Extreme™
Customer-Driven Networking

ExtremeControl Guest and IoT Manager Configuration

Release 8.2.4
9035909-02
March 2019

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

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

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: www.extremenetworks.com/support/policies/software-licensing

Contents

Chapter 1: About this Document

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

Purpose

Guest and IoT Manager provides a simple and personalized web user interface through which an operational team can quickly and securely manage visitor network access.

It is intended for system administrators who will be installing, managing, and configuring the Guest and IoT Manager application.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that can be used throughout this document.

Table 1: Notice Icons

Icon	Alerts you to...
Important:	Key information that does not carry with it the risk of personal injury, death, system failure, service interruption, loss of data, damage to equipment, or electrostatic discharge.
Note:	Important features or instructions.
Tip:	Helpful tips and notices for using the product.
Warning:	A potential hazard exists that, if not avoided, can result in harm to hardware or equipment.

Table continues…

Icon	Alerts you to...
Caution:	Practices that are not safe or are potential hazards not covered by danger or warning messages.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon. Examples: • Click **OK**. • On the **Tools** menu, choose **Options**.
Italic Text	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.
`Plain Courier Text`	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages. Examples: • `show ip route` • `Error: Invalid command syntax [Failed][2018-09-12 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation tree, expand the **Configuration** > **Edit** folders.

Documentation and Training

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

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

Table continues…

Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

Getting Help

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

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 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

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

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

   Note:
   You can modify your product selections or unsubscribe at any time.
4. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. 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, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Chapter 2: New in this Document

The following sections detail what is new in this document.

Sponsored LDAP search Root

The Sponsored LDAP search Root can ONLY contain LDAP-defined Container Objects (CN) or an Organizational Unit (OU). For more information, see Configuring Sponsor Approval on page 74.

Reference to XMC user guide

Once the procedures for GIM configuration are complete, you need to configure GIM on Extreme Management Center (XMC). To know how to complete the XMC side of the GIM deployment, refer to **Extreme Control User Guide**. For more information, see Configuring the Guest and IoT Manager Virtual Appliance on page 26.

UI changes

There are UI changes in the following sections:

- The **Common** screen has been updated in Configuring the Common Details on page 65.
- The **Summary** screen is updated in Modifying and Viewing an Onboarding Template on page 98.
- The **Add Self-Service Provisioner** screen is updated in Creating Self-Service Provisioners on page 115.

Chapter 3: Guest and IoT Manager Overview

Welcome to the ExtremeControl Guest and IoT Manager Web Application! The Guest and IoT Manager (GIM) is an application that integrates with ExtremeControl. The purpose is to provide non-IT personnel with the ability to provision Guest Users and / or Devices within the constrains defined by the Administrator. Guest and IoT Manager communicates with the ExtremeControl Engine(s) for provisioning of Guest Users and Devices that may access the network through standard process of authentication and authorization by ExtremeControl.

Guest and IoT Manager allows the Administrator to perform the following:

- Create and customize Onboarding Templates for Guest Users and Devices.
- Create Internal Provisioners.
- Assign one or more Onboarding Templates to Internal or External Provisioners Provisioners (Provisioners on AD / LDAP)
- Enable and customize Guest and IoT Manager REST APIs for integration with third party applications.
- Enable and customize Guest and IoT Manager Outlook Plug-in.

Furthermore, Guest and IoT Manager allows the Provisioners to use the Onboarding Template(s) and provision Guest User and / or Devices based on their customized constrains. Provisioners may be:

- **External Provisioners** : They can be Employees or Students that reside on an AD or LDAP server.
- **Internal Provisioners** : These are created by the Administrator and are Business Partners, Vendors, Suppliers, Contractors, Front Desk Personal, Security Guards and so on.

The Guest and IoT Manager Administrator and the Provisioner have different splash login pages. When the Provisioner logs in;

- In case of external Provisioner, authentication happens by the Extreme Control engine against AD / LDAP.
- While in case of an Internal Provisioner it is against the Local Repository.

Once the Provisioner logs in, then the Provisioner has access to the Onboarding Templates that the Administrator has provided and is able to provision Guest User and / or Devices.

The Guest and IoT Manager Overview chapter provides information on the following:

Guest and IoT Manager Application Framework

The Extreme Management Center 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.
- Access Control Engine that authenticates and authorizes users who desire to connect to your network.
- Extreme Management Center Application to create the authorization policies that determine which users can connect to specific parts of your network.
- **Optionally :** Extreme Management Center Captive Portal : The web-based authentication helps users connect their “Bring Your Own Device” (BYOD) devices to enterprise network even though if it is not equipped with 802.1X authentication software.

User Roles and Access Controls

Roles are an important concept in the Guest and IoT Manager application. Roles determine what users can view or perform, including what they can monitor and the types of changes they can make. Parts of the UI features are not available to users whose role does not authorize access to those features. The Guest and IoT Manager application facilitates the following user roles.

The three roles defined with different access control in the system are:

Guest and IoT Manager Administrator Role

The Guest and IoT Manager Application has single Administrator account. The Administrator of this account can set / modify access rights such as Username, Password, delete Guest User accounts, Device records and can also perform the following actions.

- Create the Onboarding Template.
- Configure application settings.
- Create and manage the Provisioner accounts. Each account has its own Username and Password.
- Connect the application to the Extreme Management Center appliance. The Administrator must ensure that the connection is stable for the Provisioners to use it.
- Manage Guest User accounts and Device records to remove the expired user accounts.

Provisioner Role

The Provisioner uses the Guest and IoT Manager application to manage Guest Users and Devices that they have created.

Each provisioner account is stored either in the Local Password Repository (LPR) internal store or in Lightweight Directory Access Protocol (LDAP).

Important:

Guest Users and Devices onboarded by the Provisioner can only be managed from Guest and IoT Manager.

Guest Users Role

A Guest User is a visitor or other temporary user to whom you grant specific limited rights to use the network. A Provisioner uses the Guest and IoT Manager Application to create any number of Guest User accounts. Guest User accounts are stored in Local Password Repository (LPR).

The created Guest User account contains the following attributes:

- **Account Details:** Includes Username and Password for the temporary account.
- **Personal Data:** Includes first name, last name, email address, and mobile number of the User.
- **Access Duration:** Specifies the account activation time for network access usage and the duration.
- **Auto Expiry Deletion:** Removes the Guest Users automatically after the specified duration.
- **Notification Settings:** Sends an Email or SMS notification stating that the Guest account has been created. The notification contains the Guest User's Name and Password and is usually sent directly to the Guest.

Using the Online Help System

The Guest and IoT Manager documentation is available as online help within the Application.

Important:

The menu icon ☰ at the top right corner of the screen provides links to additional information about your application.

Accessing Help

There are several ways to access the online help system:

- Select the ? **Help** icon in the top right corner of your browser.
- Press **F1** or **Fn + F1** on the keyboard to open the Help to the context-sensitive topic associated with the screen or dialog box you are using in the Application.

Help Features

The help is context-sensitive and as such, the topic displayed in the right panel changes as you navigate. To prevent the help topic from changing when you change screens in the Application, click the ⏸ **Pause** icon at the top of the help screen. Click ▶ **Resume** icon to resume the help.

To open the help in a separate tab, click the **Launch Help** icon. The left panel contains the Table of Contents. Items with a **>** indicate that clicking the TOC item opens another menu of options.

The Help toolbar also contains buttons to search all topics. Use the **Search** tab to search for a word or phrase in the help. In the **Search for** box type the word or combination of words you want to find, and click **Search**. The topics that contain the word or words you entered is displayed. Click the topic to be displayed in the topic pane.

Searching Within Topics

To search for specific instances of a term in only the currently accessed help topic, type **Ctrl + F** to open your browser's search box. Use this to search for the term or phrase in the currently accessed help topic.

Chapter 4: Installing Guest and IoT Manager

This chapter describes how to install Guest and IoT Manager Application. You can install Guest and IoT Manager as a virtual appliance on a VMware ESXi 5.5, 6.0 or 6.5 server.

System Requirements

To install and configure Guest and IoT Manager Application, you need:

- A running Access Control Engine, reachable on the network from where you run Guest and IoT Manager.
- An OVA file, if you are deploying the Guest and IoT Manager in ESXi.
- An installation of the Extreme Management Center application on the system. Make sure you have a copy of Installation document.

VMware ESXi Server Requirements

Hardware platforms supported by VMware's ESXi server versions 5.5, 6.0 or 6.5. For more information on list of supported hardware platforms for ESXi, see http://www.vmware.com/

See the 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 uses Ubuntu as base Operating System.

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, UNIX 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. We do 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, We cannot guarantee that the VM works 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

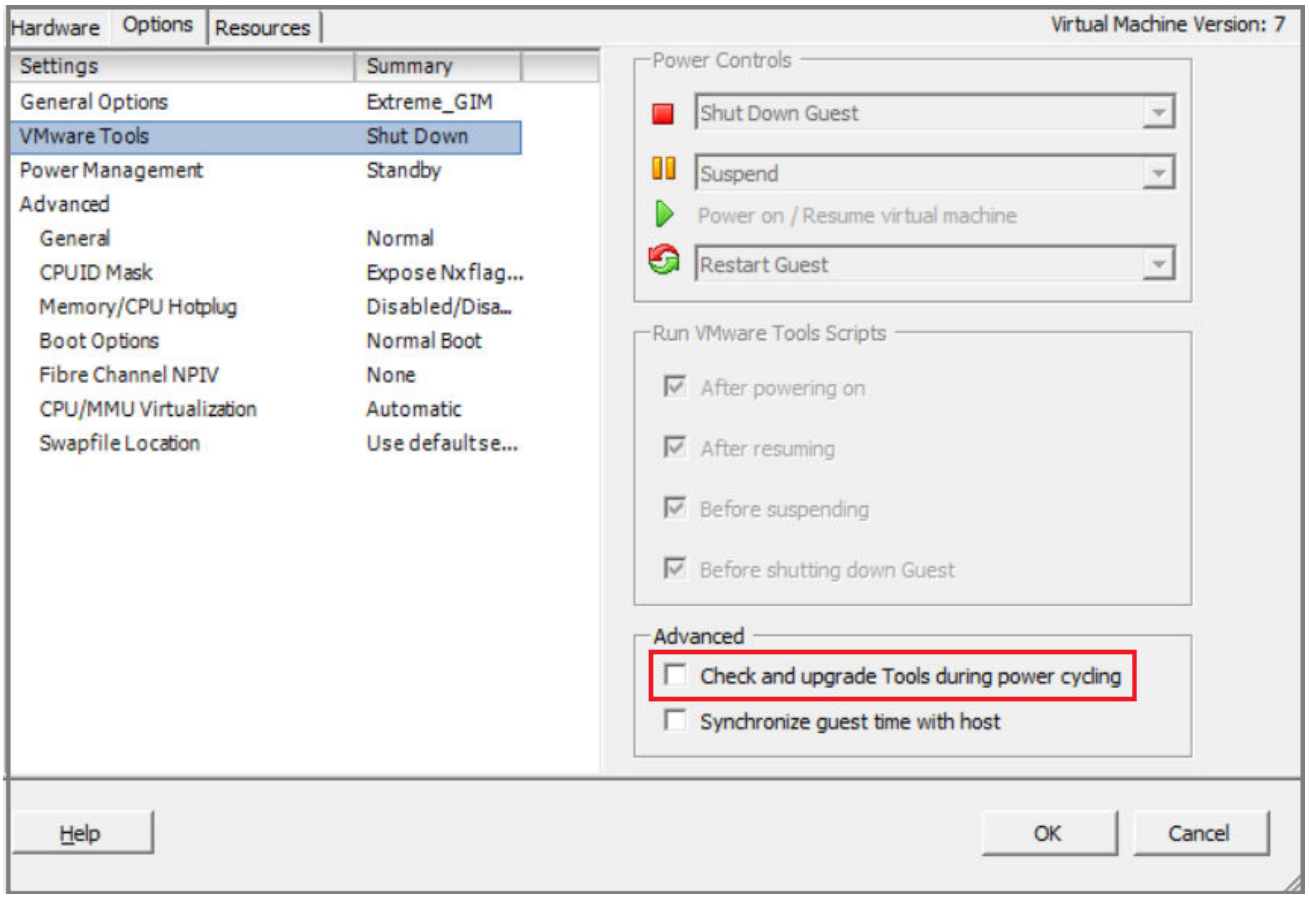
We strongly recommend you to prevent automatic VMware Tool updates and use only the tools that are delivered bundled with the installation package. Use this procedure to prevent automatic VMware Tools updates.

Use this procedure 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** checkbox is not selected. This is the supported setting.
3. Click **OK**.

Example



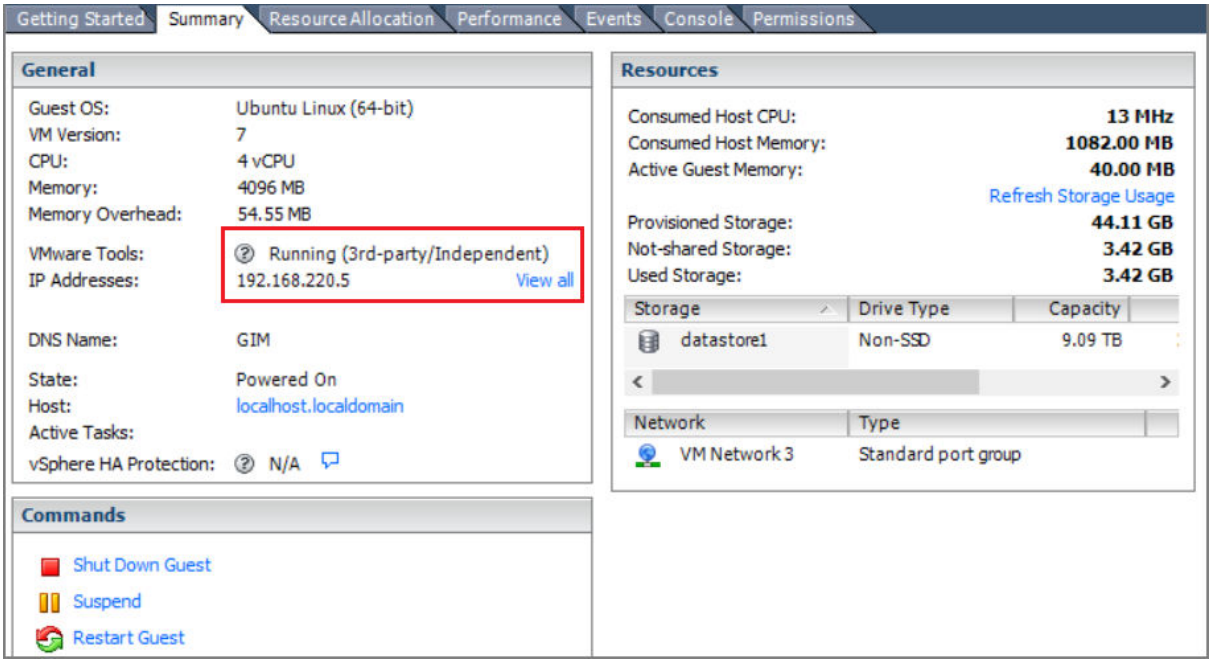
Checking the VMware Tools Status on an ESXi Server

The **Summary** tab of the VM describes the VMware Tools status. Use this procedure 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:

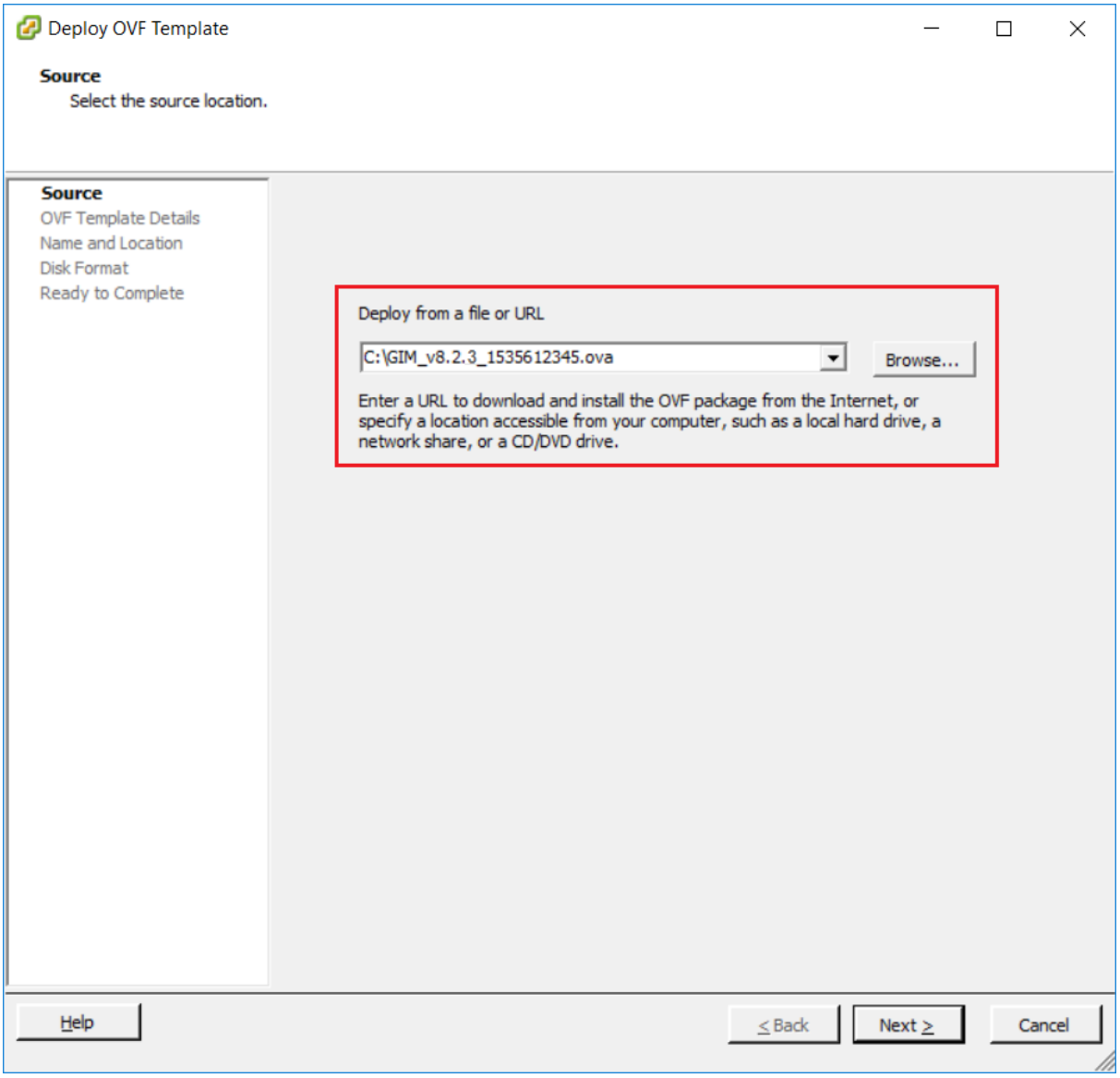
- **Admin :** The Admin interface provides connectivity to the Guest and IoT Manager Administrator and Provisioner web sessions. By default, this interface is also used for handling the connection with Access Control Engine.
- **Service A :** Depending on the network deployment, Access Control Engine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

Installing the Guest and IoT Manager Virtual Appliance

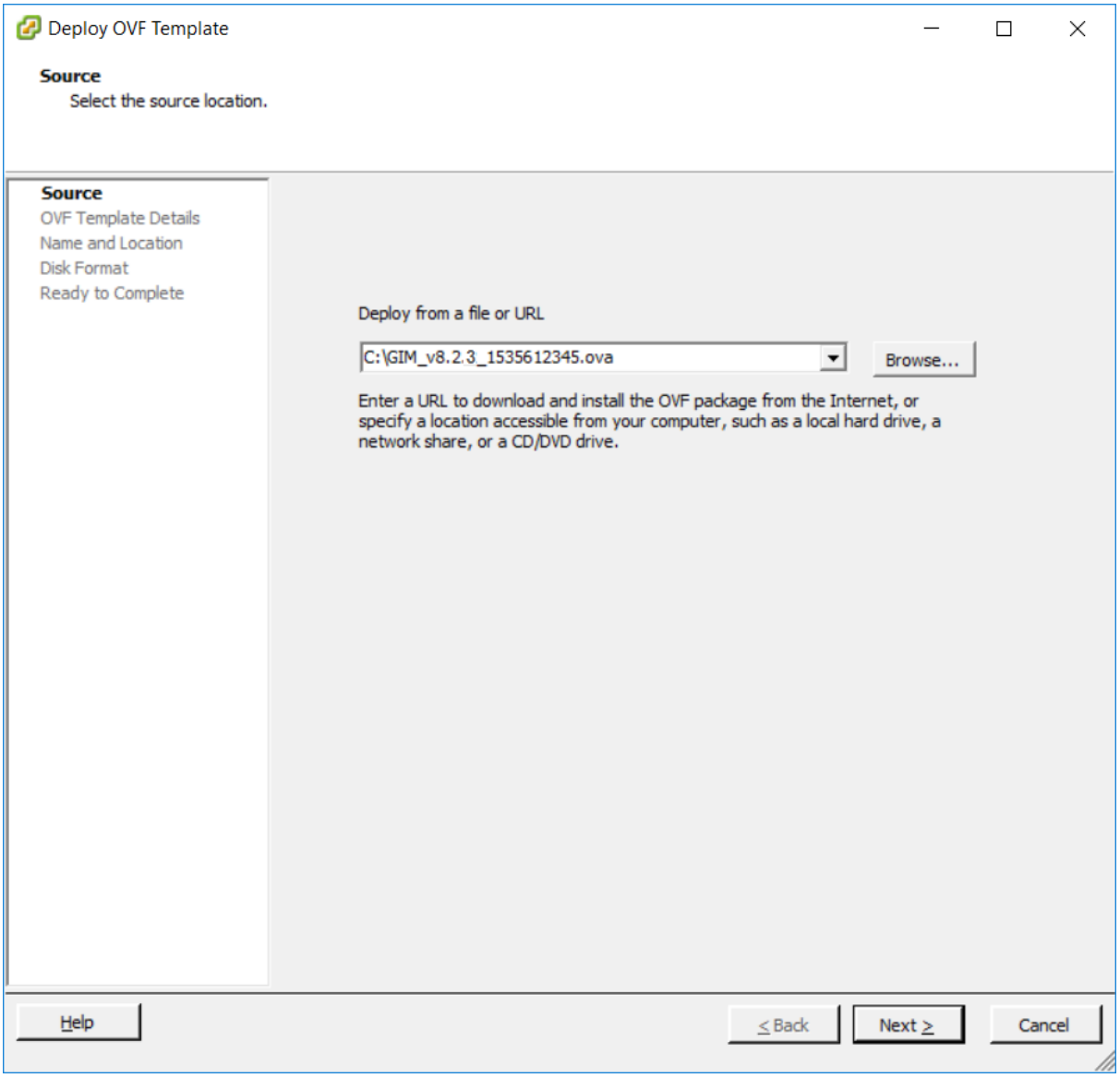
We strongly recommend that you use VMware vSphere Client to import the VM into your system. Start the VMware vSphere Client and log in to the ESXi server on which you want to install Guest and IoT Manager. Use the **Virtual Appliance Deploy OVF** option.

