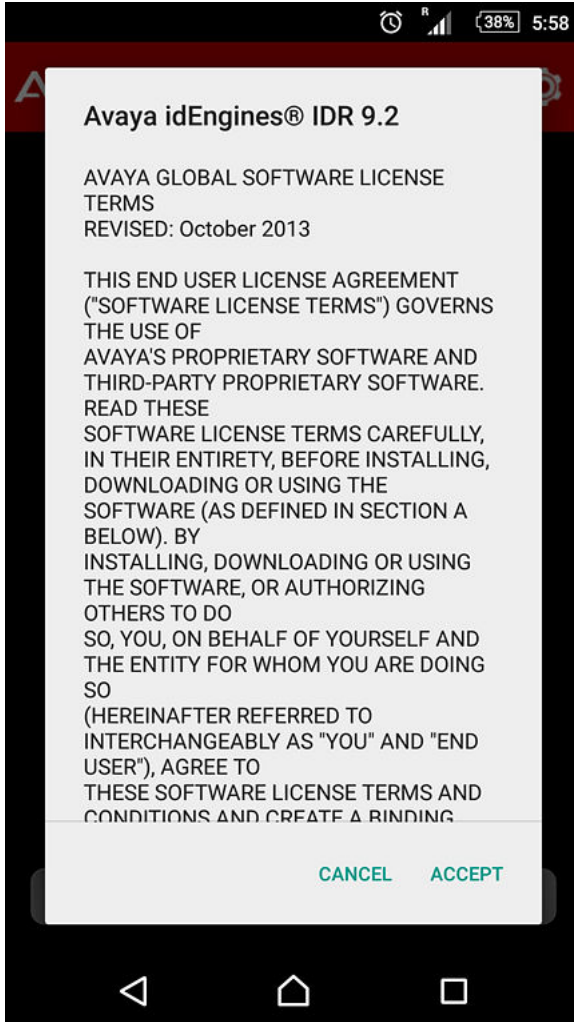


Launching Identity Engines IDR Android App

Use the following procedure to launch the Identity Engines IDR Android App.

Procedure

1. Click **Identity Engines IDR Android App** icon.
The End User License Agreement appears.



2. Click **ACCEPT**.

Clicking on **CANCEL** closes the app. The End User License Agreement appears the next time you launch the app.

*** Note:**

The End User License Agreement must be accepted to access the app.

The application help messages appears, you can skip the help by clicking **Skip** or click **Next** to read the help messages till you get the last message.

Note that the help message appears only the first time you launch the app.

3. Click **Done** to close the help message box.

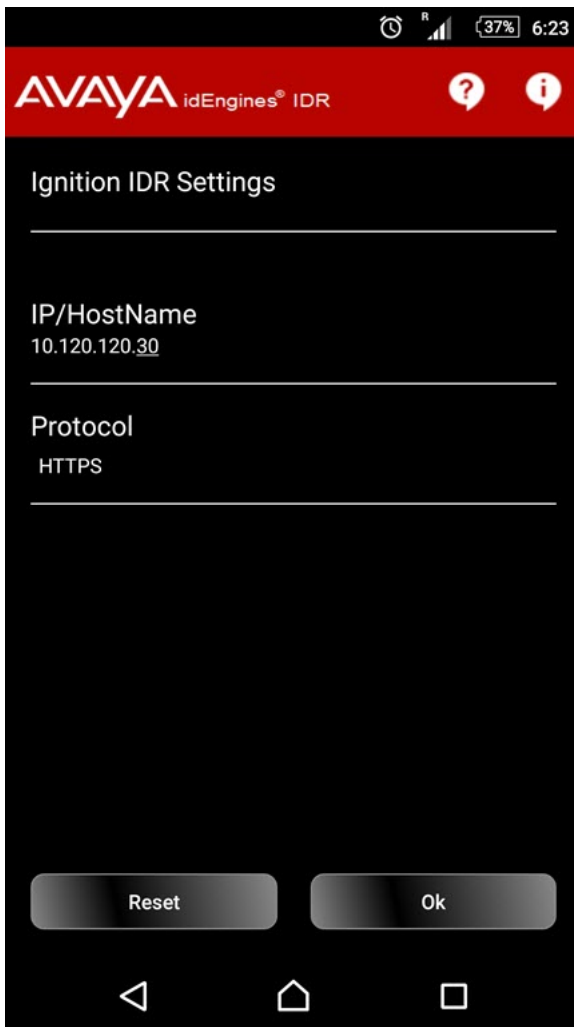
The login page appears.