Procedure

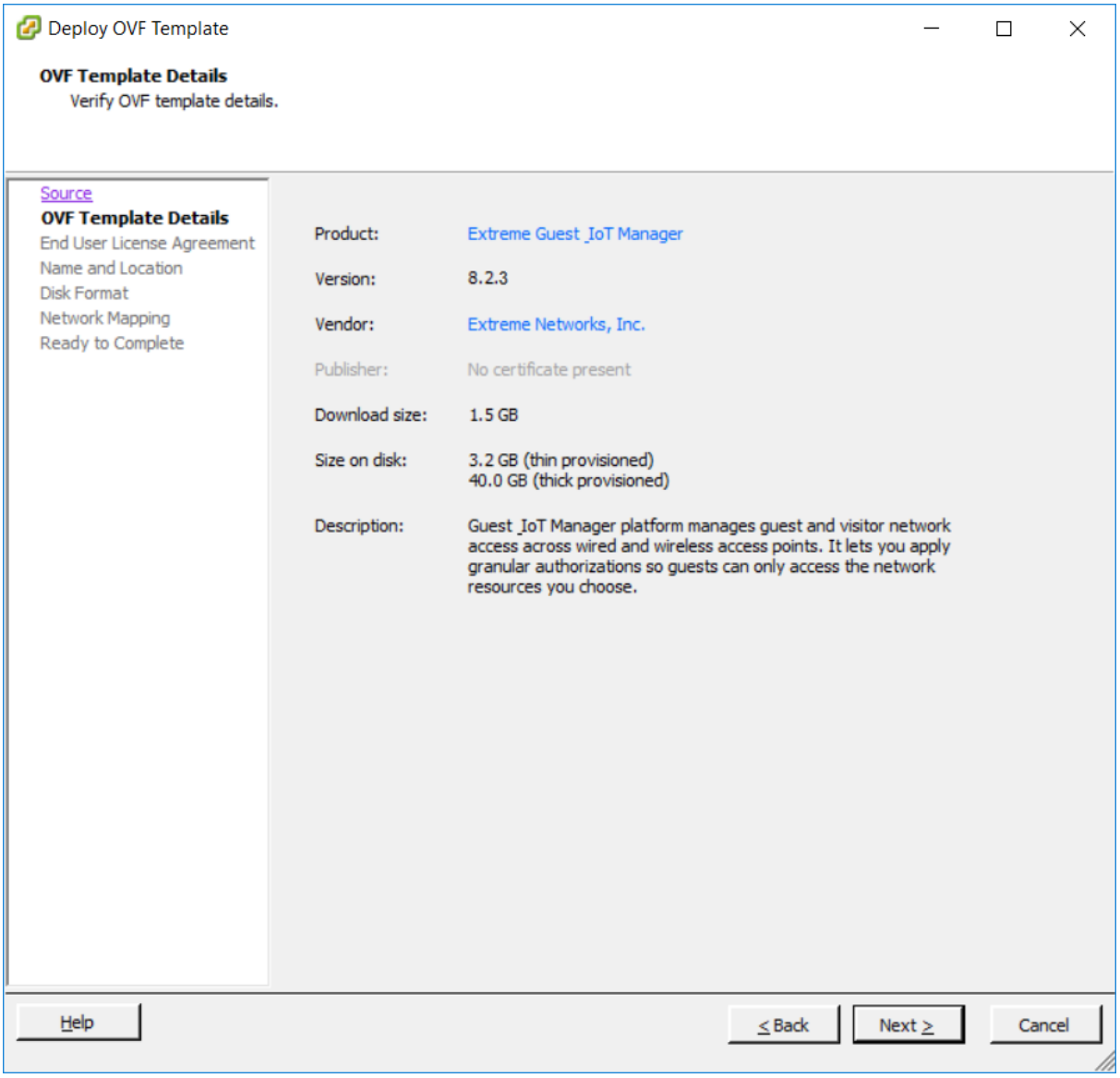
1. From the VSphere Client, select **File** > **Deploy OVF Template**.



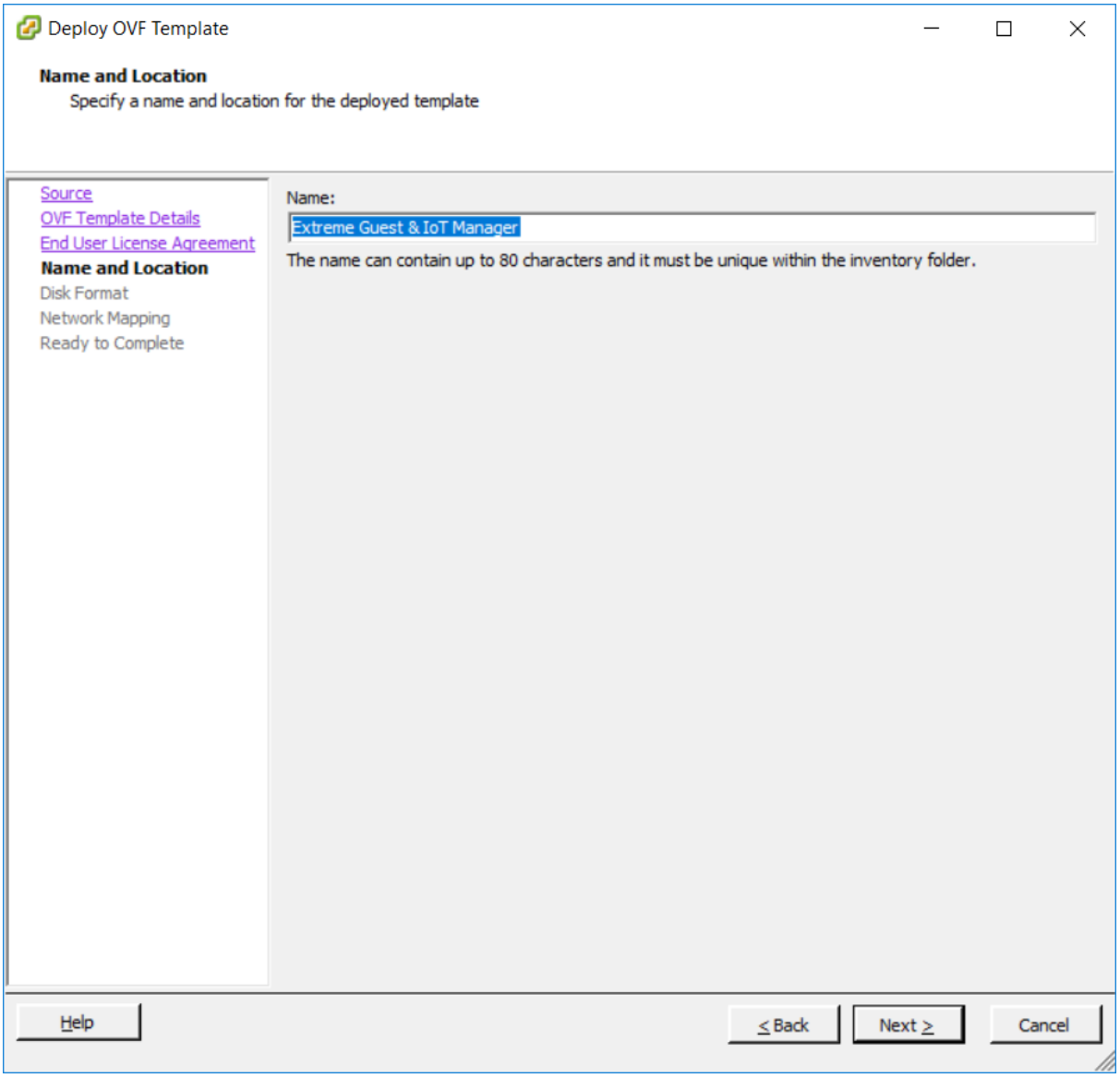
2. On the Source screen, select the location from which you want to import the Guest and IoT Manager virtual appliance and click **Next**.



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

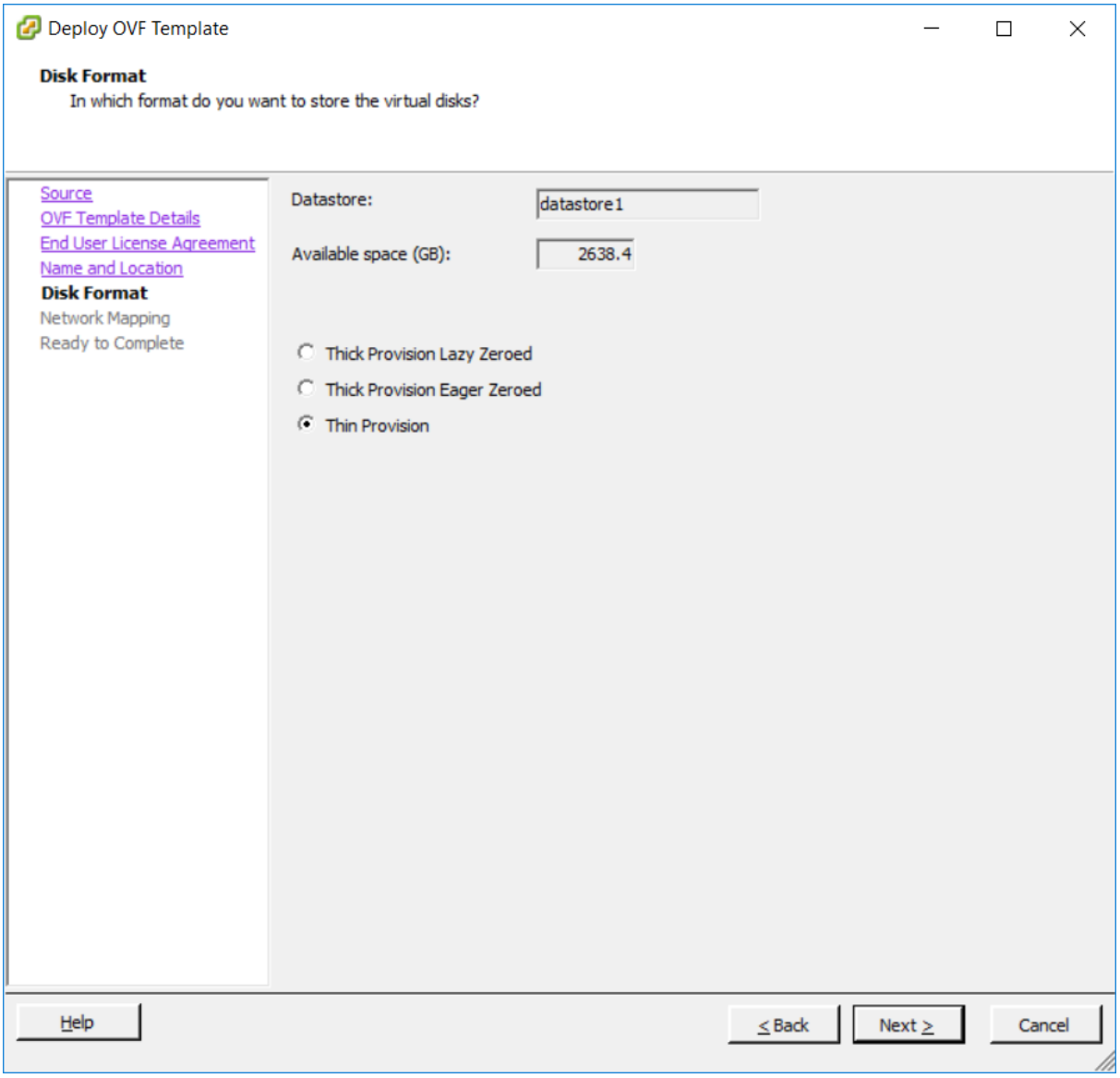


4. On the End User License Agreement screen, click **Accept** to accept the license and click **Next**.
5. On the Name and Location screen, enter a name for the virtual machine and click **Next**.

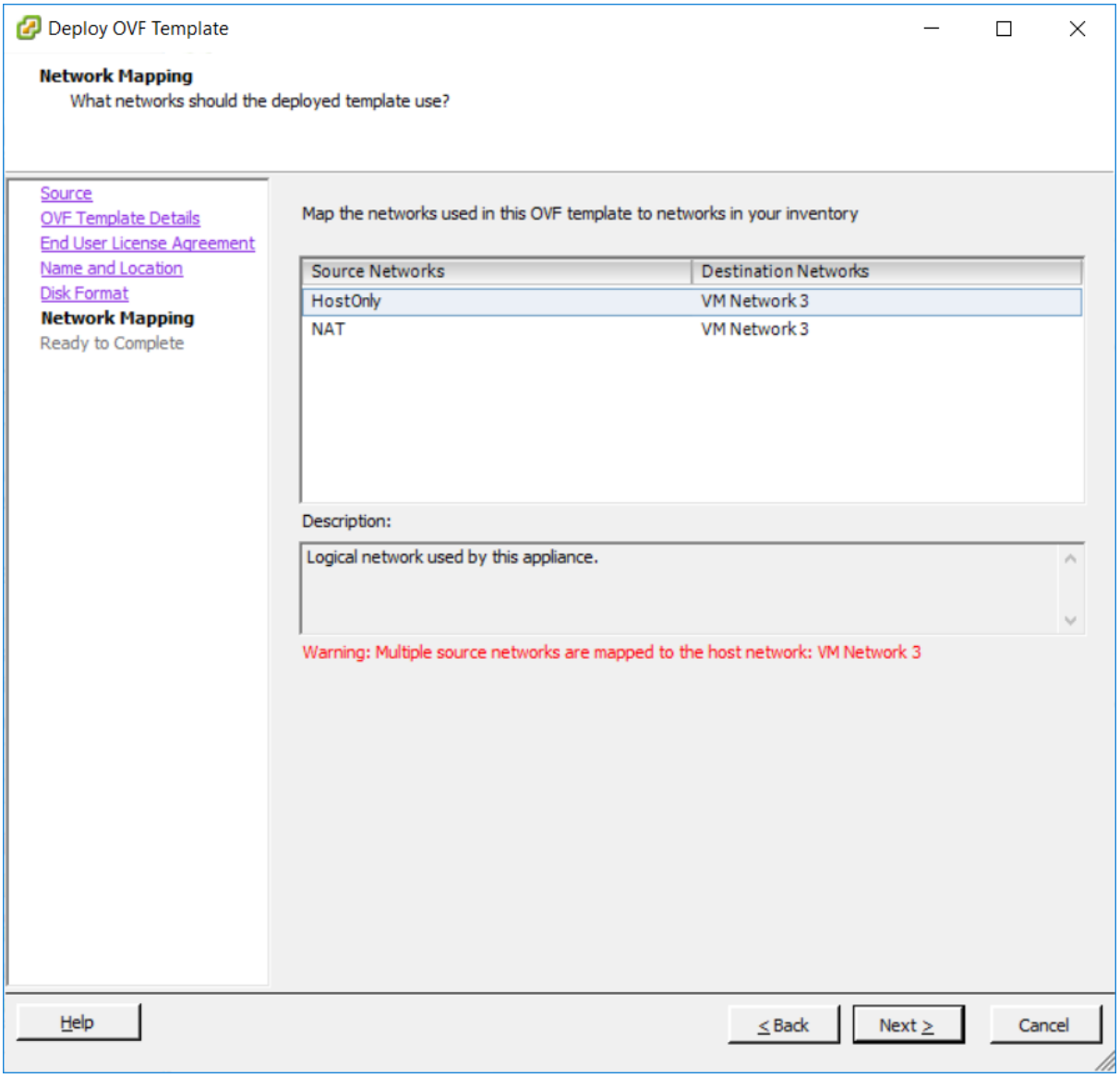


6. On the Disk Format screen, select a format in which to store the virtual machine's virtual disks and click **Next**.

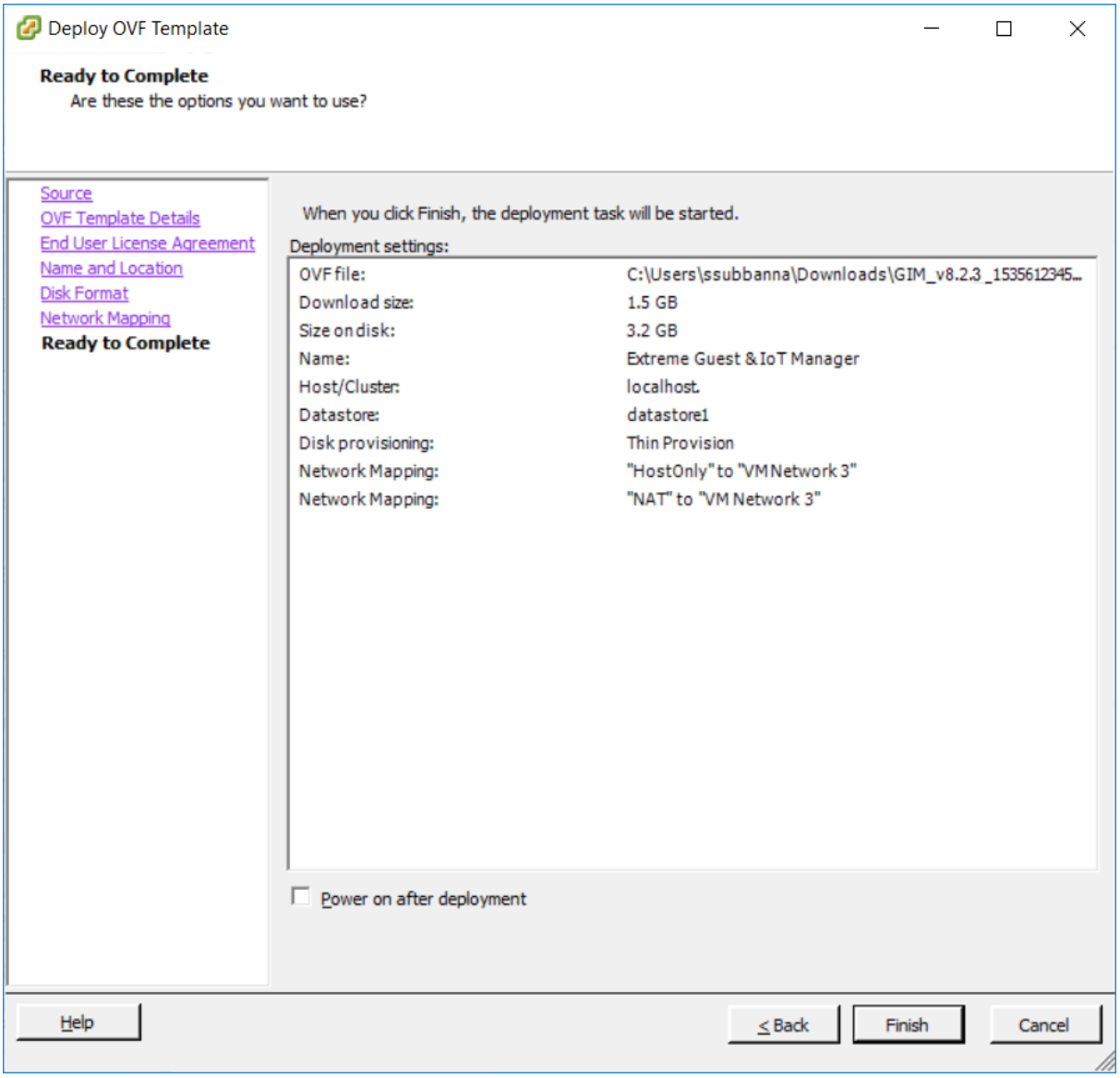
   We recommend to use **Thin Provision** mode.



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



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



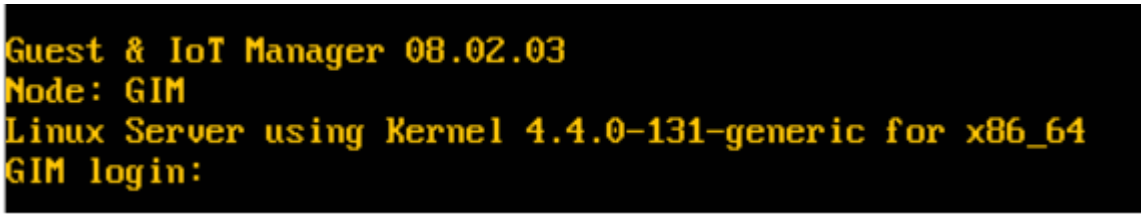
Configuring the Guest and IoT Manager Virtual Appliance

Use this procedure to configure the VM settings after you complete importing the VM to your system. This is the minimum configuration required to start Guest and IoT Manager Application.

Procedure

1. Power on the VM and launch the Guest and IoT Manager console. Enter the User Name and Password. The default User Name and Password is `admin`.

   The Guest and IoT Manager login screen is displayed.



2. Enter the IP address for Guest and IoT Manager administrator interface.

   `[Default: 192.168.220.5]: 10.133.133.143`

3. Enter the IP netmask for Guest and IoT Manager.

   `[Default: 24]:`

4. Enter the gateway address.

   `[Default: 10.133.133.1]:`

5. Enter the Primary DNS address.

   `[Default: 192.168.220.5]: 134.141.162.20.`

   You will receive the status message as "*Please wait while the configuration is set...*".

   Once completed, you will view the status as:

   - "Generating new self-signed certificates for IP `10.133.133.143`. Tomcat restart completed successfully.
   - Restarting the web services to listen on the new IP Address.
   - Please verify the route setting using the "`route command`".
   - Changing the DNS Setting. Tomcat restart completed successfully.

6. To continue setup of Guest and IoT Manager, open a browser to the following URL: `https://<IP address of GIM>/GIM/admin/`. Use admin as the username and password to login and continue the setup procedures as listed in the following sections.

7. Once the user has completed the procedures mentioned above, follow the steps from **Guest and IoT Configuration in Extreme Management Center and Access Control** in **Extreme Control User Guide**. For more information, see page number 698 in https://documentation.extremenetworks.com/netsight/8.2/9035980-03_XMC_ExtremeControl_User_Guide_8.2.pdf

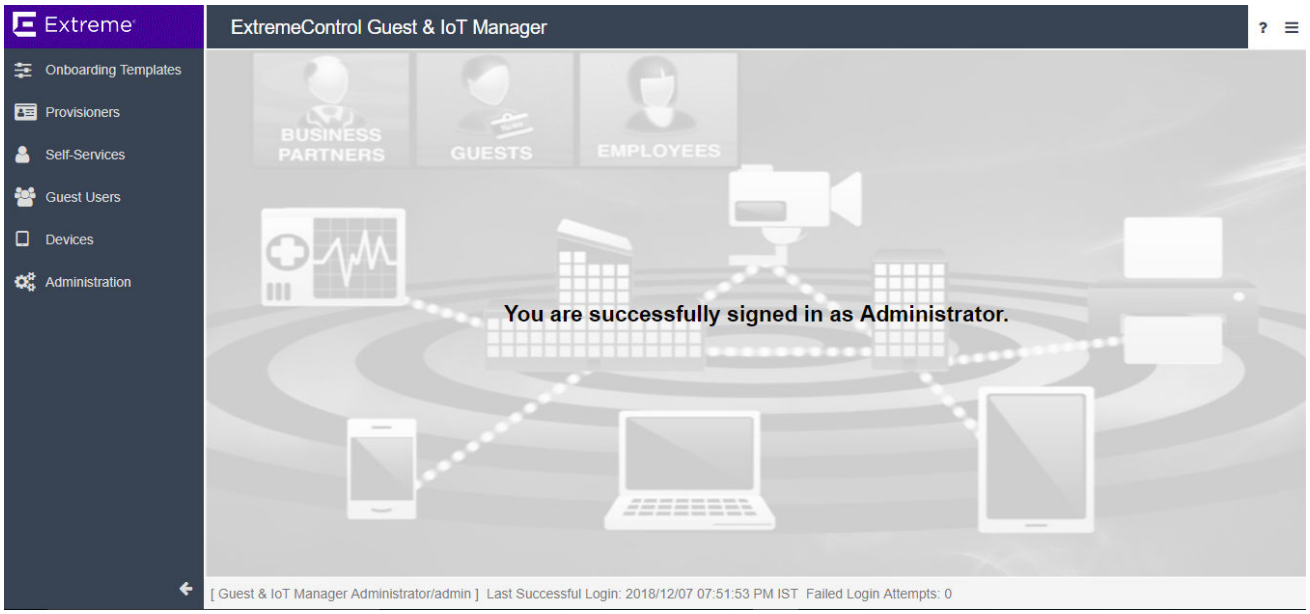
Launching Guest and IoT Manager

The Access Control Engine settings must be configured prior launching the Guest and IoT Manager application for the first time. For more information, see *ExtremeControl Guest and IoT Manager Configuration*.

Guest and IoT Manager consists of two applications:

- **Administrator Application**: The Application that the Administrator uses to configure Guest and IoT Manager to create Provisioner(s) and Self-Service accounts.
- **Provisioner Application**: The Application that Provisioners use to create Guest Users and Devices.

Administrator Home Screen

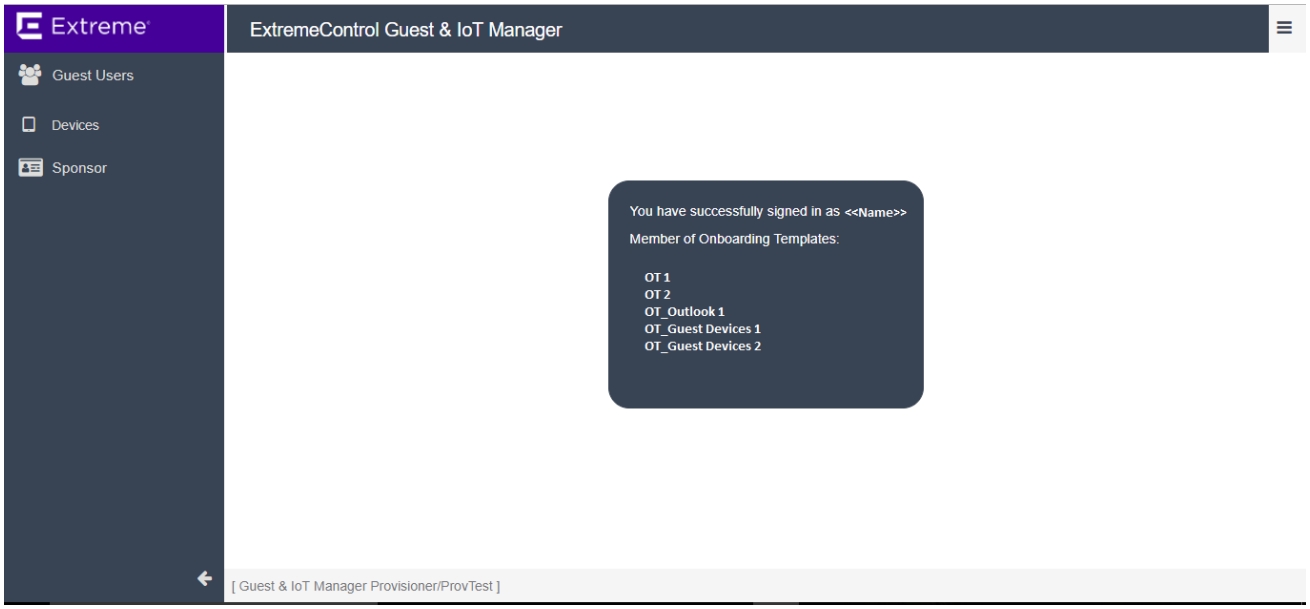


When Administrator logs into Guest and IoT Manager Web UI, the **Last Successful Login**, date, time, and the number of **Failed Login Attempts** between two successful logins of the Administrator account are displayed on the footer of the page.

Note:

You can also change the password after your first login. For more information, see *ExtremeControl Guest and IoT Manager Configuration*.

Provisioner Home Screen



The Onboarding Template associated with the logged in Provisioner is displayed in the Home screen.

Running the Administrator Application

Use this procedure to launch the Administrator Application.

Procedure

1. Open your web browser and enter the URL of the Administrator Application.

   `http://<Guest Manager machine>/GIM/admin/`

   OR

   `https://<Guest Manager machine>/GIM/admin/`

2. In the Login screen, enter the Administrator login credentials.
3. Click **Login**.
   a. If the login attempt succeeds, the Application displays the successful message: *You have successfully signed in as* `<UserName>`.
   b. If your login attempt fails, the Application displays an alert message.
4. **(Optional)** Click **Download GIM Outlook Add-In** to configure an outlook add-in to a Windows or MAC machine. For more information on the GIM Outlook Add-In, see the *ExtremeControl Guest and IoT Manager Configuration*.

Note:

The Administrator web session disconnects, if it is inactive for a period of time as specified in the inactive time-out settings. You need to login again to use the Application. For more information about how to configure the administrator account, see *ExtremeControl Guest and IoT Manager Configuration*.

5. Click **close[x]** to accept and close the cookie policy information displayed at the end of the login screen. Click the hyperlink to view the organization Privacy and Cookies Policy as specified in the Administrator **Preference** settings.

Running the Provisioner Application

Use this procedure to launch the Provisioner Application.

Procedure

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

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

   OR

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

2. In the Login screen, enter the Provisioner login credentials.

   Note:

   Provisoner can be LPR user or LDAP user.

   If you do not have a Provisioner account, contact Guest and IoT Manager Administrator.

3. Click **Login**.

   a. If the login attempt succeeds, the Application displays the successful message: *You have successfully signed in as* `<UserName>`.

   b. If your login attempt fails, the Application displays an alert message.

4. **(Optional)** Click **Download GIM Outlook Add-In** to configure an outlook add-in to a Windows or MAC machine. For more information on the GIM Outlook Add-In, see *ExtremeControl Guest and IoT Manager Configuration*.

   Note:

   The Provisioner Application session disconnects, if it is inactive for a period of time as specified in the inactive time-out settings. The Guest and IoT Manager Administrator sets the time-out threshold limit. You need to login again to use the Application. For more information about setting the inactivitiy timeouts, see *ExtremeControl Guest and IoT Manager Configuration*.

Provisioner login associated with REST API Onboarding Template and Outlook Add-in Onboarding Template cannot create new Guest User or Device. Only view option is available.

5. Click **close[x]** to accept and close the cookie policy information displayed at the end of the login screen. Click the hyperlink to view the organization Privacy and Cookies Policy as specified in the Administrator settings.

Chapter 5: Administering Guest and IoT Manager

This module is intended for Guest and IoT Manager Administrator and describes how to manage and troubleshoot the Application and its components.

If you are a Provisioner, you may skip this module and proceed to *ExtremeControl Guest and IoT Manager Configuration*.

Connecting to the Guest and IoT Manager Admin Page

Use this procedure to connect to the Guest and IoT Manager Administrator.

Procedure

1. Connect to the Guest and IoT Manager Admin page by entering the URL of the Administrator Application in your web browser: `https://<IP address of GIM>/GIM/admin/`
2. Use `admin/admin` as the username and password to login.

   Once you login, continue the setup procedures as listed in the following sections.

Configuring the Administrator Account

The **Account** tab in Administration menu allows you to modify the password and timeout values for Administration, Provisioner, and Outlook sessions.

Connecting to the Guest & IoT Admin Page

Procedure

1. Connect to the Guest and IoT Manager Admin page by opening a browser to the following URL: `https://<IP address of GIM>/GIM/admin/`

2. Use admin as the username and password to login and continue the setup procedures as listed in the following sections.

Field Descriptions

Use the data in the following table to use the **Administrator** section.

Name	Description
Username	By default, Username field is disabled.
Current Password	Specifies the current password that is used to login the Guest and IoT Manager Application.
New Password and **Confirm New Password**	Configures a new password for the Administrator account. The Guest and IoT Manager encrypts the password. The new password must meet the following complexity checks: • Ensure that you use minimum of eight characters in the password. • Password must be a combination of Lowercase, Uppercase, One Number, and at least one Special character from the following: `! @ # $ % ^ & * ( ) – +` • New password cannot match the three recently used passwords. If the password does not meet the complexity criteria, the system displays an error message. **Note:** We recommend that you change the Administrator password after you have completed the initial setup of Guest and IoT Manager Application.

Setting Inactivity Timeouts

Use this procedure to modify the timeout values for Administration, Provisioner and Outlook sessions.

Procedure

1. In the navigation pane, click **Administration** > **Account** tab.
2. In the **Inactivity Timeout** section, modify the duration and select the duration units from the **Idle Timeout** and **Outlook Idle Timeout** drop-down list.
3. Click **Save** to save the configuration.

Field Descriptions

Use the data in the following table to use the **Inactivity Timeout** section.

Name	Description
Idle Timeout	Configures the idle time-out period. The time-out period disconnects the Administrator / Provisioner Application after a period of inactivity that exceeds the applicable threshold. You must log in again to use the application with the new changes. The default time-out period is 30 minutes and the maximum period is 24 hrs.
Outlook Idle Timeout	Configures the idle time-out period for Outlook. The time-out period disconnects the Outlook Application after a period of inactivity that exceeds the applicable threshold. You must log in again to use the application with the new changes. The default time-out period and the maximum period is 24 hours.

Setting Preferences

The **Preferences** tab in Administration menu allows you to customize the User Interface to fit your personal preferences like changing the application logo, name, language, file manager, terms of use and privacy policy information. You can use these settings to brand the application's look and feel as per the requirement.

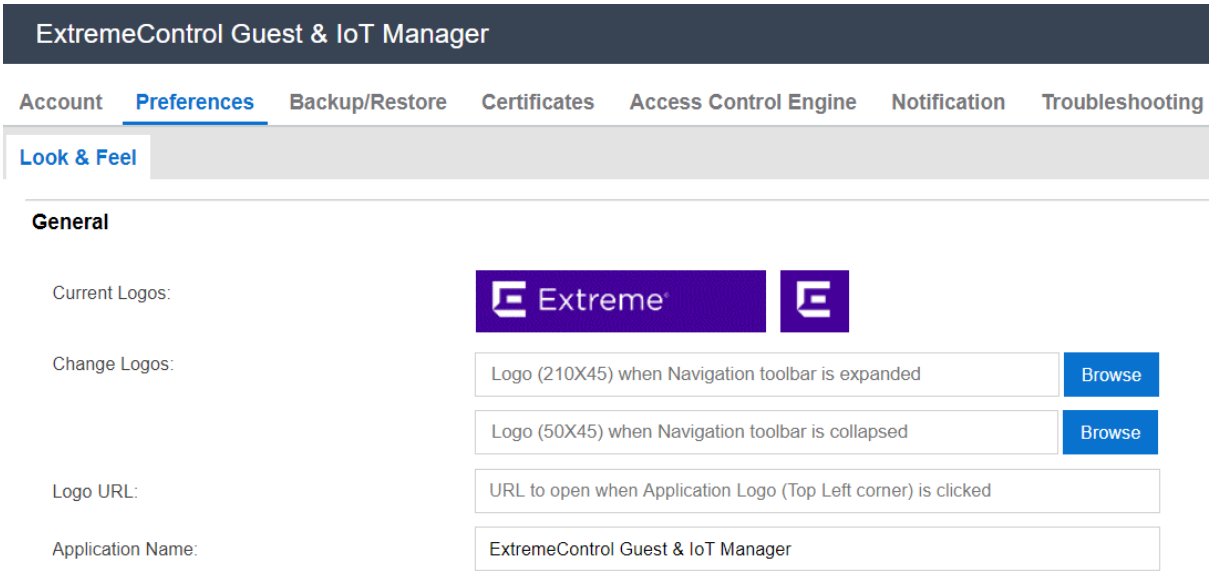
Customizing General Preferences

Use this procedure to modify the logo and application name.

Procedure

1. In the navigation pane, click **Administration** > **Preferences** tab.

   By default, the Look and Feel screen is displayed along with the current logo used in the application.



2. In the **General** section, configure the Logo, URL and Name as following:
   a. Click **Browse** to navigate to the file you wish to upload in the **Change Logo** field, when the navigation toolbar is expanded / collapsed.
   b. **(Optional)** Enter the specified URL address in the **Logo URL** field.
   c. Enter the application name that you want to change in the **Application Name** field.
3. Click **Save** to save the configuration or **Restore to Defaults** to cancel the changes and restore to default value.

Field Descriptions

Use the data in the following table to use the **General** section.

Name	Description
Current Logos	Displays the default or currently configured logo.
Change Logos	Navigates to the file you prefer to upload when navigation toolbar is expanded or collapsed. **Note:** The height and width of the expanded logo must be 210 * 45 pixels and collapsed logo must be 50 * 45 pixels.
Logo URL	Configures the URL to the Logo button. You can access the specified link in a new window when you click on the Logo.
Application Name	Customize the name of the Guest and IoT Manager application.

Setting the Locales

Use this procedure to change the language preference of the Application.

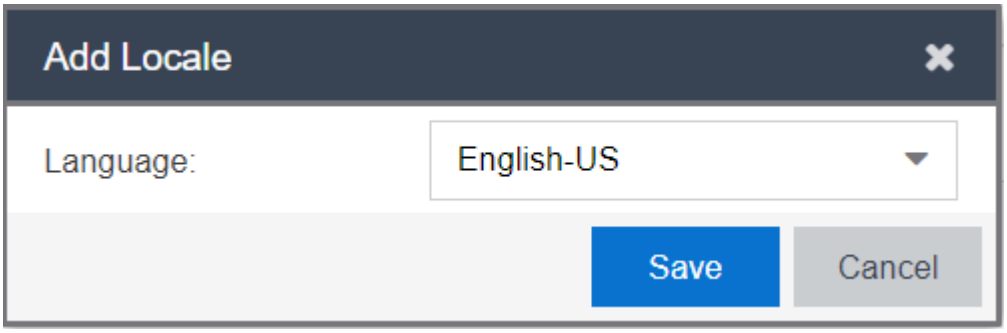
Note:

This setting applies to only Provisoner, Self-Service and Outlook Add In Provisioner. The Provisioner has to login again to view the modified changes.

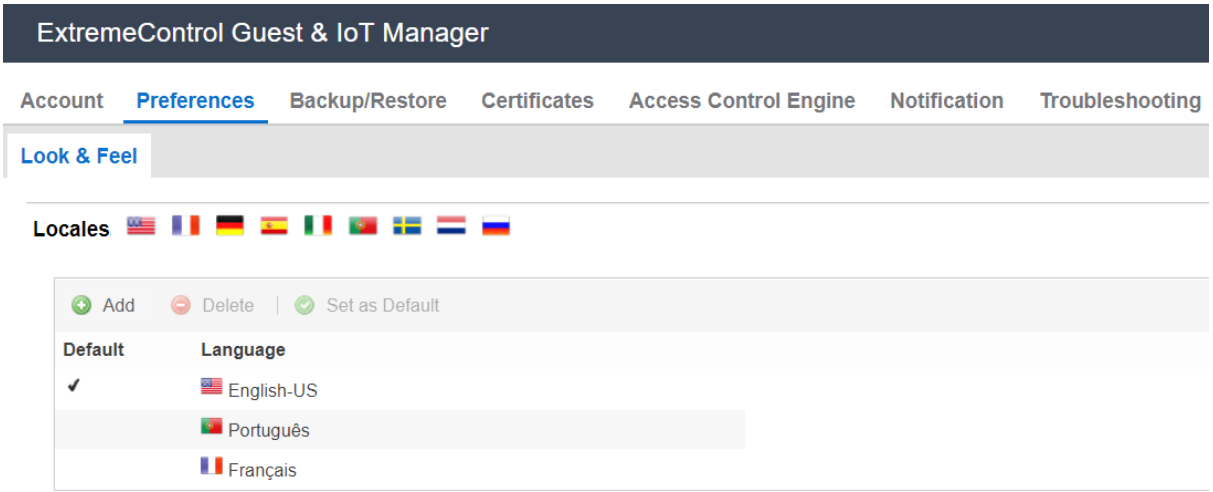
Procedure

1. In the navigation pane, click **Administration** > **Preferences** tab.
2. In the **Locales** section, click **Add**.

   The Add Locale screen is displayed.



3. In the Add Locale screen, select the required language preference from the **Language** field drop-down list and click **Save**. The selected language preference is added to the list.



4. Select the required language and click **Set as Default**. The selected language is displayed as default language during Provisioner login.
5. **(Optional)** Select the required language(s) and click **Delete** to clear the added language.

   Tip:

   The default language cannot be removed.

   Use Ctrl / Shift to select multiple records to delete.

6. Click **Save** to save the configuration or **Restore to Defaults** to cancel the changes and restore to default value.

Field Descriptions

Use the data in the following table to use the **Locales** section.

Name	Description
Language	Displays the preferred language in which you want the application to be displayed for the Provisoner. Currently, the Guest and IoT Manager application is available in the following languages: English, French, German, Spanish, Italian, Portuguese, Swedish, Dutch, and Russian. Administrator can select a maximum of three languages including default language and also select any one of the three languages as default. Custom Attributes in Onboarding Template can be configured using these languages. The configured languages are available for the Guest and IoT Manager Provisioner, Self-Service Provisioner, and Outlook Add In. • **Provisioners / Outlook Add-In Page**: The login page loads with the default language selected. On clicking a desired language, the page reloads with the selected language. **Note:** The Provisioner has the option to select language only in the login page. The selected language in the login page is used throughout the Provisioner's session. Provisioner's language preference is stored in the browser as a persistent cookie and used for subsequent sessions. Provisioner can change this by selecting any other language to overwrite the cookie. • **Self-Provisioning Page**: The languages are displayed in both Guest User and Device Registration page. On clicking a desired language, the page reloads with the selected language.

Configuring the File Manager

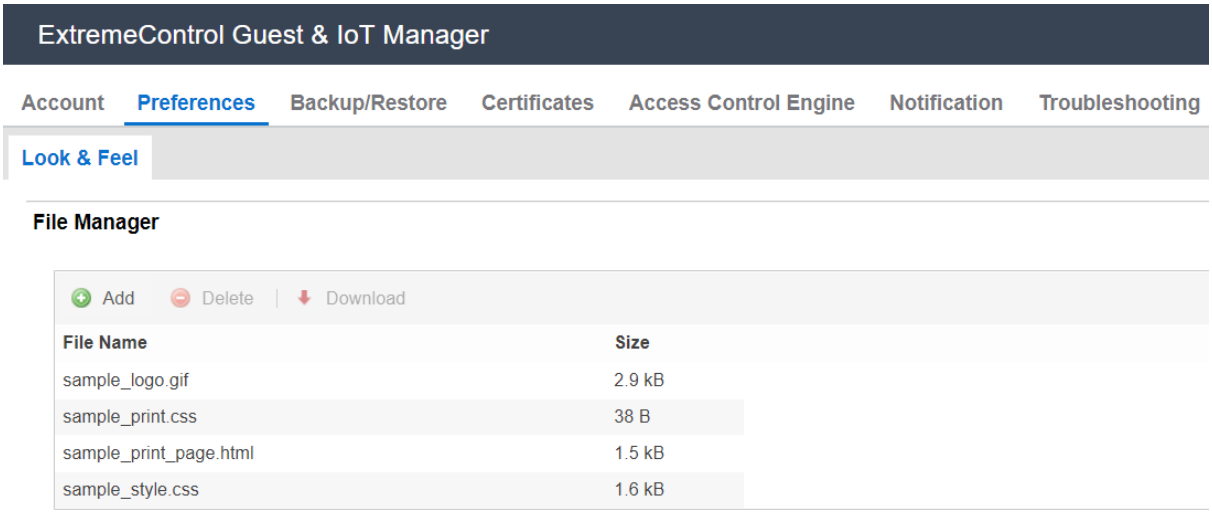
Use this procedure to upload a file and customize the printer friendly page.

Procedure

1. In the navigation pane, click **Administration** > **Preferences** tab.
2. In the **File Manager** section, click **Add**.

   The Add File screen is displayed.

3. In the Add File screen, click **Browse** to navigate to the file you wish to upload.
4. Click **Upload**, to upload the files to the File Manager. The uploaded file can be used in Onboarding Template to customize the printer friendly page.



5. **(Optional)** Select the required file name from the displayed list and click **Download** to download the file.
6. **(Optional)** Select the required file(s) name from the displayed list and click **Delete** to delete existing uploaded file.

   Use Ctrl / Shift to select multiple records to delete. You cannot delete the file,

   - If the selected sample file is an HTML file and used in any of the Onboarding Template.
   - If the selected file is a default file.
7. Click **Save** to save the configuration or **Restore to Defaults** to cancel the changes and restore to default value.

Field Descriptions

Use the data in the following table to use the **File Manager** section.

Name	Description
Add File	Uploads the files to customize the printer friendly page. By default, the application is pre-installed with the following four samples: • `sample_print.css` • `sample_print_page.html` • `sample_style.css` • `sample_logo.gif` **Important:** Ensure that the total size of all the files is less than 10 MB, though there is no restriction on number of files in File Manager.

Guest User Attributes:

Select the Guest User attributes that you want to display in the page by adding the following appropriate variables in the HTML file:

Attributes	Definition
`$username`	Displays the Guest User Name.
`$password`	Displays the Guest account password.
`$firstname`	Displays the Guest first name.
`$lastname`	Displays the Guest last name.
`$email`	Displays the Guest email address.
`$mobilephone`	Displays the Guest mobile phone number.
`$starttime`	Displays the start time when the Guest account becomes usable.
`$endtime`	Displays the end time of the Guest account.
`$termsofuse`	Displays the terms of use text. For more information, see Terms of Use and / or Additional information to be included as part of guest account confirmation page on page 91.
`$usercustom1` to `$usercustom6`	Displays additional information required during user creation.

Note:

You can retrieve the uploaded External Images / CSS files from the File Manager by using the URL in the following format and also entering the actual file name in place of the file name variable:

```
/GIM/uploads/<file_name>
```

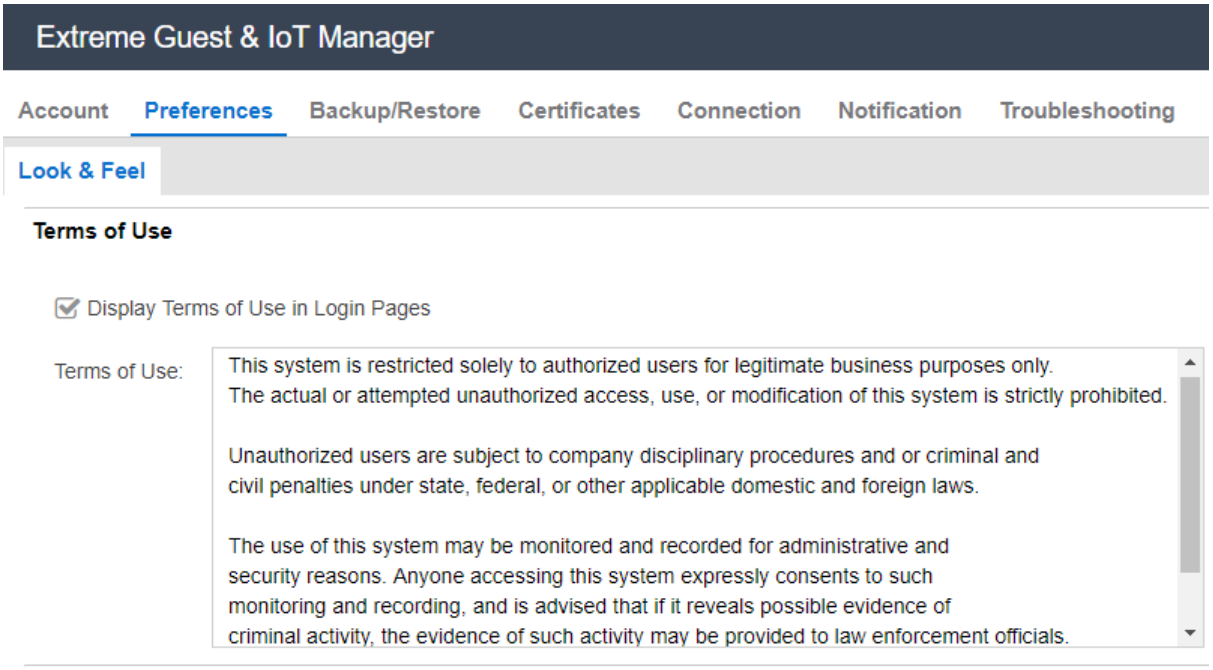
```
Sample: <img src="/GIM/uploads/sample_logo.gif">
```

Configuring Terms of Use

Use this procedure to configure Terms of Use to be displayed on the login page.

Procedure

1. In the navigation pane, click **Administration** > **Preferences** tab.
2. In the **Terms of Use** section, select **Display Terms of Use in Login Pages** to display the terms of use information on the login page. By default, this is selected.



3. **(Optional)** Edit the default text given in the **Terms of Use** section as its a free form text box.
4. Click **Save** to save the configuration or **Restore to Defaults** to cancel the changes and restore to default value.