4. Enter provisioner **Username** and **Password** and click **Login**.

App will try to connect to default Guest and IoT Manager (default hostname is Identity Engines-IGM). If App cannot connect to default Hostname, it displays appropriate error message.

You can also configure the default hostname (Identity Engines-IGM) as your hostname. For more information, see [Configuring hostname as Extreme-IGM](#) on page 236.

5. In the top-right, click on the settings icon to change the **IP/HostName** and **Protocol** and click **OK**.



Configuring hostname as Extreme-IGM

Use the following procedure to configure the default hostname Extreme-IGM as your hostname.

Procedure

1. In DNS server, configure domain and hostname (Extreme-IGM).
2. Map Extreme-IGM with Guest and IoT Manager Server IP address.
3. Configure Dynamic Host Configuration Protocol (DHCP) server with scope options, Domain Name System (DNS) servers (option 6) and DNS domain name (option 15).
4. In Extreme Identity Engines IDR Android App, enter hostname as Extreme-IGM or enter Fully Qualified Domain Name (FQDN) as Extreme-IGM.domain and connect mobile to network.

 **Note:**

Make sure that the Guest and IoT Manager server and android mobile app are on the same network.

5. The hostname or FQDN is resolved when mobile receives the IP address from DHCP server.

Registering a Device using Identity Engines IDR Android App

Use the following procedure to register a device using Identity Engines IDR Android App.

Before you begin

The Media Access Control (MAC) address is a unique identifier used to register a device. The MAC address is mandatory and the remaining fields visibility is decided when creating a provisioner group to use IDR Android App.

Procedure

1. After Login, the device registration page appears.
2. Enter the following fields to add a device:
 - a. Tap **Registration Templates** and select **Provisioning Group** from the drop-down.

For more information about creating a provisioning group, see [Creating a provisioning group](#) on page 132.

- b. Tap **MAC Address** to manually enter the MAC address of device or click Quick Response (QR) Code icon to scan the device MAC address.

QR code is the trademark for the two dimensional type barcode. The Android App scans QR codes and parses MAC address of the guest device that is being registered with Guest and IoT Manager. This makes the provisioner's MAC address configuration easy and to avoid any error due to manual configuration of guest device's MAC address.

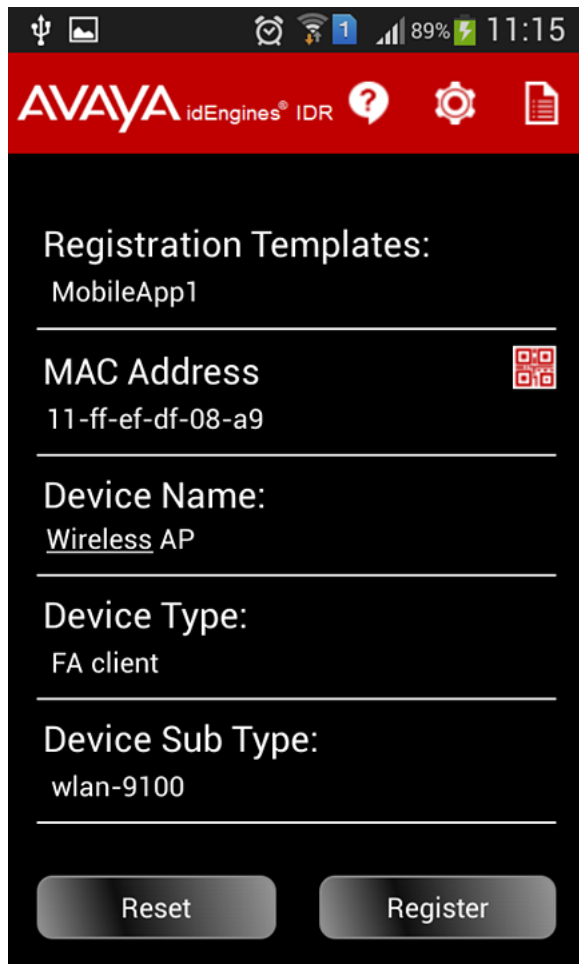
Note that the Identity Engines IDR Android App supports only Extreme QR code format. Following is the Extreme QR code format:

```
SERIAL:xxxxxxxxxxxxxxxxxxxxx  
MAC:xx:xx:xx:xx:xx:xx  
VPORT:16  
PEC:EC1100010-E6  
MAN:AVA  
MOD: ONA 1101GT  
REV:xxx.xxxx
```

- c. Tap **Device Name** to enter the device name.
- d. Select **Device Type** from the drop-down.