Configuring Privacy Policy

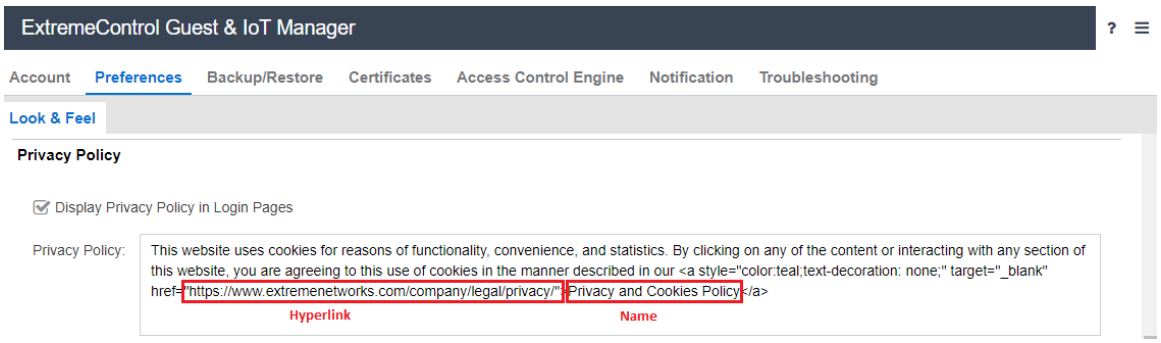
Use this procedure to configure Privacy Policy to be displayed on the login page.

Procedure

1. In the navigation pane, click **Administration** > **Preferences** tab.
2. In the **Privacy Policy** field enter the required privacy policy information.
3. **(Optional)** Edit the default text given in the **Privacy Policy** field as it is a free form text box.

Note:

You can change the privacy policy hyper link inside the “href” tag, if required. You can also change the name specified for the hyperlink on need basis.



4. Click **Save** to save the configuration or **Restore to Defaults** to cancel the changes and restore to default value.

Backup and Restore Configurations

The **Backup / Restore** tab in the Administration menu allows you to backup and restore Guest and IoT Manager configurations. This capability enables you to port the configurations between multiple Guest and IoT Manager deployments.

The configurations you can backup and restore include:

- Access Control Engine configurations
- RADIUS configurations
- Root certificates
- HTTPD Web server configuration (HTTP, HTTPD Certificates, SSL, and so on)
- Configuration such as SMTP, SMS Gateway, SMS Provider and files that are present in the File Manager.

Note:

Guest Users, Devices, Provisioners, Self-Service Provisioner, and Onboarding Templates configurations are stored on the Extreme Management Center database for corresponding Guest and IoT Manager domain and are not part of the Guest and IoT Manager backup / restore operations.

You can only store a maximum of 25 backup configurations per Guest and IoT Manager domain.

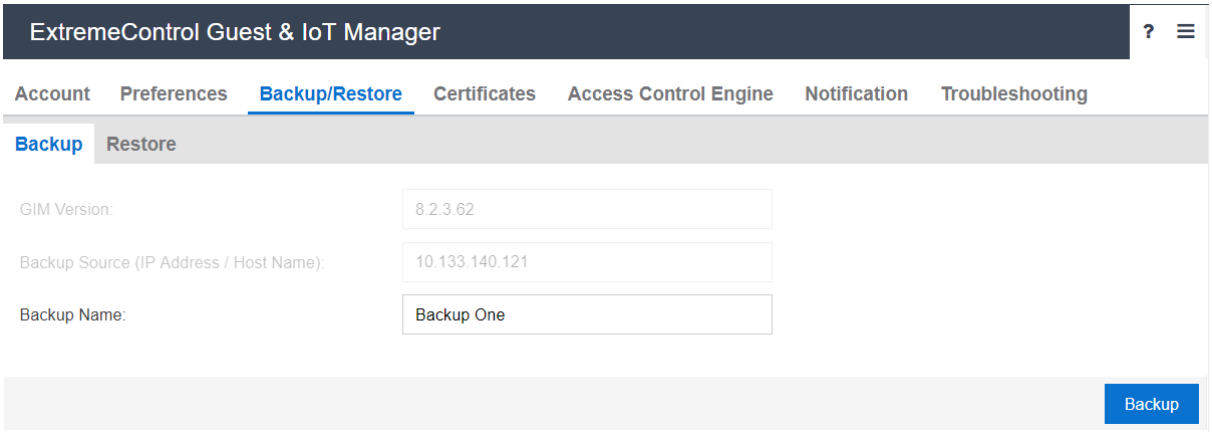
Storing Backup Configuration

Use this procedure to backup the configurations.

Procedure

1. In the navigation pane, click **Administration** > **Backup / Restore** tab.

   By default, the Backup screen is displayed along with Application Version and IP Address / Host Name.



2. In the **Backup Name** field, enter the name of the file.
3. Click **Backup** to save the local configurations.

Field Descriptions

Use the data in the following table to use the Backup screen.

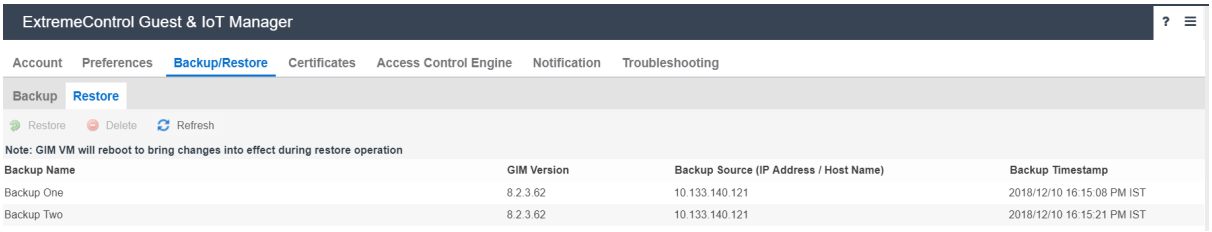
Name	Description
GIM Version	Displays the Guest and IoT Manager Application version number.
IP Address / Host Name	Displays the IP address / Host name of the Guest and IoT Manager Application for readability.
Backup Name	Configures the name of the backup file. When you specify the name for the backup file, it will be saved with the same unique name and will be displayed in the Restore screen.

Restoring Configuration

Use this procedure to restore the configurations.

Procedure

1. In the navigation pane, click **Administration** > **Backup / Restore** tab.
2. Click **Restore**. The Restore screen displays all the available backup configurations in the Restore screen along with Application Version, IP Address / Host Name and Backup Timestamp details.



3. Select the required backup file, and click **Restore**.

   The Restore confirmation message is displayed requesting whether to restore the network configuration.

4. In the Restore screen, do the following:
   a. Click **Yes**, to include network configuration while restoring the backup configuration.

      Network configuration includes:

      - Interface IP addresses and subnet masks.
      - Static routes.
      - DNS IP addresses and domain.

   b. Click **No**, to restore the configuration without network configuration.
   c. Click **Cancel**, to cancel the operation.

      Note:

      The Guest and IoT Manager Application automatically reboots the Virtual Appliance.

5. **(Optional)** Select the required backup(s) and click **Delete** to clear the added backup file. You will be asked to confirm the deletion.

   Tip:

   Use Ctrl / Shift to select multiple records to delete.

6. **(Optional)** Click **Refresh** to display the most recent changes.

Managing HTTPD Certificates

The **Certificates** tab in the Administration menu allows you to add, bind, or delete a certificate or key.

Adding a Certificate

Use this procedure to add a new certificate.

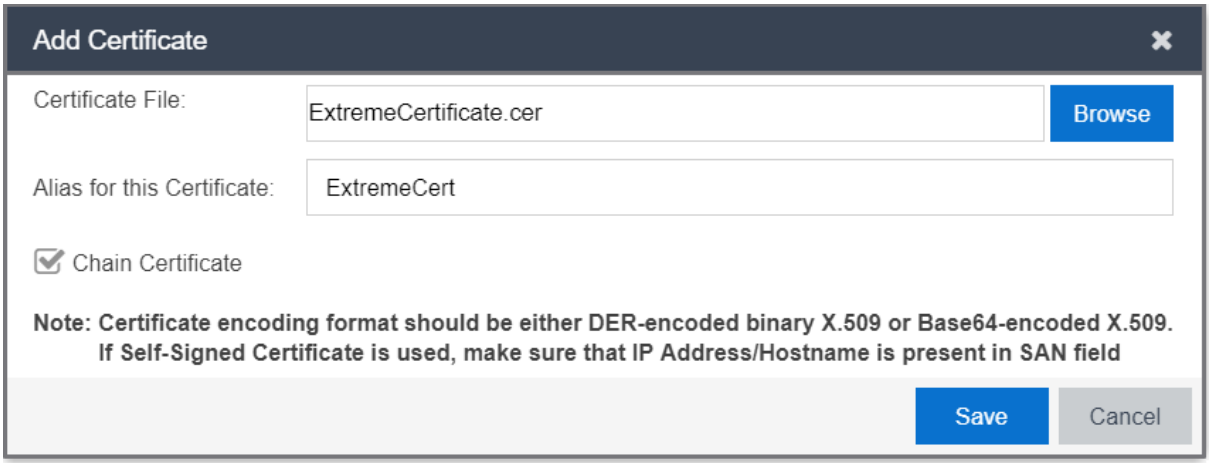
Procedure

1. In the navigation pane, click **Administration** > **Certificates** tab.

   The Certificates screen is displayed.

2. In the Certificates screen, click **Add** > **Add Certificate** to add a new certificate.

   The Add Certificate screen is displayed.



3. In the **Certificate File** field, click **Browse** to select the certificate from the local folder and click **Open** to upload.
4. In the **Alias for this Certification** field, enter the alias name to assign another name for the selected new certificate.
5. Select **Chain Certificate** checkbox to upload a chain certificate.
6. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   The added certificate and chain certificate details are displayed in the certificates table.

7. **(Optional)** Select the required certificate(s) and click **Delete** to remove certificates.

   Tip:

   Active and default certificates cannot be deleted.

   Use Ctrl / Shift to select multiple records to delete.

Field Descriptions

Use the data in the following table to use the Add Certificate screen.

Name	Description
Certificate File	Configures a new certificate for the application. This must be one of the following: • DER encoded binary X.509 file containing the certificate.

Table continues…

Name	Description
	• Base64 encoded file containing the certificate.
Alias for this certificate	Configures a unique string to identify the key entry of the certificate.
Chain Certificates	Uploads a chain certificate. A chain certificate 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.

Adding a Key

Use this procedure to add a new private key.

Procedure

1. In the navigation pane, click **Administration** > **Certificates** tab.

   The Certificates screen is displayed.

2. In the Certificates screen, click **Add** > **Add Key** to a new private key.

   The Add Private Key screen is displayed.

3. In the **Private Key File** field, click **Browse** to select the private key from the local folder and click **Open** to upload.
4. In the **Passpharse** field, enter the passphase for the selected private key.
5. In the **Alias for this Key** field, enter the alias name to assign another name for the selected new key.
6. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   The added private key details are displayed in the certificates table.

7. **(Optional)** Select the required private key(s) and click **Delete**, to remove keys.

   Tip:

   Active and default private keys cannot be deleted.

Use Ctrl / Shift to select multiple records to delete.

Field Descriptions

Use the data in the following table to use the Add Private Key screen.

Name	Description
Private Key File	Configures a new private key for the certificate to encrypt messages intended for a particular recipient. These messages can be deciphered only by using the defined private key.
Passpharse	Configures the passphrase that needs to be used to decrypt the file containing the private key. If the private key is not encrypted, leave this field blank.
Alias for this Key	Configures a unique string to identify the key entry of the certificate which you intend to use.

Binding a Certificate

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

Before you begin

Ensure that you have a added a certificate to the application and the same is listed in the **Administration** > **Certificates** table.

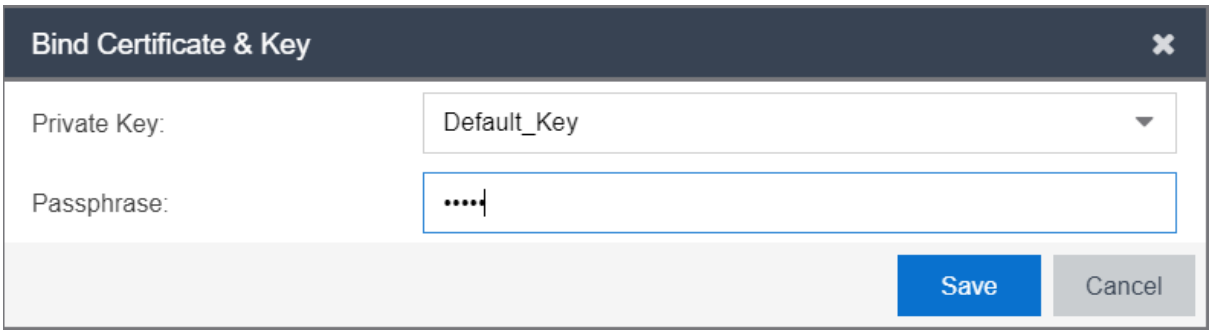
Procedure

1. In the navigation pane, click **Administration** > **Certificates** tab.

   The added certificates, chain certificates, and private key are displayed along with the name and type details.

2. Select the required certificate you want to bind in the **Name** column.
3. Click **Bind** and select **Bind Certificate** from the drop-down list.

   The Bind Certificate and Key screen is displayed.



Note:

Bind Certificate option in the drop-down list is disabled, if you select a incorrect certificate.

4. In the **Private Key** field, select the required key from the drop-down list.
5. **(Optional)** In the **Passpharse** field, enter the passphase for the selected private key.
6. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Field Descriptions

Use the data in the following table to use the Bind Certificate screen.

Name	Description
Private Key	Specifies a new private key for the certificate to encrypt messages intended for a particular recipient. These messages can be decoded only by using the defined private key.
Passpharse	Configures the passphrase that needs to be used to encrypt the file containing the private key. If the private key is not encrypted, leave this field blank. **Note:** Ensure that you provide the valid passphrase, so that the bind does not fail and result in HTTPD restart failure.

Binding a Chain

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

Before you begin

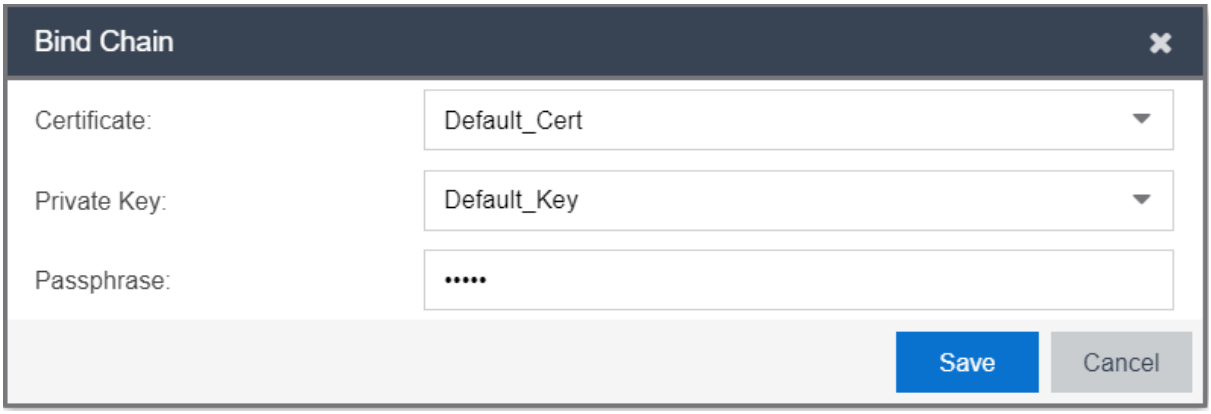
Ensure that you have a added a chain certificate to the application and the same is listed in the **Administration** > **Certificates** table.

Procedure

1. In the navigation pane, click **Administration** > **Certificates** tab.

   The added certificates, chain certificates, and private key are displayed along with the name and type details.
2. Select the required chain certificate you want to bind in the **Name** column.
3. Click **Bind** and select **Bind Chain** from the drop-down list.

   The Bind Chain screen is displayed.



Note:

If a chain certificate is not selected, **Bind Chain** option in the drop-down list is disabled.

4. In the **Certificate** field, select the required certificate from the drop-down list.
5. In the **Private Key** field, select the required private key from the drop-down list.
6. **(Optional)** In the **Passpharse** field, enter the required passpharse for the selected certificate and private key.
7. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Field Descriptions

Use the data in the following table to use the Bind Chain screen.

Name	Description
Certificates	Specifies the available certificates for selection.
Private Key File	Specifies a new private key for the certificate to encrypt messages intended for a particular recipient. These messages can be decoded only by using the defined private key.
Passpharse	Configures the passphrase that needs to be used to encrypt the file containing the private key. If the private key is not encrypted, leave this field blank. **Note:** Ensure that you provide the valid passphrase, so that the bind does not fail and result in HTTPD restart failure.

Managing Access Control Engine

The **Access Control Engine** tab in the Administrator menu supports the Guest and IoT Manager Application to configure Access Control Engine.

Important:

Guest and IoT Manager does not automatically connect to the Access Control Engine upon start-up. You need to configure the Access Control Engine providing the necessary details. And also, Guest and IoT Manager *need not* be connected to allow Guest Users to use their accounts.

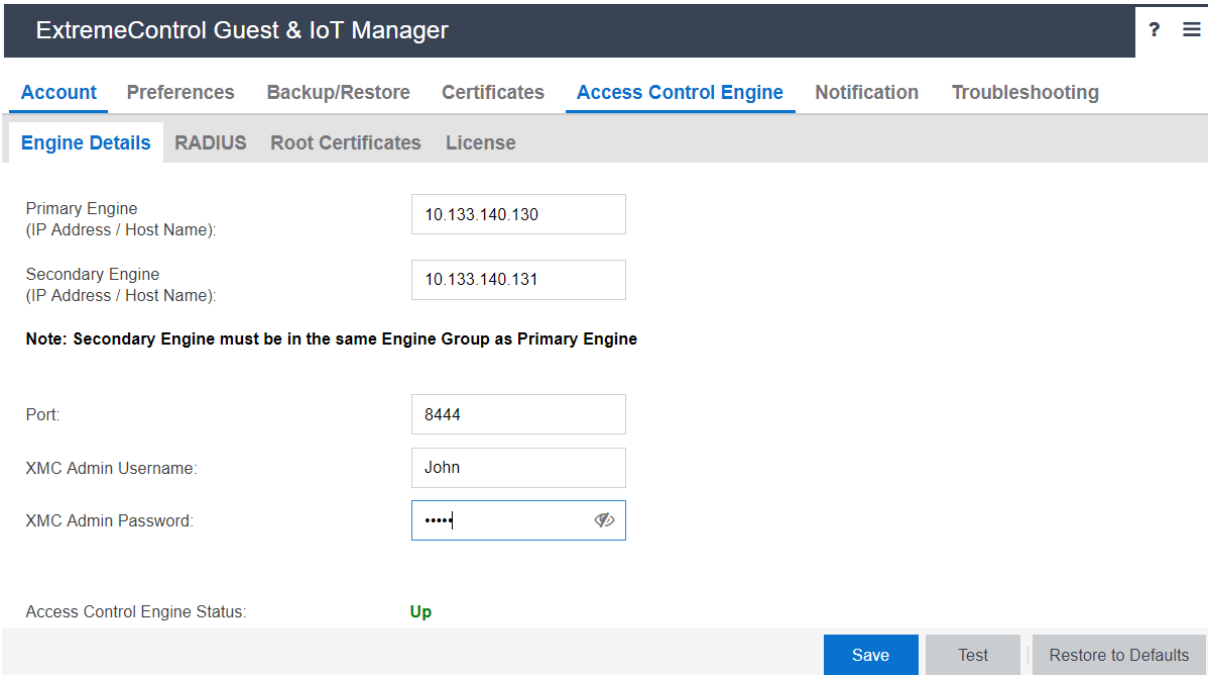
Configuring Engine Details

Use this procedure to configure Guest and IoT Manager to Access Control Engine.

Procedure

1. In the navigation pane, click **Administration** > **Access Control Engine** tab.

   The Engine Details screen is displayed.



2. In the **Primary Engine** field, enter the IP address or host name of Access Control Engine.
3. **(Optional)** In the **Secondary Engine** field, enter the IP address or host name of any other Access Control Engine which is part of the same Engine Group as the Primary Engine.
4. In the **Port** field, enter the port number used for communicating with the Access Control Engine.
5. Enter the **XMC Admin Username** and **XMC Admin Password** of the Extreme Management Center administrative user having appropriate Guest and IoT Manager read / write access capability.

6. Click **Save** to store the valid configuration in Guest and IoT Manager Application.

   Note:

   The Guest and IoT Manager uses this configuration to establish connection with the Access Control Engine.

   In the absence of these settings, Guest and IoT Manager is no longer connected to Provisioner and Self-Service Provisioning Application.

7. **(Optional)** Click **Test** to verify the Access Control Engine configuration.

   The successful / failure test configuration message is displayed.

8. **(Optional)** Click **Restore to Defaults** to reset the configuration to default.

Field Descriptions

Use the data in the following table to use the Engine Details screen.

Name	Description
Primary Engine	Configures the Primary Control Engine IP address / host name of the Access Control Engine.
Secondary Engine	**Optional**: Configures Secondary Control Engine IP address / host name for the Access Control Engine. When the primary appliance goes down the application switches to secondary appliances and vice verse with a maximum down time of 10 seconds.
Port	Configures the Access Control Engine port number to identify a specific process to which the connections needs to be forwarded when it arrives at a server. By default, the proxy value 8444 is displayed.
XMC Admin Username and XMC Admin Password	Specifies the Username and Password of the Extreme Management Center administrative user which has Guest and IoT Manager Application read / write access.

Configuring RADIUS Settings

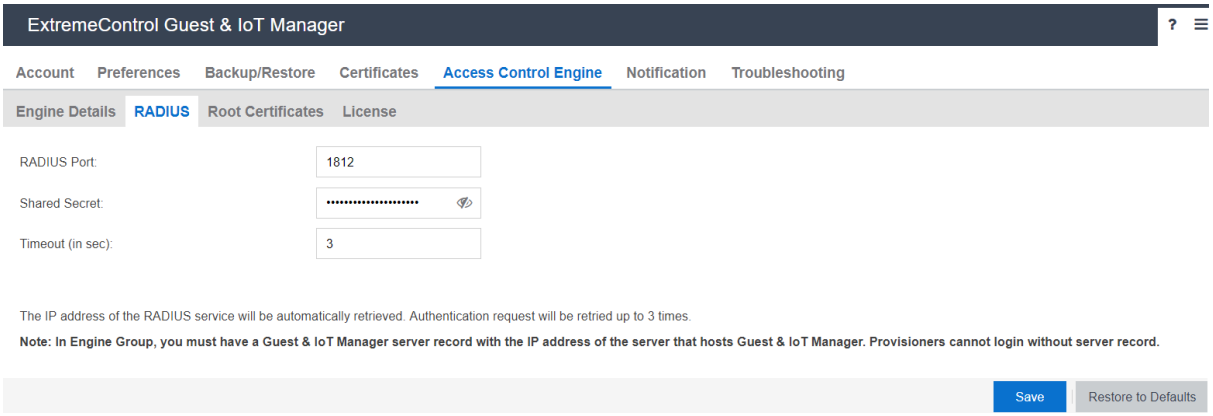
Use this procedure to specify the RADIUS settings in Guest and IoT Manager Application.

For more information on RADUIS settings, see Guest and IoT Manager Configuration Document in Extreme Management Center.

Procedure

1. In the navigation pane, click **Administration** > **Access Control Engine** tab.
2. Click **RADIUS**.

   The RADIUS screen is displayed.



3. In the **RADIUS Port** field, enter the port number for authentication request.
4. In the **Shared Secret** field, enter the pre shared key to establish the connection.
5. In the **Timeout** field, enter the period in seconds.
6. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   In Engine Group, you must have a Guest and IoT Manager Server record with the IP address of the Server that hosts Guest and IoT Manager. Provisioners cannot login without Server record.

Field Descriptions

Use the data in the following table to use the RADIUS screen.

Name	Description
RADIUS Port	Configures the RADIUS port number where the Access Control Engine is running for centralized Authentication, Authorization, and Accounting (AAA) network access management. The default number is 1812. Access Control Engine uses RADIUS to authenticate Provisioners.
Shared Secret	Configures the proof of identity for authentication. The Shared Secret can be randomly selected bytes. The default shared secret is : `ETS_TAG_SHARED_SECRET`
Timeout (in sec)	Configures the maximum length of time in seconds to wait (for the real-time), so that Guest and IoT Manager Application retires the RADUIS login. If **No** Response, the application displays an error message. The default is 3 seconds.

Adding Root Certificate

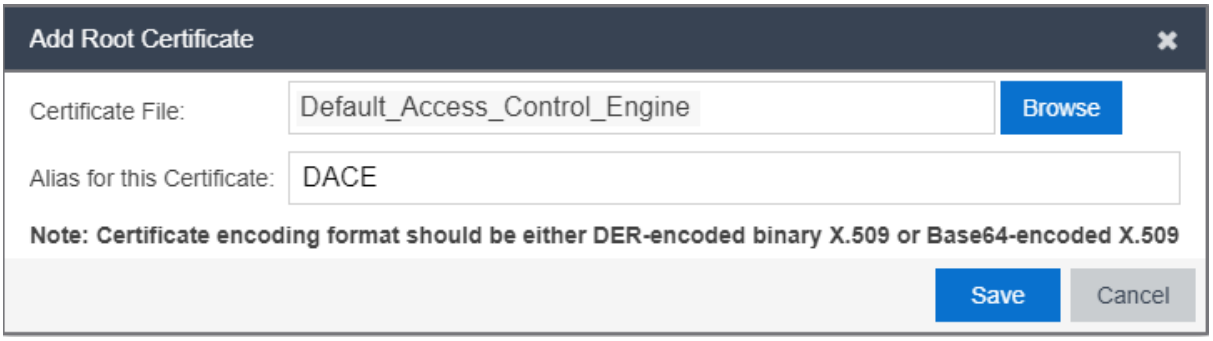
Use this procedure to add a new Root Certificate.

See How to Update Extreme Access Control Engine Server Certificates in Extreme Management Center for more information on how to replace the server certificates used by the Extreme Access Control Engine.

Procedure

1. In the navigation pane, click **Administration** > **Access Control Engine** tab.
2. Click **Root Certificates** > **Add**, to add a new certificate.

   The Add Root Certificate screen is displayed.



3. In the **Certificate File** field, click **Browse** to select the certificate from the local folder and click **Open** to upload.
4. In the **Alias for this Certification** field, enter the alias name to assign another name for the selected new certificate.
5. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   The added Root Certificate details are displayed in the Root Certificates table and **Update Trust Mode** is enabled.
6. Click **Trust Mode**.

   There are two options under the **Update Trust Mode**:

   a. Select **All server certificates are accepted**. By default, this option is selected where all the server certificates are accepted. However, the Trust Mode gets highlighted in RED.

   b. Select **Any untrusted server certificate is rejected** so that the certificate from the server is validated against the root certificates available in Guest and IoT Manager. The untrusted certificates are rejected if the identity is not verified. We recommend this as the safest option to be selected.

   c. Click **Save** to save the configuration or click **Cancel** to cancel the changes.
7. **(Optional)** Select the required Root Certificate(s) and click **Delete** to remove the certificates.

   Tip:

   Use Ctrl / Shift to select multiple records to delete.

Field Descriptions

Use the data in the following table to use the Add Root Certificate screen.

Name	Description
Certificate File	Adds a new Root Certificate for the application. The certificate file must contain PEM-encoded certificate. Make sure that the certificate does not have a password associated with it. The certificate encoding format must be any one of the following format. **Note:** • DER encoded binary X.509 file containing the certificate. • Base64 encoded file containing both the certificate and the private key.
Alias for this certificate	Configures a short unique string to identify the key entry of the Root Certificate in the keystore. You can use any name; Access Control Engine uses this Alias name as a key to identify the certificate in the keystore. All 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.

Viewing License Status

When you deploy Guest and IoT Manager for the first time, ensure that a valid Guest and IoT Manager license is added and enforced in Extreme Management Center so that Access Control Engine details can be configured in Guest and IoT Manager. For more information, see Configuring Engine Details on page 49.

If the license is expired:

- License status is displayed as "*Not Installed / Expired*".
- Provisioner users are logged out including Outlook Provisioner and all the configured self-services become non-operational.
- Valid new license needs to be added again to function.

Different License Status

Scenario	License Status
When engine details not configured	Not Available
Invalid Credentials	Not Available
Not compatible	Not Available
Not Reachable	Not Available

Table continues…

Scenario	License Status
Not Trusted	Not Available
Reachable and valid license present	Valid
Reachable and there is no valid license present	Not Installed / Expired

For more information on Server License, see Diagnostics in Extreme Management Center.

Note:

When the connection fails from Guest and IoT Manager to Access Control Engine, the system waits for a minute and if the connection does not restore, all the configured self-services become non-operational.

When the connection restores, all the services are reactivated automatically.

Setting Notification Parameters

The **Notification** tab in the Administrator menu specifies the Email and SMS configuration that are used to notify the Guest Users created by the Provisioners. The usual way to provide the credentials (User Name and Password) is through email. Alternatively, the Administrator can send the credentials in an email to the front desk personnel who can pass them to the Guest as a hard copy.

For more information, see Enabling E-mail Notification on page 55.

The Administrator can also configure the application to send the credentials via an SMS text message to the mobile phone. The configured carrier Gateway / Provider communicate with the Guest and IoT Manager on how to send the messages.

For more information, see Adding SMS Gateway on page 57 and Adding SMS Provider on page 59.

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.

Google blocks sign-in attempts from unknown sources. To avoid this issue, you need to allow access to apps to get authenticated. You can 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 Let less secure apps access your account.

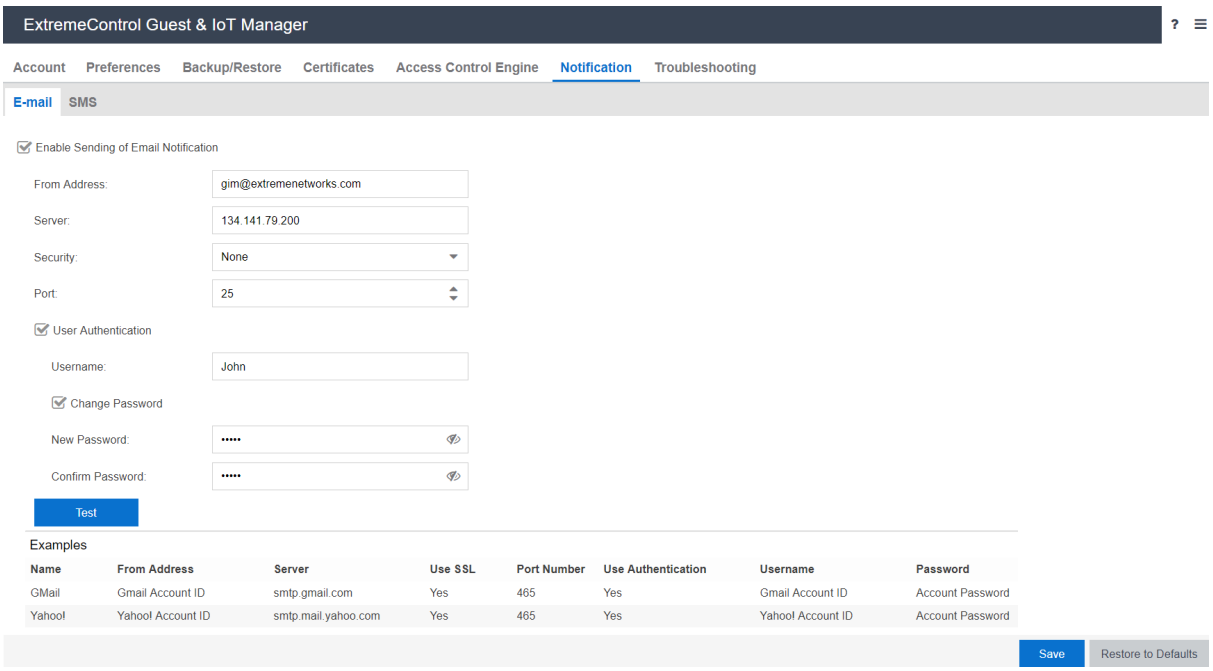
Enabling E-mail Notification

Use this procedure to configure SMTP email settings.

Procedure

1. In the navigation pane, click **Administration** > **Notification** tab.

   By default, the E-mail screen is displayed.



2. In the E-mail screen, select the **Enable Sending of Email Notification** checkbox to configure SMTP.
3. In the **From Address** field, enter the email address that needs to be displayed in the “From” line of the messages that application sends.
4. In the **Server** field, enter the fully-qualified domain name or the IP address.
5. In the **Security** field. select **None**, **SSL/TLS** or **STARTTLS** options from the drop-down list.

   By default, **None** option is selected to process email with Non-SSL connections.

   If you select **STARTTLS** option, enter the port number to send the encrypted email.

If you select **SSL/TLS** option, the **SSL Certificate** field is enabled. You can perform the following:

a. Select **System** option from the **SSL Certificate** field drop-down list, to use the known Root Certificates that are shipped along with Guest and IoT Manager Application.

b. Select **Custom** option from the **SSL Certificate** field drop-down list to import the SMTP server certificate specified in **Administration** > **Connection** > **Certificate** tab. When you successfully import the certificate, this certificate is used to establish trust with the SMTP server.

6. In the **Port** field, enter the SMTP port number.
7. **(Optional)** Select **User Authentication** checkbox, if your SMTP server requires authentication.

   The **User Name** and **Change Password** fields are enabled.

   a. Enter the login credentials of SMTP server user in the **Username** field.

   b. Select **Change Password** checkbox, to modify the password details.

8. **(Optional)** Click **Test** to verify that the application can reach the server using the specified email address before saving the configuration.

   The Test SMTP Configuration screen is displayed.

   a. Enter the sample email address in the **Test Destination Email** field.

   b. Click **Send Test Email** to send the email or click **Cancel** to cancel the operation.

   Note:

   Ensure that you set up an appropriate email notification template. For more information, see Configuring the Account Notification Templates on page 89.

9. Click **Save** to save the configuration or **Clear** to clear the configuration.

   For more information, sample email domains are listed as examples in the E-mail screen beneath frame. For example, Yahoo, Gmail, and so on.

Field Descriptions

Use the data in the following table to use the E-mail screen.

Name	Description
Enable Sending of Email Notification	Configures the Application to send Guest Users, Provisioners, and / or others an email notification, when Guest User accounts are created and / or updated.
From Address	Configures email address that needs to be displayed in the “From” line of the messages. For example, user provisioning notifications contains a **From Address** such as `guestreception@extremenetworks.com`.

Table continues…

Name	Description
	This address appears in all types of emails that Guest and IoT Manager Application sends.
Server	Configures the domain name or the IP address assigned to the mail server that transmits email notifications from the application. The SMTP server name can be an email address. You can enter a public mail server such as Gmail or Yahoo as the SMTP server.
Security	Specifies **SSL/TLS** and **STARTTLS** options.
SSL Certificate	Specifies **System** and **Custom** options. • **System**: Uses the shipped Root Certificate to establish trust with the SMTP server. If the application fails to establish trust, the email functionality does not work. • **Custom**: Fetches the custom SMTP server certificates that are binded in the Application. For more information, see Binding a Certificate on page 46. Upon successful import this certificate is used to establish trust with SMTP server.
Port	Configures the SMTP port number to be used by the application for the SSL connection.
Username	Specifies the login name of the SMTP server user.
New Password and Confirm Password	Configures a new password for the account.
Test Destination Email	Verifies the SMTP settings by sending the sample email.

Configuring SMS Gateway / Provider

The Administrator can perform the following procedure to send the login credentials to Guest Users.

- Adding SMS Gateway on page 57
- Adding SMS Provider on page 59
- Modifying SMS Gateways / Providers on page 61

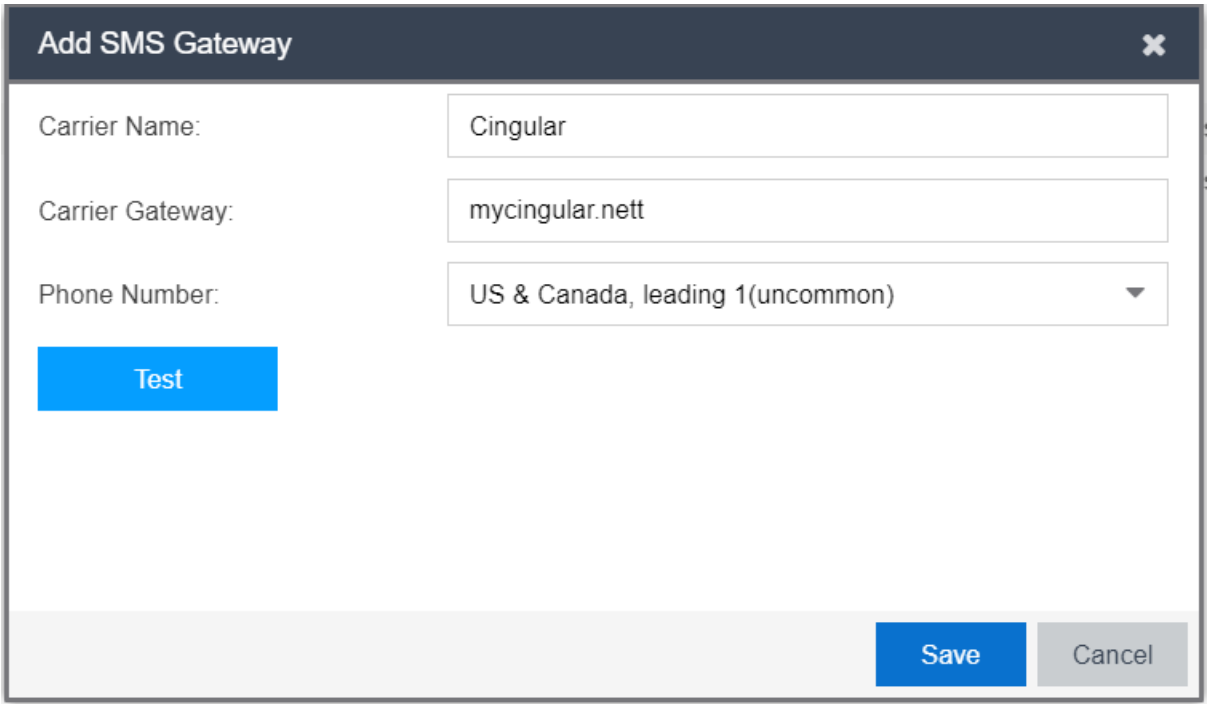
Adding SMS Gateway

Use this procedure to configure carrier gateways settings to send SMS messages to mobile service providers.

Procedure

1. In the navigation pane, click **Administration** > **Notification** > **SMS** tab.
2. Click **Add** and select **Add SMS Gateway** option from the drop-down list.

   The Add SMS Gateway screen is displayed.



3. In the **Carrier Name** field, enter the name of the carrier.
4. In the **Carrier Gateway** field, enter the carrier gateway address.
5. In the **Phone Number** field, select the required calling options from the drop-down list.
6. Click **Test** to test the added gateway service configuration.

   The Test Gateway Configuration screen is displayed.

   a. Enter the phone number in the **Test Destination Mobile Number** field.

   b. Click **Send Test SMS** to send the SMS or click **Close** to close the screen.

   Note:

   Ensure that you set up an appropriate email notification template. For more information, see Configuring the Account Notification Templates on page 89.
7. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   The added carrier gateways details are displayed in the SMS Gateway screen along with *Phone Carrier* and *Gateway* details.
8. **(Optional)** Select the required added carrier gateway and click **Set as default** option in the **SMS Gateway** screen.

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

Note:

The first SMS gateway is always a default gateway. You can select the required gateway and Set as default, if required.

9. **(Optional)** Select the required added carrier and click **Edit** to modify the SMS gateway. For more information, see Modifying SMS Gateways / Providers on page 61
10. **(Optional)** Select the required added carrier gateway(s) and click **Delete** option in the **SMS Gateway** screen to clear the added carrier service. You will be asked to confirm the deletion.

Tip:

Use Ctrl / Shift to select multiple records to delete.

Field Descriptions

Use the data in the following table to use the Add SMS Gateway screen.

Name	Description
Carrier Name	Configures the carrier service provider name. It is mandatory to configure a gateway for each mobile phone provider to whom the application sends the Guest User login details.
Carrier Gateway	Configures the carrier gateway address to send SMS text messages.
Phone Number	Specifies the phone number format of the selected country. If you select specify length option from the drop-down list, the **Digits (single number or range. For example, 10 — 15)** field is enabled.
Digits (single number or range. For example, 10 — 15)	Configures the number range for the phone number input field.
Test Destination Mobile Number	Verifies the SMS configuration by sending a sample SMS to the specified mobile number.

Adding SMS Provider

Use this procedure to configure Clickatell gateways settings to send bulk SMS messages to mobile service providers.

Before you begin

Ensure that you have completed Clickatell registration and have activated your account ID. The account activation email received includes User ID and Email address information.

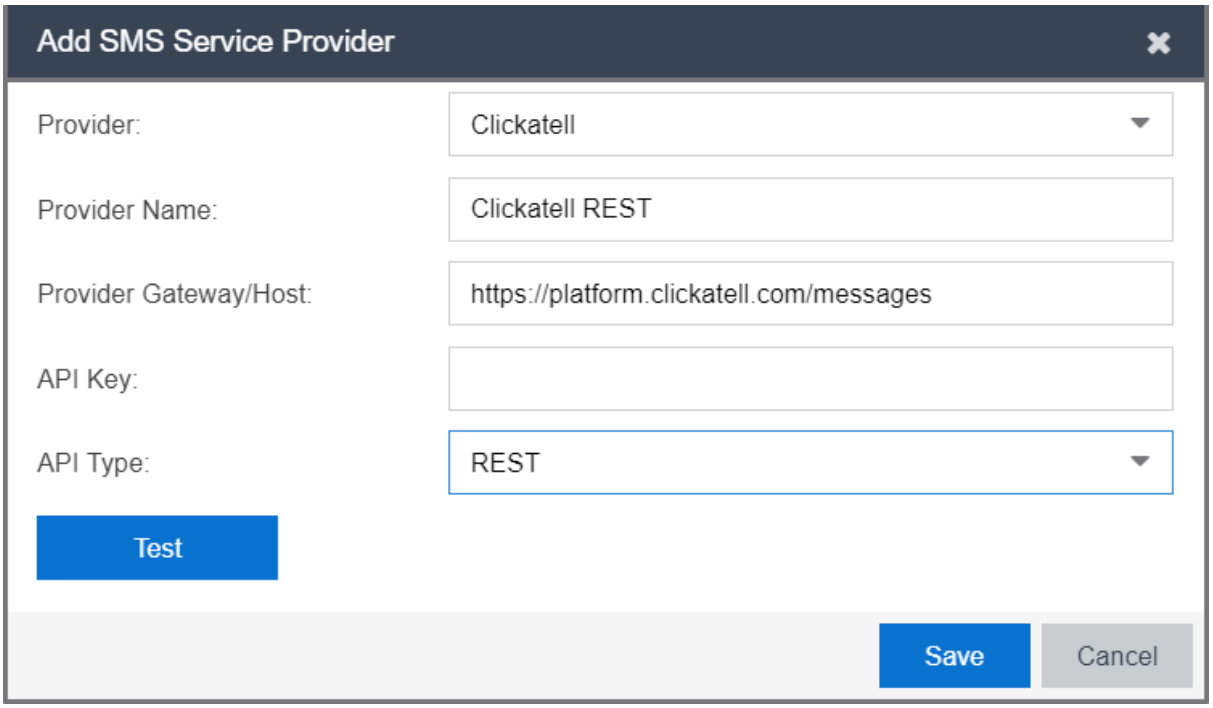
Note:

If Do not Disturb (DND) service is enabled in your mobile network, you will not be able to receive any SMS notification.

Procedure

1. In the navigation pane, click **Administration** > **Notification** > **SMS** tab.
2. Click **Add** and select **Add SMS Provider** option from the drop-down list.

The Add SMS Provider screen is displayed.



3. In **Provider** field, select the name of the provider.

   Currently, Clickatell is the only available service provider.
4. In the **Provider Name** field, enter the name of the provider.
5. In the **Provider Gateway / Host** field, check the available URL details.

   The value displayed in this field is based on the option selected in the **API Type** field.
6. In the **API Key** field, enter the key details obtained from Clickatell.
7. In the **API Type** field, select the type from the drop-down list.

   By default, **REST** option is selected.
8. Click **Test**, to test the added gateway services configuration.

   The Test Gateway Configuration screen is displayed.
9. In the Add SMS Provider screen, do the following:
   a. Enter the phone number in the **Test Destination Mobile Number** field.
   b. Click **Send Test SMS** to send the SMS or click **Close** to close the screen.
10. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

    The added provider gateways details are displayed in the SMS Gateway screen along with *Phone Provider*, *Provider Gateway* and *Protocol (REST / HTTP)* details.
11. Select the required added provider gateway and click **Set as default** option in the **SMS Gateway** screen.

12. **(Optional)** Select the required added carrier and click **Edit** to modify the SMS provider. For more information, see Modifying SMS Gateways / Providers on page 61
13. **(Optional)** Select the required added provider gateway(s) and click **Delete** option in the **SMS Gateway** screen to clear the added provider service. You will be asked to confirm the deletion.

Tip:

Use Ctrl / Shift to select multiple records to delete.

Field Descriptions

Use the data in the following table to use the Add SMS Provider screen.

Name	Description
Provider	Specifies the list of Providers. Currently, Clickatell is the only available service provider.
Provider Name	Configures the Provider name.
Provider Gateway / Host	Specifies the URL information. The default value for **Provider Gateway / Host** field is provided for both **REST** and **HTTP API** types.
API Key	Configures the API key. You need to copy the API key from Clickatell account. (`https://portal.clickatell.com/#/login`)
API Type	Specifies the API type available for the selected service provider. The options available are: • **REST** • **HTTP**

Modifying SMS Gateways / Providers

Use this procedure to modify SMS Gateways / Providers.

Procedure

1. In the navigation pane, click **Administration** > **Notification** tab.
2. Click **SMS** tab. The added carrier / provider gateway details are displayed in the SMS screen along with *Phone Carrier*, *Gateway* and *Protocol (HTTP / REST)* details.
3. Select the required phone carrier / provider from the list.
4. Click **Edit** to view the carrier details.

Note:

You can also view by double-clicking the required phone carrier / provider from the list.

5. In the Edit SMS Gateway screen, modify the fields required. The fields are displayed based on the selected phone carrier / provider type.
6. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Troubleshooting

The **Troubleshooting** tab in the Administrator menu allows the Administrator to view the logs of Guest and IoT Manager application. The default name of the log file is : `GIM_Version_log_IP_Date_Time.log`.

For more information, see Viewing the Log Files on page 62.

For any debugging issues in the Guest and IoT Manager Application, Administrator can generate a show support file that Extreme support staff can use to diagnose the problem.

For more information, see Generating a Show Support File on page 63.

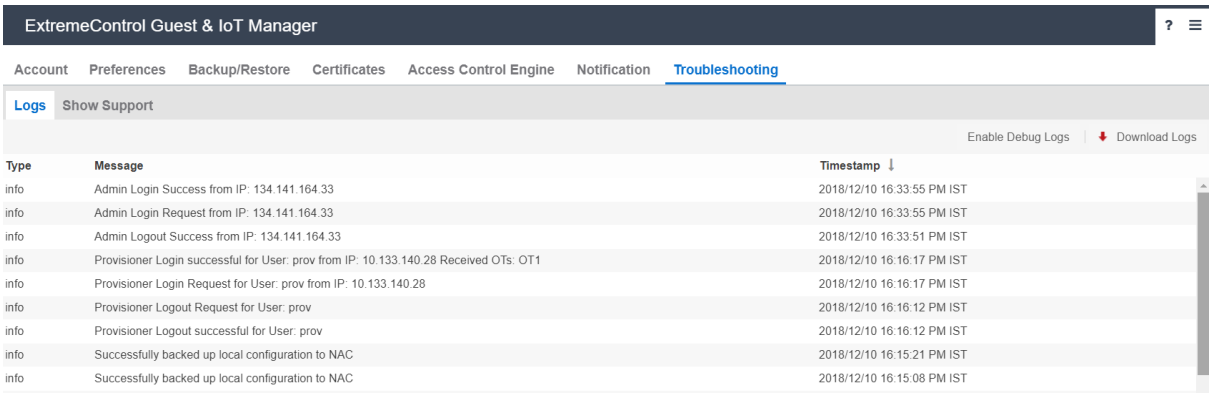
Viewing the Log Files

Use this procedure to view the log files.