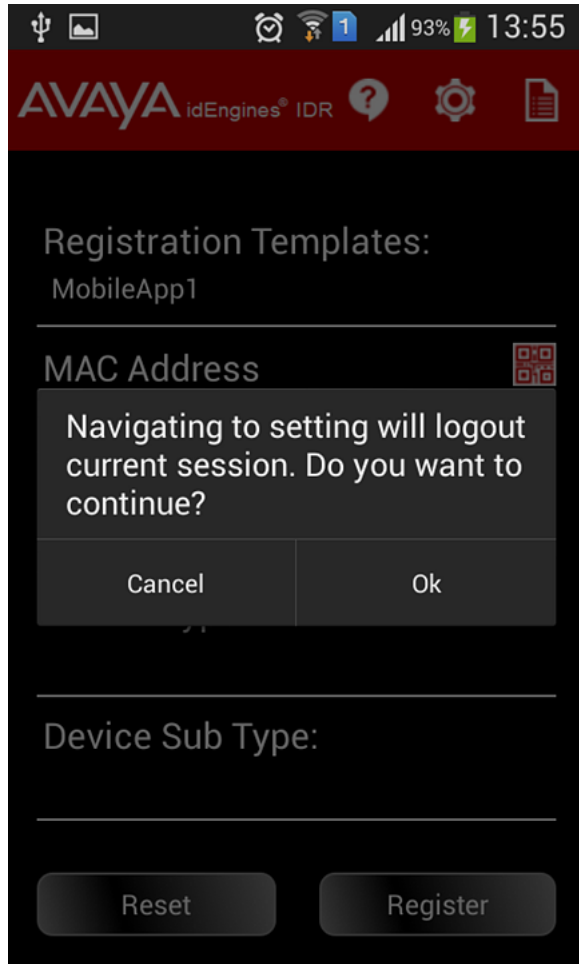
The **Device Sub Type** drop-down is populated with the default Sub Type available for the selected device type.

- e. Tap **Device Sub Type** to select appropriate Sub Type from the populated drop-down.

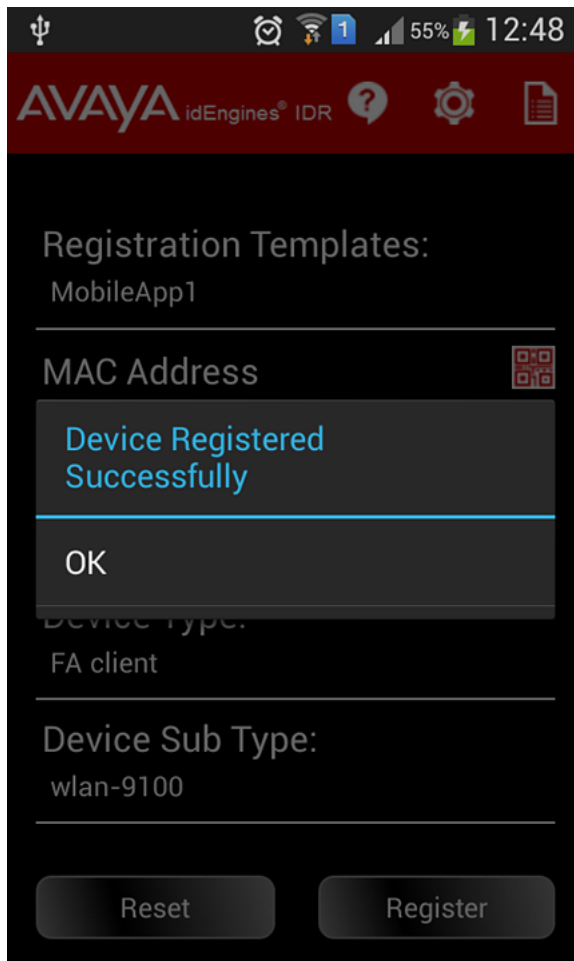


*** Note:**

After the session is established, navigating to settings page or pressing back leads to logout of current session. A confirmation message will be displayed to continue.