Procedure

1. In the navigation pane, click **Administration** > **Troubleshooting** tab.

   By default, the Logs screen is displayed along with Types (Info, Error) Message and Timestamp details.



2. Click **Enable Debug Logs** to view the logs of type "**debug**". By default, the debug logs are disabled.
3. **(Optional)** Click **Download Logs** to store and view the logs from the local drive.

Note:

The log file size is 10 MB. If the size exceeds more than 10 MB, then roll over of log file occurs.

4. Click the **Page Numbers** arrow at the bottom of the screen to page through the files.
5. Click the **Refresh** icon to reload the page being viewed with most recent generated logs.

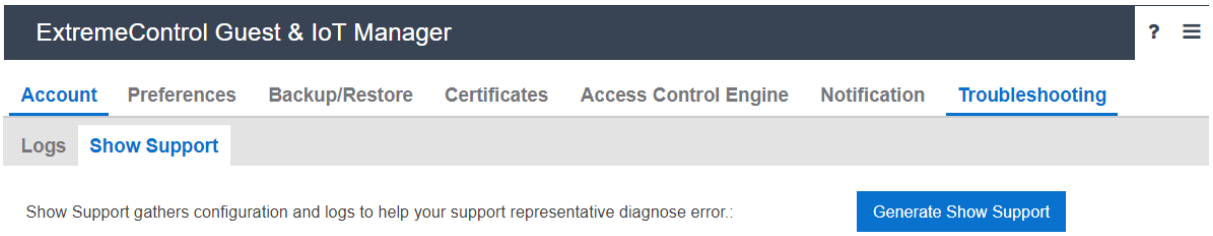
Generating a Show Support File

Use this procedure to generate a show support file for debugging the issues.

Procedure

1. In the navigation pane, click **Administration** > **Troubleshooting** tab.
2. Click **Show Support** tab.

   The Show Support screen is displayed.



3. In the Show Support screen, click **Generate Show Support** to download the zip file.
4. Save the Guest and IoT Manager show support zip file to an appropriate location and contact Extreme Networks technical support.

Note:

For more information about troubleshooting, see Troubleshooting and FAQs on page 169

Chapter 6: Configuring Onboarding Template

This module is intended for Guest and IoT Manager Administrator to create and manage Onboarding templates to be associated with Provisioner accounts.

The Guest and IoT Manager Administrator configures the Onboarding Template which specifies how Users / Devices can be onboarded by the Provisioner. Administrator can also configure Custom Attributes and Access Groups.

If you are a Provisioner, you may skip this section and proceed to *ExtremeControl Guest and IoT Manager Configuration*.

Creating an Onboarding Template

The **Onboarding Templates** tab in the Onboarding Templates menu is a collection of settings that establishes the administrative rights and account settings of the Provisioners that associate with it.

Use this procedure to create an Onboarding Template for each set of Provisioners that require a unique set of rules for creating Guest Users account / Device records. Every Provisioner must belong to at least one Onboarding Template.

Before you begin

Login to the Guest and IoT Manager application and ensure that it is connected with the Access Control Engine. For more information, see Configuring Engine Details on page 49.

Procedure

1. In the navigation pane, click **Onboarding Templates** > **Add**.
2. In the **Common** tab, configure the name and common details for the Onboarding Template. For more information, see Configuring the Common Details on page 65.
3. In the **Guest Users** tab, configure the Guest User and Outlook Add-in account details. For more information, see Configuring the Guest User Account Details on page 68 and Configuring Guest User Provisioning Using Outlook Add-in on page 76.

4. In the **Sponsor** tab, configure Sponsor approval, if Self-Service Guest Users must be approved by a Sponsor before they are granted access. For more information, see Configuring Sponsor Approval on page 74.
5. In the **Devices** tab, configure User Device details for this Onboarding Template. For more information, see Configuring the Devices Record Details on page 84.

   Important:

   If Sponsor Approval is configured, Provisioners belonging to this Onboarding Template cannot manage Devices.
6. In the **Device Type Groups** tab, configure the Device Type(s) and Group(s) for the particular Onboarding Template. For more information, see Configuring Device Type Groups on page 87.
7. In the **Notification** tab, configure the notification templates used for sending account details to Guest User / Sponsor. For more information, see Configuring the Account Notification Templates on page 89.
8. In the **Advanced** tab, configure the advanced details for this Onboarding Template if required. For more information, see Configuring Advanced Details on page 95.
9. Check your entries and click **Save** to save the configuration.

   Guest and IoT Manager creates the Onboarding Template.

   Note:

   For more information on modifying, copying and deleting Onboarding Templates, see Managing Onboarding Templates on page 97.

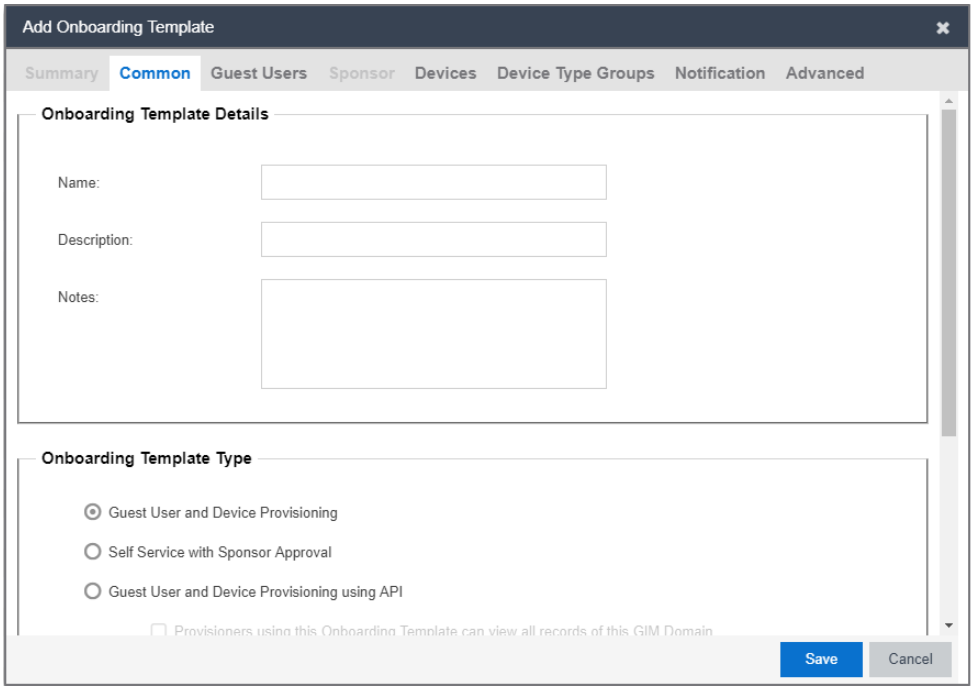
Configuring the Common Details

Use this procedure to configure common details for Onboarding Template.

Procedure

1. In the navigation pane, click **Onboarding Templates** > **Add** > **Common** tab.

   The Common screen is displayed.



2. In the **Onboarding Template Details** section, enter the name of the template, description, and any template related notes.
3. In the **Onboarding Template Type** section, select an option as required.

   Note:

   If Provisioners are associated with REST API or Outlook Onboarding Templates then they will not be able to create new Guest Uses and Devices. Only view option is visible.
4. Select **Provisioners belonging to this Onboarding Template can view and edit each other's records** checkbox to manage Guest User / Device accounts of all the Provisioners belonging to this Onboarding Template.
5. In the **Temporary Accounts Validity** section, enter the maximum account validity that can be granted to a Guest / Devices in minutes, hours, or days.
6. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Field Descriptions

Use the data in the following table to use the **Common** tab.

Name	Description
Onboarding Template Details	Configures the details of the Onboarding Template. • **Onboarding Template Name**: Configures the template name. The template name can be configured using alphanumeric / special

Table continues…

Name	Description
	characters and space between words. Only these special characters are allowed : # =()_-! [] • **Description**: Configures a short description of the Onboarding Template. The description is limited to 60 characters. • **Notes** : Configures any notes specific to the template. Only 250 characters are allowed.
Onboarding Template Type	Specifies the type of Onboarding Template. • **Guest User and Device Provisioning**: Creates an Onboarding Template that has Guest User and Device Provisioning rights. By default, this option is enabled. The tabs enabled are: - Guest User - Devices - Device Type Group - Notification - Advanced • **Self Service with Sponsor Approval**: Creates an Onboarding Template with Guest User Self-Provisioning rights with additional sponsor approval requirements. The tabs enabled are: - Guest User - Sponsor - Notification - Advanced • **Guest User and Device Provisioning using API** : Creates an Onboarding Template with Guest User and Device provisioning rights for thrid party APIs. The tabs enabled are: - Guest User - Devices - Device Type Group - Notification - Advanced **Note:** When you select **Guest User and Device Provisioning Using API**, a new checkbox **Provisioners belonging to this Onboarding Template can view all records of this GIM Domain** is displayed that allows the Provisioners belonging to this template to view all Guest User / Device data in the Guest and IoT Manager domain irrespective of the template they belong to.

Table continues…

Name	Description
	• **Guest User Provisioning using Outlook Add-in** : Enables Provisioners to login from the MS Outlook add-in and to provision users in the meeting invite. The tabs enabled are: - Guest User - Notification - Advanced • **Guest User Provisioning using Voucher** : Enables Provisioners to create Guest Users in bulk. The tabs enabled are: - Guest Users - Advanced
Provisioners belonging to this Onboarding Template can view and edit each other's records	Configures the Provisioners in this template to manage all the Guest Users / Device accounts provisioned using this Onboarding Template. If you want to limit each Provisioner to view only the guest accounts that they have created, do not select this option.
Temporary Accounts Validity	Configures the maximum account validity the Provisioners can grant to a Guest. The access is denied if the account is expired. • **minutes**: Indicates the minutes units for accounts validity. • **hours**: Indicates the hours units for accounts validity. • **days** : Indicates the days units for accounts validity.

Configuring the Guest User Account Details

Use this procedure to configure the Guest User account details for the Onboarding Template.

Before you begin

In the **Common** tab, select **Guest User and Device Provisioning** or **Self Service with Sponsor Approval** or **Guest User and Device Provisioning using API** or **Guest User Provisioning using Voucher** option to configure the Guest User account details.

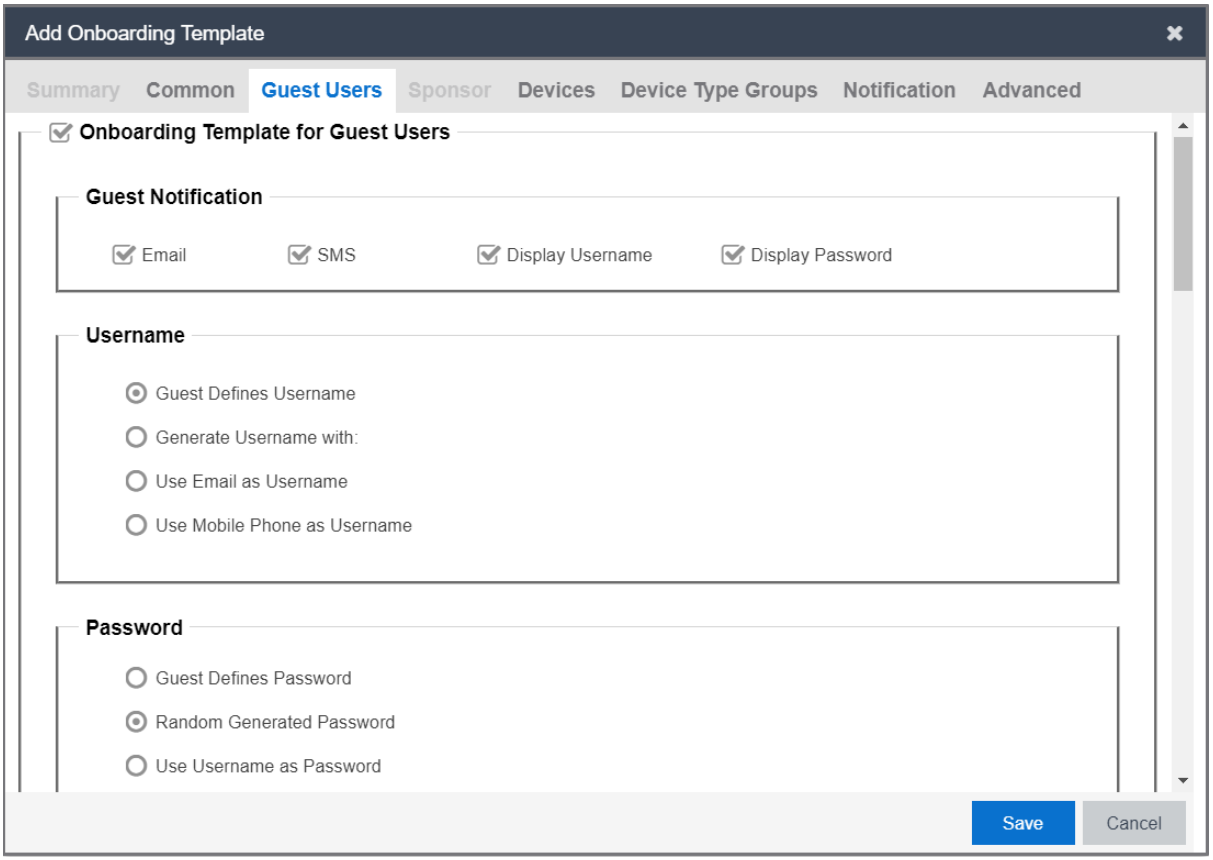
Note:

If you select **Guest User Provisioning using Outlook Add-in** option, skip this section and refer Configuring Guest User Provisioning Using Outlook Add-in on page 76 for more information.

Procedure

1. In the navigation pane, click **Onboarding Templates** > **Add** > **Guest Users** tab.

   The Guest Users screen is displayed.



2. In the Guest Users screen, select the **Onboarding Template for Guest Users** checkbox to configure the Guest User account details. By default it is selected.
3. In the **Guest Notification** section, select the required checkboxes.
4. In the **Username** section, select an option as required.
5. In the **Password** section, select an option as required.
6. In the **Password Complexity Check** section, set the password complexity selecting the required alphanumeric checkbox.
7. **(Optional)** Select **Guest User Account Limit** checkbox to restrict the number of guest accounts created within the specified duration in the **Limit the number of Guest Accounts that can be created for a given Email / Mobile Phone number within** field.
8. **(Optional)** Select **Customize Printer Friendly Page** to enable printable Guest User information page. You must select appropriate file from **Select Uploaded HTML file** drop-down list. For more information, see Configuring the File Manager on page 37.
9. In the **Access Groups** section, select the Single and Multiple Memberships Access Groups as required. For more information, see Configuring Access Groups on page 103.
10. In the **Accessible to Provisioner** section, configure the **General** and **Custom Attributes** as required.
11. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Field Descriptions

Use the data in the following table to use the **Guest User** tab.

Name	Description
Guest Notification	Configures the mode of communication to notify guests about their new account details. • **Email**: Notifies Guest Users their new account details by Email. • **SMS**: Notifies Guest Users their new account details by SMS. • **Display Username**: Notifies Guest Users with Username in the message that is displayed when a guest user account is successfully created through Self-Service or Provisioner Application. • **Display Password**: Notifies Guest Users with password in the message that is displayed when a Guest User account is successfully created through Self-Service or Provisioner Application.
Username	Specifies the different available options of Username that the Administrator can enable. • **Guest Defines Username**: Allows the Provisioner / User to specify Username during Provisioner Guest creation or Self Service Provisioning Services. • **Generate Username With**: Specifies the format of the Guest Username. - **Random Generated Username**: Random generated Username is a combination of Uppercase letters, Lowercase letters and Numbers. By default, all are enabled. Enter the length as a single value / range (within 3 - 40). Depending on the checkbox(es) selected (**lower case**, **upper case** and **number**), a random Username within the specified length is generated. For example, the length specified is 6 characters, and you have selected “lower case”, “upper case”, and “number”; the Username / Password must contain at least one lowercase, one uppercase, and one number. Valid Usernames are: “`a1Bacd`”, “`2aBBCD`” and so on. **Note:** Provisioner Application and Self-Service Application Create User Screen displays the randomly generated Username in the **Username** text box. - **FirstnameLastname**: Combination of Firstname and Lastname of the Guest User with an optional suffix / prefix. By default, **No Prefix Suffix** option is selected. For example, if first name is "Tom" and the last name is “Jones,” Guest and IoT Manager default the Username to “TomJones”. - **firstintiallastname**: Combination of the initial of the Firstname and Lastname of the user with an optional suffix / prefix. By default, **No Prefix Suffix** option is selected.

Table continues…

Name	Description
	For example, if firstname is "John" and the lastname is “Smith", Guest and IoT Manager default his Username to “jsmith”. **Note:** Administrator can restrict the Guest User and Provisioner from editing the auto-generated Username. Deselect the **Username field editable** checkbox to disable editing. By default, it is enabled. • **Use Email as Username**: Specifies to use the Email address as Username. • **Use Cell Phone Number as Username**: Specifies to use cell phone number as Username.
Password	Specifies the different available options of password that the Administrator can enable. • **Guest Defines Password**: Allows the Provisioner / User to specify Password during Provisioner Guest creation or Self Service Provisioning Services. • **Random Generated Password**: Generates random password with the specified password complexity. For example, the length specified is 6 characters, and you have selected “lower case”, “upper case”, and “number”; the Username / Password must contain at least one lowercase, one uppercase, and one number. Valid Usernames are: “`a1Bacd`”, “`2aBBCD`” and so on. • **Use Username as Password** : Allows the Guest User to login with only a Username. • **Static Password**: Allows you to set the password as a fixed string so that a single password can be used for multiple accounts.
Password Complexity Check	Configures the parameters to enforce when guests change their account passwords. Different levels of password complexity is required to select passwords that contain different combinations of characters, lowercase letters, uppercase letters, digits and symbols. If multiple combinations are selected, the different levels of password complexity is selected appropriately. • **characters**: Configures the number of characters in the password. • **lower case**: Indicates the password must have lower case only. • **upper case**: Indicates the password must have upper case only. • **number**: Indicates the password must have number only. • **special characters**: Indicates the password must have special characters only. Special characters are: `! @ # $ % ^ & * ( ) – +`
Guest User Account Limit	Limits the number of Guest User accounts that can be created for a given Email / Mobile Phone within the specified time period. For example, if the

Table continues…

Name	Description
	limit is set to 2 for a time period of 1 hour, then the user can only create 2 distinct users having the same Email / Mobile Phone in the 1 hour time frame.
Customize Printer Friendly Page	Enables or disables printable Guest User information page. Uploads the required file from **Select Uploaded HTML file** drop-down list. **Note:** Provisioner can print the Guest User details in the specified HTML file. For more information on customizing and uploading a file using File Manager, see Configuring the File Manager on page 37.
Access Groups	Configures the Access Groups for this Onboarding Template. Select the required checkbox(s) from the available options. If there are no groups available, click the links to select the required User Groups. For more information, see Configuring Access Groups on page 103. • **User Groups - Single Membership**: Configures Single Membership User Groups for the Onboarding Template. • **User Groups - Multiple Memberships**: Configures Multiple Memberships User Groups for the Onboarding Template.
Accessible to Provisioner	Configures the Guest User settings accessible to Provisioner using this Onboarding Template. The options selected in this section are available to the Provisioner. Each section allows you to customize the required fields to be **Optional** / **Mandatory**. • **General**: Configures the general Guest User settings. - **Email**: Configures the Email address of the Guest User. - **Mobile Phone**: Configures the contact number of the Guest User. - **SMS Gateway List**: Enables the SMS Gateway list to be accessible to Provisioner / Self-Service Guest User registration. If disabled, SMS messages are sent using the Administrator selected default SMS gateway for each service provider. **Important:** If a Guest User's mobile phone service provider does not support the selected default gateway, the SMS messages are not sent. - **Delete on Expire**: Specifies if the account has to be deleted when account validity duration expires. If you select **Delete on Expire** checkbox, Provisioner will be able to view this field during Guest User creation. Provisioner can select this to override the specified conditions (**Delete on Expire** / **Do Not Delete On Expire**) and remove the accounts upon expiry. If you do not select **Delete on Expire** checkbox, Provisioner will not be able to view this field during Guest User account creation. If you select

Table continues…

Name	Description
	Delete on Expire option, the Guest Account is removed on expiry. If you select **Do Not Delete On Expire** option, the account needs to be removed manually. - **Account Activation**: Specifies the type of account activation to be accessible to Provisioner. If you select **Time Based**, Provisioner can configure start time and duration (upto to a maximum set limit) during guest account creation. If you select **First Login**, Provisioner can configure guest account duration that is valid from the moment the Guest User first logs in. **Note:** **First Login** option enabled Guest User account will not expire until the user actually logs in. Once the user logs in, the account expires as per the specified duration. - **Account Expiration**: Enables or disables the account expiration to be accessible to the Provisioner. If you select **Max Expiration Time**, Provisioner can configure the account validity duration up to the maximum value specified in the **Onboarding Template** > **Common** > **Temporary Accounts Validity** field. If you select **Permanent**, a permanent Guest User account is created. This account does not have account activation preference and will not be deleted on expiry. - **Firstname & Lastname**: Allows the Provisoner to configure first name and last name of the Guest User. - **Access Groups**: Configures the selected Access Groups. - **Resend Password**: Enables or disables the display of resend password on the Self-Service registration screen. • **Custom Attributes**: Configures the custom attributes for Guest User. For more information, see Configuring Custom Attributes on page 100.

Perform any one of the following:

- If Sponsor approval is required for the Self-Service Guest Users in this Onboarding Template, go to Configuring Sponsor Approval on page 74.
- To configure Vouchers for Guest Users, go to Configuring Guest User Provisioning Using Vouchers on page 80.
- If this Onboarding Template manages devices, go to Configuring the Devices Record Details on page 84.
- Otherwise go to Configuring the Account Notification Templates on page 89.

Configuring Sponsor Approval

Use this procedure to configure Sponsor approval if Self-Service Guest Users must be approved by a Sponsor before they are granted access.

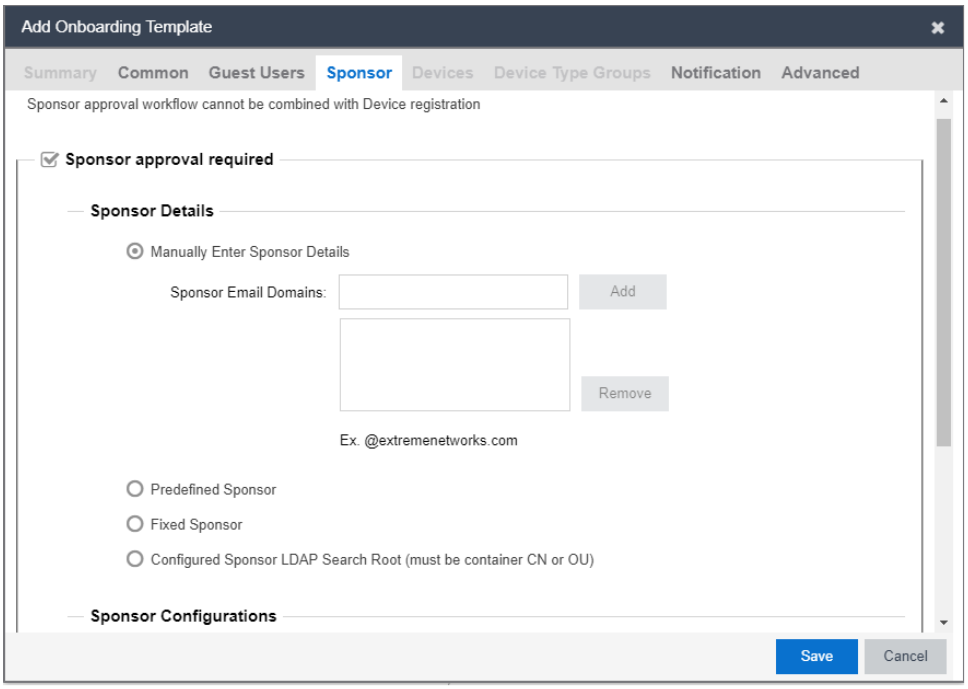
Before you begin

In the **Common** tab, select **Self Service with Sponsor Approval** to enable **Sponsor** tab.