3. Click **Register** to register the device.



Viewing Device List

Use the following procedure to view the device list.

Procedure

1. In the top-right, click **Device List Icon**.
The **Device List** is displayed.

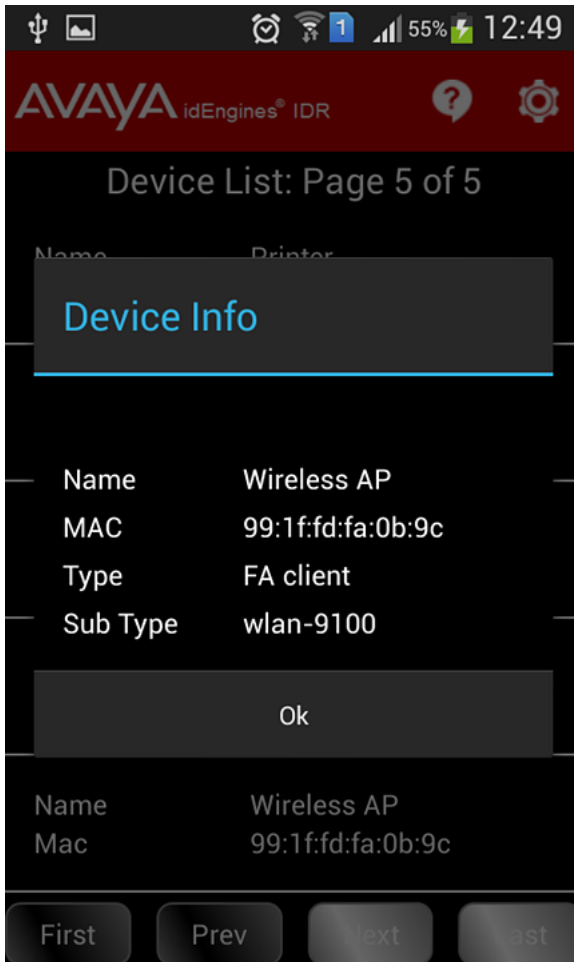
AVAYA idEngines® IDR

Device List: Page 5 of 5

Name	IP Camera
Mac	00:11:a2:0e:1d:dc
Name	IP Phone
Mac	f0:11:a2:0e:1d:dc
Name	Printer
Mac	f0:f1:a2:0e:1d:dc
Name	Portable Ultrasound
Mac	11:ff:ef:df:08:a9
Name	Wireless AP
Mac	11:ff:ef:df:08:af

First Prev Next Last

2. Select the desired device to view the device details.



3. You can view the devices using Navigation buttons. Following are the Navigation buttons that are used to view the devices.

The device list displays five devices in a page.

- **Next:** Displays next five devices.
- **Previous:** Displays the previous five devices.
- **Last:** Displays the last five devices.
- **First:** Displays the first five devices.

Chapter 12: Troubleshooting and FAQs

This chapter provides answers to common questions and helps you troubleshoot your queries when you encounter errors while using Identity Engines Guest and IoT Manager.

Trouble Ticket

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

Creating a trouble ticket

Procedure

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

Problem: Provisioner cannot login

Cause

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

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 and IoT Manager Provisioner Application with a *Guest and IoT Manager administrator account*.

Solution

To fix this, check the Guest and IoT Manager entry in Ignition Dashboard to make sure it has the correct IP address and RADIUS shared secret of your Guest and IoT Manager host machine. Follow

the steps in [Making RADIUS Settings on the Ignition Server](#) on page 60 and follow the steps in [Making RADIUS settings in Guest and IoT Manager](#) on page 61.

Problem: Connection to appliance fails

Condition

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

Solution

- Check that the Ignition Server is running correctly from Dashboard to verify that the appliance is running.
- Check Guest and IoT Manager 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 connection to the appliance: check whether the machine that hosts the Guest and IoT Manager appliance can ping the IP address of the SOAP port of the Identity Engines Ignition Server. If it cannot, check your network settings.
- Check to make sure the SOAP service is enabled on the appliance. Run Ignition Dashboard (see [Launching Ignition Dashboard](#) on page 245), connect to the appliance, click on **Configuration** tab, select the site, click on Services tab, click your node, and click the **SOAP** tab. See [Making SOAP settings on the Ignition Server](#) on page 56 for details.
- Check that the correct admin root certificate has been installed in Guest and IoT Manager. See [Installing the SOAP certificate](#) on page 54.

Problem: Errors reported during bulk saves and deletes

Condition

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 and IoT Manager application may report the error: `java.net.SocketTimeoutException: Read timed out`. You may safely ignore this error.

Cause

This error is reported because Ignition Server 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: Guest and IoT Manager Email Sending Failed

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

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

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

Identify failure details by following :

1. Perform Test Email. For more information, see [Set Up E-Mail Notification Parameters](#) on page 62.
2. Create a trouble ticket.
3. Unzip the file and open `logs/catalina.out`.
SMTP debug logs displays at the bottom of the screen.

Problem: SOAP Service might be disabled

The error appears in Guest and IoT Manager GUI, when IDE server is rebooted.

1. Wait for at least 5 minutes after any reboot was carried out on the Ignition Server and try again.
2. If the error still persists, then from Ignition Dashboard disable or enable the SOAP service.

Launching Ignition Dashboard

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

Procedure

1. On the Windows PC where Ignition Dashboard is installed, double-click the Ignition Dashboard icon on the desktop or select the command **Start:Programs: Ignition Dashboard: Ignition Dashboard**. The login window appears.
2. Type the Ignition Server administrator **User Name** and **Password**. The default user name and password are `admin` and `admin`.

3. In the **Connect To** field, do one of the following:
 - To connect to an individual Ignition Server site, type the hostname or IP address of your Ignition Server.
 - To connect to a group of Ignition Server sites that you manage, choose the Site Group Name in the **Connect To** drop-down list.
4. Click **OK**. If you are unable to log in, see the section, “Problem: Cannot Connect to Ignition Dashboard” in the *Identity Engines Ignition Server Configuration, NN47280-600*.

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

Problem: Virtual machine issues

Guest and IoT Manager URL is not Accessible

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

Guest and IoT Manager HTTPS is not using the Custom Certificate

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

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

Guest and IoT Manager CLI

If you are not able to ping the Guest and IoT Manager VM after you assign the IP address and configure the route, enter `reboot` from the CLI.

Launching IDR Android App

The following section explains the common failures that can occur while launching IDR Android App.

Could not resolve hostname

1. Check hostname in settings page and verify if it is correct.
2. Verify the Mobile device and Guest and IoT Manager Server are on same network.
3. Provide fully qualified Domain Name in hostname.

Connection timeout error

1. Check wireless network in android mobile if it is fluctuating or slow.
2. Verify the android mobile and Guest and IoT Manager Server are on same network.

Ignition Guest and IoT Manager not connected to Ignition Server

Ignition Guest and IoT Manager Server is not connected to appropriate Ignition Server. Login into Guest and IoT Manageradmin account and connect to Ignition Server.

No provisioning group configured for device registration

No device registration template configured for device registration from mobile app. Login to Guest and IoT Manager admin account and create a device registration template (provisioning group) with mobile app permission and associate to provisioner.

Import Configuration Troubleshooting

Condition

- Guest and IoT Manager URL is not accessible
- Https certificate is not working after importing new configuration

Note:

As part of every Guest and IoT Manager import, the backup of the existing configuration is maintained in the system.

Location: `/operational/backup/Guest&IOTManager_<date>_time` (where date and time correspond to when the import was triggered from Guest and IoT Manager application).

Solution

1. Login to Guest and IoT Manager VM with admin account.
2. From the CLI, enter :

```
user root enable
exit
```
3. Login to Guest and IoT Manager VM as root.
4. Navigate to `/operational/backup/Guest&IOTManager_<date>_time`.
 - a. Copy/Replace `GuestManager/*` to `/operational/GuestManager/`
 - b. Copy/Replace `tomcat6/*` to `/etc/GuestManager/tomact6/idEngines/`

5. Perform reboot.

VM Configuration Troubleshooting

Condition

1. Guest and IoT Manager URL is not accessible.
2. Guest and IoT Manager HTTPS is not using custom certificate.
3. Guest and IoT Manager CLI: If Guest and IoT Manager VM is not pinging after you assign IP and route.

Solution: URL is not accessible and HTTPS is not using custom certificate

1. Login to Guest and IoT Manager VM with admin account
2. Issue httpd restart.

Solution: If Guest and IoT Manager VM is not pinging after you assign IP and route

1. Login to Guest and IoT Manager VM with admin account.
2. Issue reboot.