Procedure

1. In the navigation pane, click **Onboarding Templates** > **Add** > **Sponsor** tab.

   The Sponsor screen is displayed.



2. In the Sponsor screen, select **Sponsor approval required** to configure the Sponsor approval details.
3. In the **Sponsor Details** section, select the required options.
4. In the **Sponsor Configuration** section, select the required checkboxes.
5. In the **Sponsor Authentication** section, select the **Authentication Before Approval** checkbox to login to the Provisoner account and approve or deny the request.

6. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Field Descriptions

Name	Description
Sponsor approval required	Configures the Sponsor approval settings accessible in this Onboarding Template. • **Sponsor Details**: Configures any one of the Sponsor details. - **Manually Enter Sponsor Details**: Configures the **Sponsor Email Domains**. You can add email domain name (2– 32 character length). If the entered domain name is less than 2 characters or more than 32 characters, the **Add** button is disabled. For example, the domain name must be in the following the format: • `<name>@healthbenifits.co.in` • `<name>@companyname.org` • `<name>@extremenetworks.travelersinsurance.com` If you have added the **Sponsor Email Domains**, it forces the Guest User to have a Sponsor in particular email domain. For more information, see Sponsor Details on page 156. - **Predefined Sponsor**: Configures the Sponsor email address. Add the Sponsor email address in the **Predefined Sponsor Email** field. In the **Sponsor Email Field**, select *Guest Selects from Predefined Sponsor list* to select Sponsor email address from the predefined list or *Guest must specify Sponsor Email to match* to specify the Sponsor email address that matches one of the email address from the predefined list. For more information, see Sponsor Details on page 156. - **Fixed Sponsor**: Configures the optional **First Name**, **Last Name** fields. The **Email** field is mandatory to be configured. These details are not visible to the Guest User. For more information, see Fixed Sponsor on page 157. - **Configured Sponsor LDAP Search Root**: Configures the Sponsor **LDAP Search Root**. This field can ONLY contain LDAP-defined Container Objects (CN) or an Organizational Unit (OU). LDAP Group member of attributes are not valid for thos search, so do not enter an LDAP Group CN into this search field. Enter the full DN of the OU or Container that contains your sponsor users. The DN will be searched and provide the self-service user a list of Sponsors, which the user can / must select for approval. All the Sponsors retrieved from the DN search are cached locally in Guest and IoT Manager and the frequency of the refresh depends on the **Sync Duration**. For example, if the duration is specified as one hour, the cache refreshes every one hour. For more information, see LDAP Sponsor on page 158. • **Sponsor Configuration**: Configures sponsor additional details. - **Admin/Sponsor Email (Always Notified)**: Configures the email that will always be notified for all the sponsor related mail notification.

Name	Description
	- **Sponsor Response Timeout**: Configures the time limit for Sponsor approval. If you select this, the **Default action on timeout** field is displayed. You can Approve / Deny the request post specified timeout. For example, **(0 - 480 min; 0 = Immediate Default Action)**. - **Send Initial Notification to Guest**: Enables or disables email and SMS notification sent to Guest Users as part of the Self-Service registration flow. - **Send Sponsor Response Notification to Guest**: Enables or disables email and SMS notification sent to Guest Users as part of the Self-Service registration flow when Sponsor approves or denies the access request. • **Sponsor Authentication**: Select if the Provisioner needs to login to the application prior approving or denying the Sponsor request. By default, this is enabled. - **Authentication Before Approval**: Select to send an email to the Provisoner to login to the account and approve or deny the request. If it is unchecked, the Provisioner will receive an email with a link to approve or deny the request.

Configuring Guest User Provisioning Using Outlook Add-in

Use this procedure to configure Guest User record details for using Outlook Add-in.

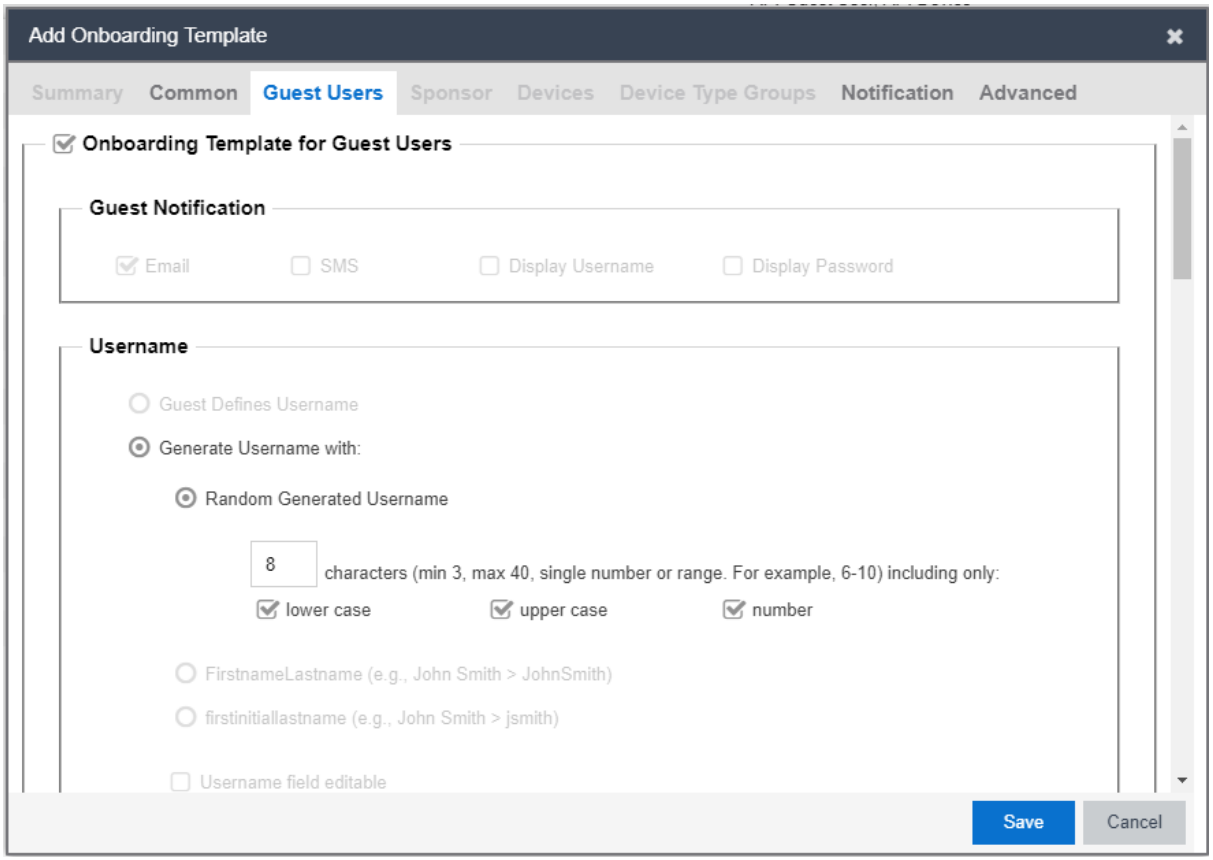
Before you begin

In the **Common** tab, select **Guest User Provisioning using Outlook Add-in** option to configure Guest User account details.

Procedure

1. In the navigation pane, click **Onboarding Templates** > **Add** > **Guest Users** tab.

   The Guest Users screen is displayed.



2. In the Guest Users screen, select the **Onboarding Template for Guest Users** checkbox to configure the Guest User account details. By default, it is enabled.
3. In the **Username** section, by default **Generate Username With** option is enabled while other options are disabled.
4. In the **Password** section, select an option as required.
5. In the **Password Complexity Check** section, set the password complexity by selecting the required alphanumeric checkbox.
6. In the **Access Groups** section, select the Single and Multiple Memberships Groups as required. For more information, see Configuring Access Groups on page 103.
7. In the **User Email Domains** section, enter the preferred domain names to be excluded from the user creation and click **Add**.
8. In the **Accessible to Provisioner** section, configure the **General** and **Custom Attributes** as required.
9. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Field Descriptions

Use the data in the following table to use the **Guest User** tab.

Name	Description
Guest Notification	**Email** notification is checked and this field is disabled for Outlook Add-in Onboarding Template.
Username	Specifies the different available options of Username that the Administrator can enable. Only **Generate Username With** field is enabled. • **Generate Username With**: Specifies the format of the Guest User Name. - **Random Generated Username**: Random generated Username is a combination of Uppercase letters, Lowercase letters and Numbers. By default, all are enabled. Enter the length as a single value / range (within 3 - 40). Depending on the checkbox(es) selected (**lower case**, **upper case** and **number**), a random Username within the specified length is generated. For example, the length specified is 6 characters, and you have selected “lower case”, “upper case”, and “number”; the Username / Password must contain at least one lowercase, one uppercase, and one number. Valid Usernames are: “`a1Bacd`”, “`2aBBCD`” and so on.
Password	Specifies the different available options of password that the Administrator can enable. • **Random Generated Password**: Generates random password with the specified password complexity. For example, the length specified is 6 characters, and you have selected “lower case”, “upper case”, and “number”; the Username / Password must contain at least one lowercase, one uppercase, and one number. Valid Usernames are: “`a1Bacd`”, “`2aBBCD`” and so on. • **Use Username as Password** : Allows the Guest User to login with only a Username. The Access Portal login screen must be modified to accept a Username without a password. • **Static Password**: Allows you to set the password as a fixed string so that a single password can be used for multiple accounts.
Password Complexity Check	Configures the parameters to enforce when guests change their account passwords. Different levels of password complexity is required to select passwords that contain different combinations of characters, lowercase letters, uppercase letters, digits and symbols. If multiple combinations are selected, the different levels of password complexity is selected appropriately. • **characters**: Configures the number of characters in the password. • **lower case**: Indicates the password must have lower case only. • **upper case**: Indicates the password must have upper case only. • **number**: Indicates the password must have number only.

Table continues…

Name	Description
	• **special characters**: Indicates the password must have special characters only. Special characters are: `! @ # $ % ^ & * ( ) – +`
Guest User Account Limit	This field is disabled for Outlook Add-in Onboarding Template.
Customize Printer Friendly Page	This field is disabled for Outlook Add-in Onboarding Template.
Access Groups	Configures the Access Groups for this Onboarding Template. Select the required checkbox(s) from the available options. If there are no groups available, click the links to select the required User Groups. For more information, see Configuring Access Groups on page 103. • **User Groups - Single Membership**: Configures Single Membership User Groups for the Onboarding Template. • **User Groups - Multiple Memberships**: Configures Multiple Memberships User Groups for the Onboarding Template.
User Email Domains	Configures the domains that need to be excluded during Guest User creation. For example, if the specified domain is "`@extremenetworks.com`"; Guest User accounts with email "`name@extremenetworks.com`" is not created.
Accessible to Provisioner	Configures the Guest User settings accessible to Provisioner using this Onboarding Template. The options selected in this section are available to the Provisioner. • **General**: Configures the general Guest User settings. - **Email**: Configures the Email address of the Guest User. This option is checked and disabled for Outlook Add-in Onboarding Template. - **Mobile Phone**: This option is disabled for Outlook Add- in Onboarding Template. - **SMS Gateway List**: This option is disabled for Outlook Add-in Onboarding Template. - **Delete on Expire**: Specifies if the account has to be deleted when account validity duration expires. - **Account Activation**: Specifies the type of account activation to be accessible to Provisioner. If you select **Time Based**, Provisioner can configure start time and duration (upto to a maximum set limit) during guest account creation. If you select **First Login**, Provisioner can configure guest account duration that is valid from the moment the Guest User first logs in. For Outlook Add-in Onboarding Template, **Time based** is selected and the field is disabled. - **Account Expiration**: Enables or disables the account expiration to be accessible to Provisioner. If you select **Max Expiration Time**, Provisioner can configure the account validity duration up to the maximum value specified in the **Onboarding Template** > **Common** > **Temporary Accounts Validity** field. If you select **Permanent**, a permanent Guest User account is created. This account does not have

Table continues…

Name	Description
	account activation preference and will not be deleted on expiry. For Outlook Add-in Onboarding Template, **Max Expiration Time** is checked and the field is disabled. - **Firstname & Lastname**: This option is disabled for Outlook Add-in Onboarding Template. - **Access Groups**: Configures the selected Access Groups. - **Resend Password**: This option is not applicable to Outlook Add-in Onboarding Template.

Configuring Guest User Provisioning Using Vouchers

Use this procedure to configure Guest User record details using Vouchers.

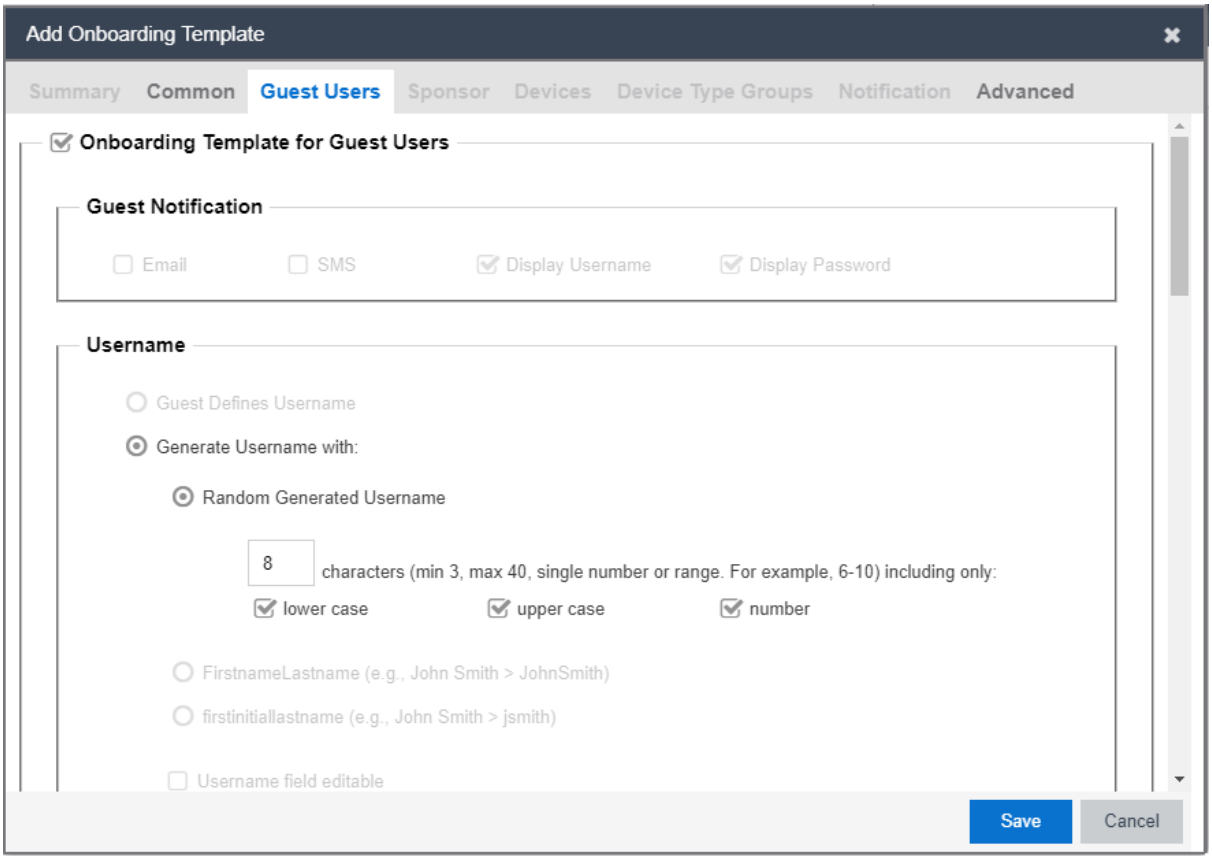
Before you begin

In the **Common** tab, select **Guest User Provisioning using Vouchers** option to configure Guest User account details.

Procedure

1. In the navigation pane, click **Onboarding Templates** > **Add** > **Guest Users** tab.

   The Guest Users screen is displayed.



2. In the **Username** section, by default **Generate Username With** along with **Random Generated Username** option is enabled while other options are disabled.
3. In the **Password** section, select an option as required.
4. In the **Password Complexity Check** section, set the password complexity by selecting the required alphanumeric checkbox.
5. In the **Access Groups** section, select the Single and Multiple Memberships Groups as required. For more information, see Configuring Access Groups on page 103.
6. In the **Accessible to Provisioner** section, configure the **General** section as required.
7. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Field Descriptions

Use the data in the following table to use the **Guest User** tab.

Name	Description
Guest Notification	**Display Username** and **Display Password** are checked and this field is disabled for Voucher type Onboarding Template.

Table continues…

Name	Description
Username	Specifies the different available options of Username that the Administrator can enable. Only **Generate Username With** field is enabled. • **Generate Username With**: Specifies the format of the Guest User Name. - **Random Generated Username**: Random generated Username is a combination of Uppercase letters, Lowercase letters and Numbers. By default, all are enabled. Enter the length as a single value / range (within 3 - 40). Depending on the checkbox(es) selected (**lower case**, **upper case** and **number**), a random Username within the specified length is generated. For example, the length specified is 6 characters, and you have selected “lower case”, “upper case”, and “number”; the Username / Password must contain at least one lowercase, one uppercase, and one number. Valid Usernames are: “`a1Bacd`”, “`2aBBCD`” and so on.
Password	Specifies the different available options of password that the Administrator can enable. • **Random Generated Password**: Generates random password with the specified password complexity. For example, the length specified is 6 characters, and you have selected “lower case”, “upper case”, and “number”; the Username / Password must contain at least one lowercase, one uppercase, and one number. Valid Usernames are: “`a1Bacd`”, “`2aBBCD`” and so on. • **Use Username as Password** : Allows the Guest User to login with only a Username. The Access Portal login screen must be modified to accept a Username without a password. • **Static Password**: Allows you to set the password as a fixed string so that a single password can be used for multiple accounts.
Password Complexity Check	Configures the parameters to enforce when guests change their account passwords. Different levels of password complexity is required to select passwords that contain different combinations of characters, lowercase letters, uppercase letters, digits and symbols. If multiple combinations are selected, the different levels of password complexity is selected appropriately. • **characters**: Configures the number of characters in the password. • **lower case**: Indicates the password must have lower case only. • **upper case**: Indicates the password must have upper case only. • **number**: Indicates the password must have number only. • **special characters**: Indicates the password must have special characters only. Special characters are: `! @ # $ % ^ & * ( ) – +`
Guest User Account Limit	This field is disabled for Voucher type Onboarding Template.

Table continues…

Name	Description
Customize Printer Friendly Page	This field is disabled for Voucher type Onboarding Template.
Access Groups	Configures the Access Groups for Voucher type Onboarding Template. Select the required checkbox(s) from the available options. If there are no groups available, click the links to select the required User Groups. For more information, see Configuring Access Groups on page 103. • **User Groups - Single Membership**: Configures Single Membership User Groups for the Onboarding Template. • **User Groups - Multiple Memberships**: Configures Multiple Memberships User Groups for the Onboarding Template.
Accessible to Provisioner	Configures the Guest User settings accessible to Provisioner using this Onboarding Template. The options selected in this section are available to the Provisioner. • **General**: Configures the general Guest User settings. - **Email**: Configures the Email address of the Guest User. This option is disabled for Voucher type Onboarding Template. - **Mobile Phone**: This option is disabled for Voucher type Onboarding Template. - **SMS Gateway List**: This option is disabled for Voucher type Onboarding Template. - **Delete on Expire**: Specifies if the account has to be deleted when account validity duration expires. - **Account Activation**: Specifies the type of account activation to be accessible to Provisioner. If you select **Time Based**, Provisioner can configure start time and duration (upto to a maximum set limit) during guest account creation. If you select **First Login**, Provisioner can configure guest account duration that is valid from the moment the Guest User first logs in. **Note:** **First Login** option enabled Guest User account will not expire until the user actually logs in. Once the user logs in, the account expires as per the specified duration. - **Account Expiration**: Enables or disables the account expiration to be accessible to Provisioner. If you select **Max Expiration Time**, Provisioner can configure the account validity duration up to the maximum value specified in the **Onboarding Template** > **Common** > **Temporary Accounts Validity** field. If you select **Permanent**, a permanent Guest User account is created. This account does not have account activation preference and will not be deleted on expiry. For Voucher type Onboarding Template, **Max Expiration Time** is selected and the field is disabled.

Table continues…

Name	Description
	- **Firstname & Lastname**: This option is disabled for Voucher type Onboarding Template. - **Access Groups**: Configures the selected Access Groups. - **Resend Password**: This option is not applicable to Voucher type Onboarding Template.

Configuring the Devices Record Details

Use this procedure to configure the Device record details for the Onboarding Template.

Before you begin

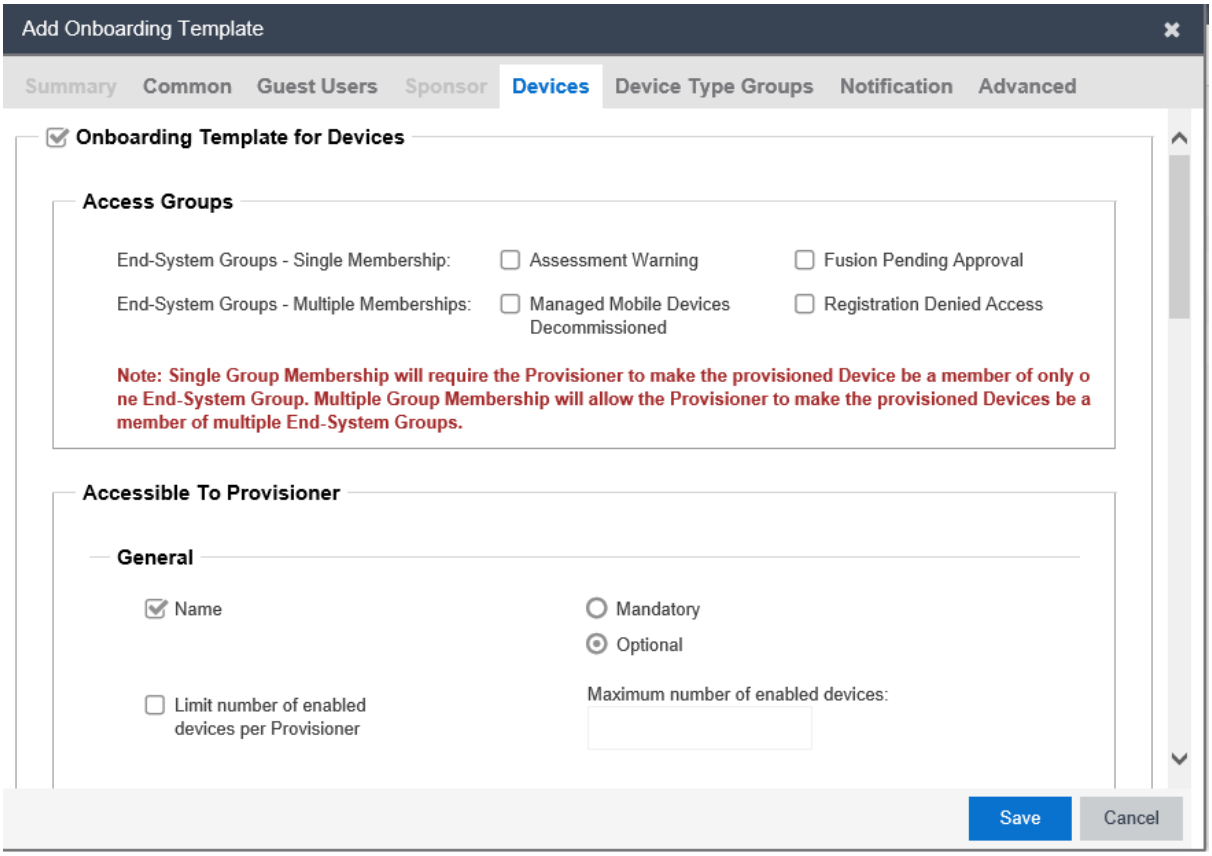
In the **Common** tab, select **Guest User and Device Provisioning** or **Guest User and Device Provisioning using API** option to enable **Devices** tab.

If you select **Provisioners belonging to this Onboarding Template can view each other's records** checkbox, the Provisioner using this Onboarding Template can view all the records of this particular Onboarding Template.

Procedure

1. In the navigation pane, click **Onboarding Templates** > **Add** > **Devices** tab.

   The Devices screen is displayed.



2. In the Devices screen, select **Onboarding Template for Devices** to configure the Device record details. By default, it is selected.
3. In the **Access Groups** section, select the Single and Multiple End-System Groups as required. For more information, see Configuring Access Groups on page 103.
4. In the **Accessible to Provisioner** section, configure the **General**, **Custom Attributes**, **Device Attributes** and **Account Validity Period** options as required.
5. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Field Descriptions

Use the data in the following table to use **Devices** tab.

Name	Description
Access Groups	Configures the Access Groups for this Onboarding Template. Select the required checkbox(es) from the available options. If there are no groups available, click the links to select the required User Access Groups. For more information, see Configuring Access Groups on page 103.

Table continues…

Name	Description
	The options available are: • **End-System Groups - Single Membership**: Configures single End-System Groups for the Onboarding Template. • **End-System Groups - Multiple Memberships**: Configures multiple End System Groups for the Onboarding Template.
Accessible To Provisioner	Configures the Devices record settings accessible to Provisioners in this Onboarding Template. The options selected in this section are available to the Provisioner. Each section allows you to customize the required fields as **Optional** / **Mandatory**. • **General**: Configures the general Devices record settings. - **Name**: Configures the Device name. - **Limit number of enabled devices per Provisioner**: Select this to restrict the maximum number of enabled Devices allowed for a Provisioner and enter the value in **Maximum number of enabled devices** field. When the limit exceeds, though Provisioner can create the Devices but disabled Devices cannot be authenticated. - **Display Admin's Comments**: Select this checkbox to enable Administrator's additional information to be displayed on the Provisioner's Create Device screen and enter the information in **Comments** field. - **Source**: Configures the default value. If you select **Auto populate with GIM-[Onboarding Template]** option, the default value populated will be Guest and IoT Manager Onboarding Template name. If you select **Static** option, user defined custom Device name can be provided. • **Custom Attributes**: Configures the custom attributes for Device record settings. For more information, see Configuring Custom Attributes on page 100. • **Device Attributes**: Configures the device attributes for Device record settings. - **Asset Type**: Configures the Device Asset Type for Permanent / Temporary. - **Device Type Groups**: Configures the Device Type Groups. - **Device Type** : Configures the Device Type of the selected Device Type Group. - **Access Groups**: Configures the selected Access Groups. • **Account Validity Period**: Configures the account validity period for Device record settings. By default, it is enabled. - **Delete on Expire**: Specifies if the Device has to be deleted when account validity duration expires.

Table continues…

Name	Description
	- **Account Activation**: Specifies the type of account activation to be accessible to Provisioner. If you select **Time Based**, Provisioner can configure start time and duration (up to a maximum set limit) during guest account creation. If you select **First Login**, Provisioner can configure guest account duration that is valid from the moment the Guest User first logs in. - **Account Expiration**: Enables or disables the account expiration to Max Expiration Time to be accessible to Provisioner.

Configuring Device Type Groups

Use this procedure to allow the Administrator to select a certain set of Device Type Groups to be made available to the Provisioner while creating Devices.

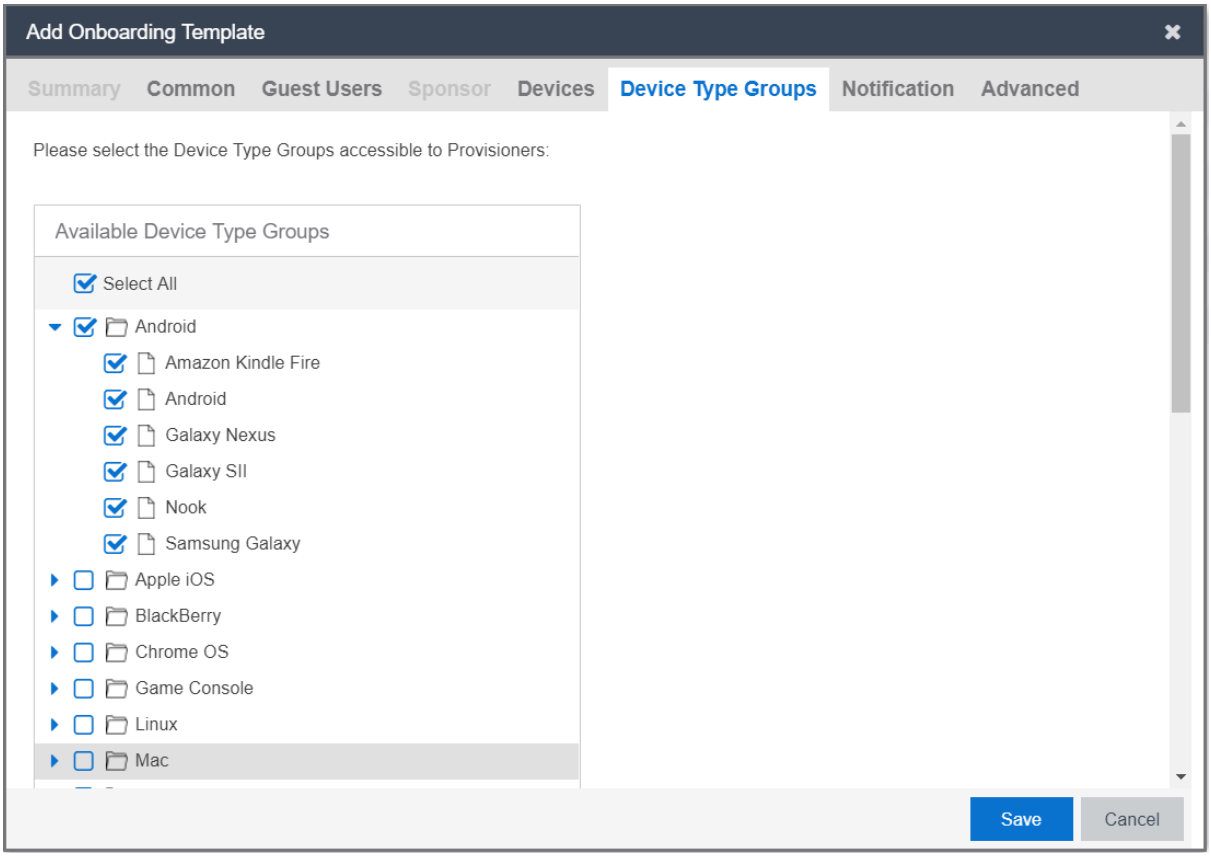
Before you begin

In the **Common** tab, select **Guest User and Device Provisioning** or **Guest User and Device Provisioning using API** option to enable **Device Type Groups** tab.

Procedure

1. In the navigation pane, click **Onboarding Templates** > **Add** > **Device Type Groups** tab.

   The Device Type Groups screen is displayed:



2. Click **Select All** to enable all the Device Type Groups. By default, it is enabled.
3. In the **Available Device Type Groups** tree list, select the **Device Type Groups** that are required.
4. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Note:

Configuring Device Type Groups limits the groups accessible to Provisioner while creating Devices.

Field Description

Use the data in the following table to use **Device Type Groups** tab.

Name	Description
Select All	Selects all the Device Type Groups accessible to Provisioners.
Available Device Type Groups	Specifies the available Device Type Groups accessible to Provisioner. By default, all are selected. You can select the required Device Type Groups.

Note:

The configured Device Type Groups apply to Self-Service, Provisioner, REST API while creating Devices.

Configuring the Account Notification Templates

Guest and IoT Manager allows you to edit the information sent in account notifications to new users. When a Guest User account is created or updated, notification is sent through an email, an SMS message, or both. You can use SMS and Email templates to edit the account notification details.

Use the **Notification** > **General** tab to send messages to the Guest User when a Provisioner saves the Guest User account or an account is created through Self-Services. You can modify the message if Sponsor Approval is required. For more information, see Configuring General Details on page 89

Use the **Notification** > **Sponsor Email** tab to notify the Sponsor for appropriate action. For more information, see Configuring Sponsor Email on page 91.

Use the **Notification** > **Sponsor Action** tab to send messages to the Guest User when the Sponsor approves or denies the user account access request. For more information, see Configuring Sponsor Action on page 93.

Note:

Ensure that you have set up your Email and / or SMS gateways. For more information, see Setting Notification Parameters on page 54.

Configuring General Details

Use this procedure to configure the account notification sent to Guest Users.

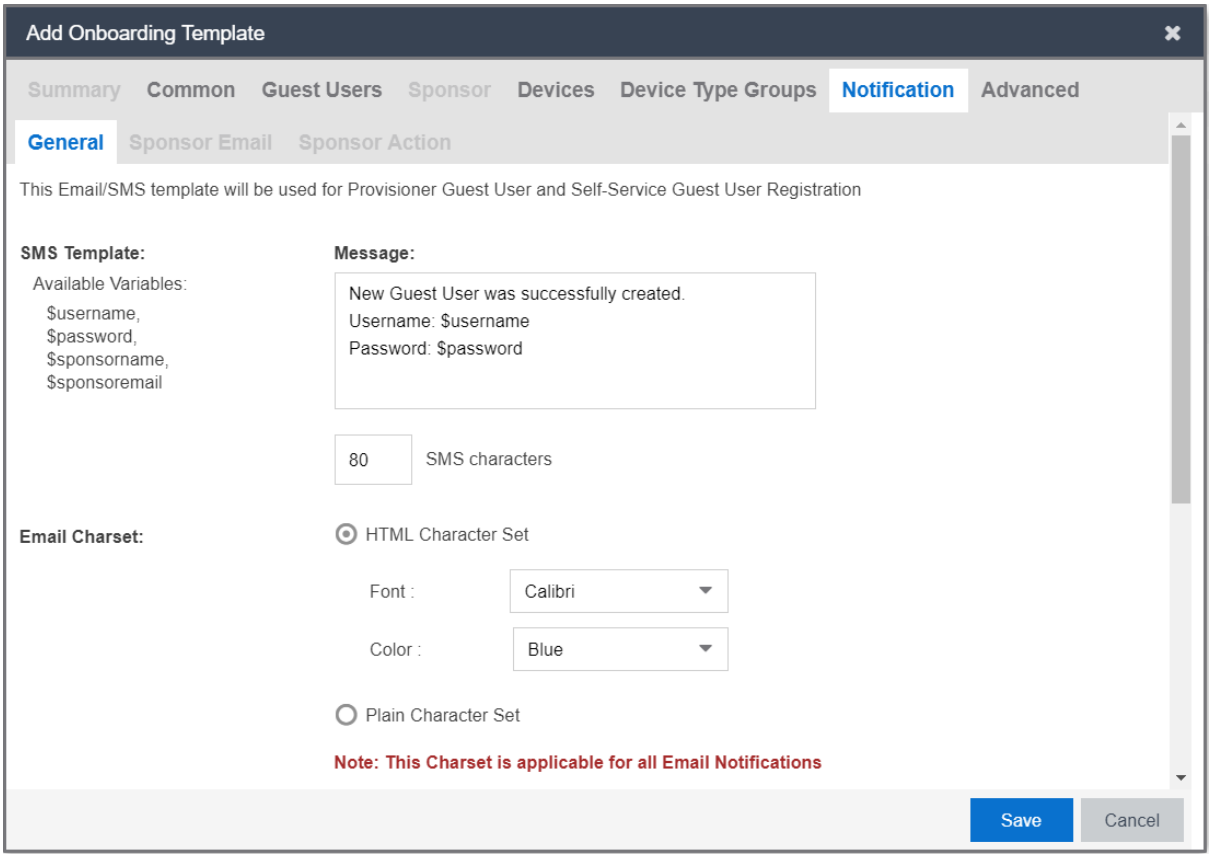
Note:

When using **SMS Template** and **Email Template**, if Sponsor approval is required, change the default message and variables to indicate that the request is pending for Sponsor approval.

Procedure

1. In the navigation pane, click **Onboarding Templates** > **Add** > **Notification** > **General** tab.

   The General screen is displayed.



2. In the **SMS Template** > **Message** field, enter the text message. You can use the available displayed variables.
3. In the **Email Charset** section, select an option as required.
4. In the **Email Template** > **Subject** field, enter the subject of email sent to the Guest User and enter the message in the **Message** field.
5. In the **Terms of Use and / or Additional information to be included as part of guest account confirmation page** field, enter the required information.
6. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Field Descriptions

Use the data in the following table to use the **General** tab.

Name	Description
SMS Template	Specifies the SMS template that is used to send an SMS to the Guest User when a Provisioner and Self-Service creates or updates the account.

Table continues…

Name	Description
	The available options are: • **Message**: Configures the message using displayed available variables such as `$username`, `$password`, `$sponsorname`, and `$sponsoremail` if required. **Note:** If Sponsor approval is required, update the message with relevant variable. • **SMS characters**: Displays the length of your message in characters. The SMS message is limited to 160 characters.
Email Charset	Specifies the type of character set for the contents of the Guest User email template. The options available are: • **HTML Character Set**: Configures the email template to support HTML content. You can select the Font and Color from the available list. By default, it is enabled. • **Plain Character Set**: Configures the email template to contain only plain characters. **Note:** This Character Set is applicable for all Email Notifications.
Email Template	Specifies the email template that is used to send an email to the Guest User when a Provisioner and Self-Service creates or updates the account. The option available are: • **Subject**: Configures the subject of the email to be sent to the Guest User. • **Message**: Configures the message using displayed available variables such as `$username`, `$password`, `$firstname`, `$lastname`, `$email`, `$starttime`, `$endtime`, `$sponsorname`, `$sponsoremail`, `$terms`, and `$userCustom1-6` if required. For example, the variable `$userCustom1-6` reflects the additional information entered by the Provisioner while creating Guest User accounts and the variable `$terms` is included to add the “Terms of Use” confidential information in the email template.
Terms of Use and/or Additional information to be included as part of guest account confirmation page	Configures a message to be displayed on the Guest account confirmation screen when an account is created. The Provisioner can print this confirmation and hand it to the Guest user. By default, text entered is appended as part of email confirmation sent to the user.

Configuring Sponsor Email

Use this procedure to configure notification email sent to the Sponsor to approve or deny the request for a Guest User account.

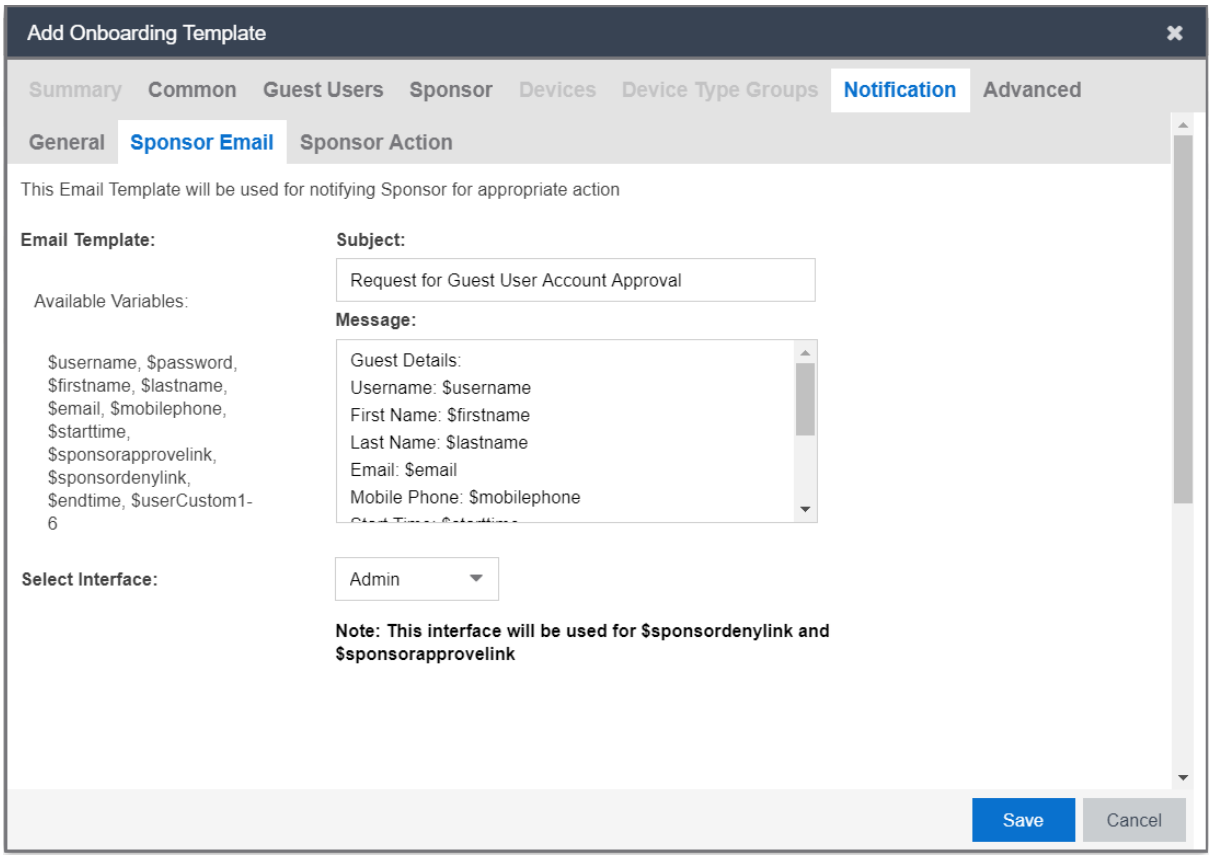
Before you begin

In the **Common** tab, select **Self Service with Sponsor Approval** option to enable the **Sponsor Email** tab.

Procedure

1. In the navigation pane, click **Onboarding Templates** > **Add** > **Notification** > **Sponsor Email** tab.

   The Sponsor Email screen is displayed.



2. In the **Email Template** > **Subject** field, enter the subject of the Sponsor request email and in the **Message** field, enter the message to be sent to the sponsor to approve or deny the access request for a Guest User account. You can use the available displayed variables.
3. In the **Select Interface** field, select the required interface from the drop-down list. By default, **Admin** is selected.
4. Click **Save** to submit the information or click **Cancel** to cancel the changes.

Field Descriptions

Use the data in the following table to use the **Sponsor Email** tab.

Name	Description
Email Template	Specifies the email template that is used to notify the Sponsor for appropriate action. The options available are: • **Subject**: Configures the subject of the email to be sent to the Sponsor. • **Message**: Configures the message using displayed available variables such as `$username`, `$password`, `$firstname`, `$lastname`, `$email`, `$starttime`, `$sponsoractionlink`, `$endtime`, and `$userCustom1-6` if required. **Note:** If you have selected **Authentication Before Approval** field in Sponsor tab, `$sponsoractionlink` variable is available. If you have unchecked, the `$sponsorapprovelink` and `$sponsordenylink` variables are available.
Select Interface	Configures 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 is **Service A** interface IP address. This action affects the `$sponsorapprovelink` and `$sponsordenylink` variable. **Note:** This field is available only if you have selected **Authentication Before Approval** field in Sponsor tab. For more information, see Configuring Sponsor Approval on page 74.

Configuring Sponsor Action

Use this procedure to configure Guest User account notification when the Sponsor approves or denies the user account access request.

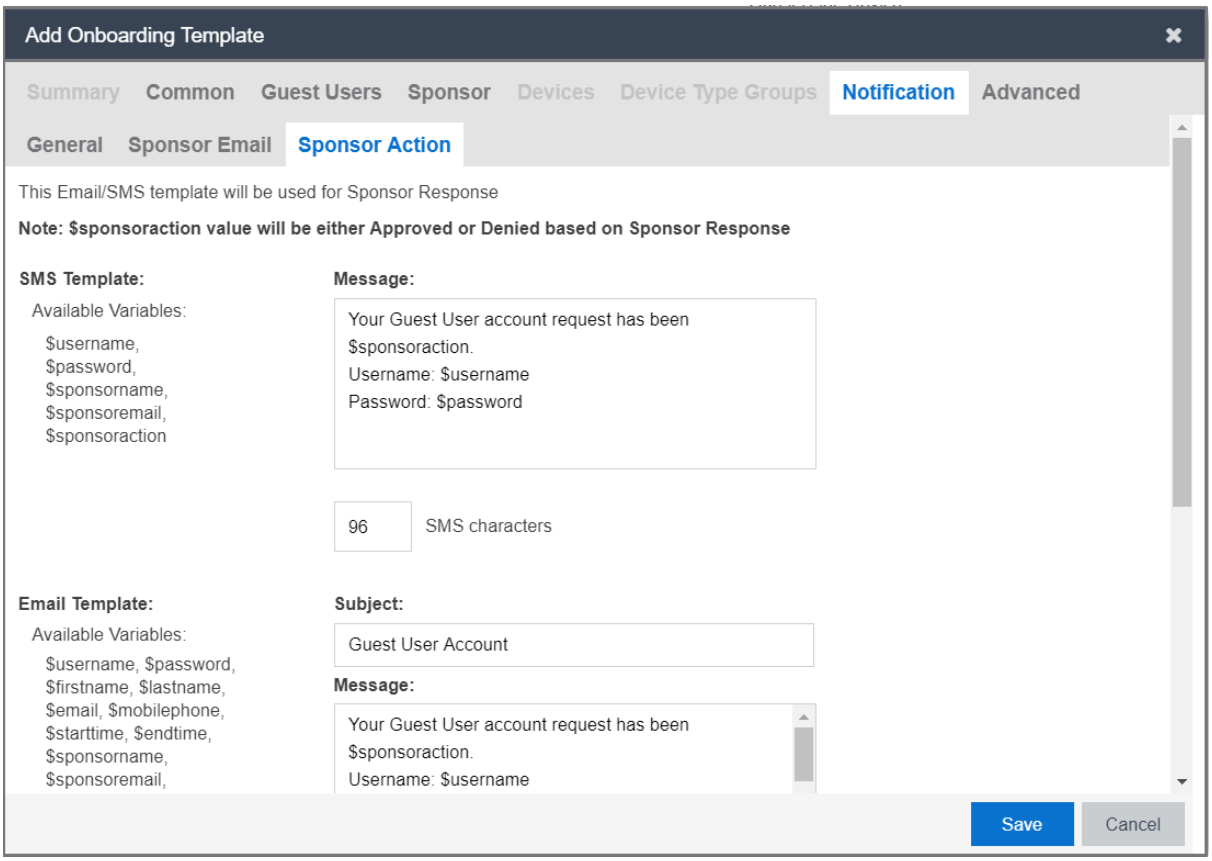
Before you begin

In the **Common** tab, select **Self Service with Sponsor Approval** option to enable the **Sponsor Action** tab.

Procedure

1. In the navigation pane, click **Onboarding Templates** > **Add** > **Notification** > **Sponsor Action** tab.

The Sponsor Action screen is displayed



2. In the **SMS Template** > **Message** field, enter the text message. You can use the available displayed variables.
3. In the **Email Template** > **Subject** field, enter the subject of the Sponsor request email and in the **Message** field, enter the message to be sent to the sponsor to approve or deny the access request for a Guest User account. You can use the available displayed variables.
4. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Field Descriptions

Use the data in the following table to use the **Sponsor Action** tab.

Name	Description
SMS Template	Specifies the email template that is used to send an email to the Guest User when a Sponsor approves or denies the Guest User account. The option available are: • **Message**: Configures the message using displayed available variables such as `$username`, `$password`, `$sponsorname`, `$sponsoremail`, and `$sponsoraction` if requried.

Table continues…

Name	Description
	• **SMS characters**: Displays the length of your message in characters. The SMS message is limited to 160 characters.
Email Template	Specifies the email template that is used to send an email to the Guest User when a Sponsor approves or denies the Guest User account. The options available are: • **Subject**: Configures the subject of the email to be sent to the Guest User. • **Message**: Configures the message using displayed available variables such as `$username`, `$password`, `$firstname`, `$lastname`, `$email`, `$starttime`, `$endtime`, `$sponsorname`, `$sponsoremail`, `$sponsoraction`, and `$sponsortext` if required.

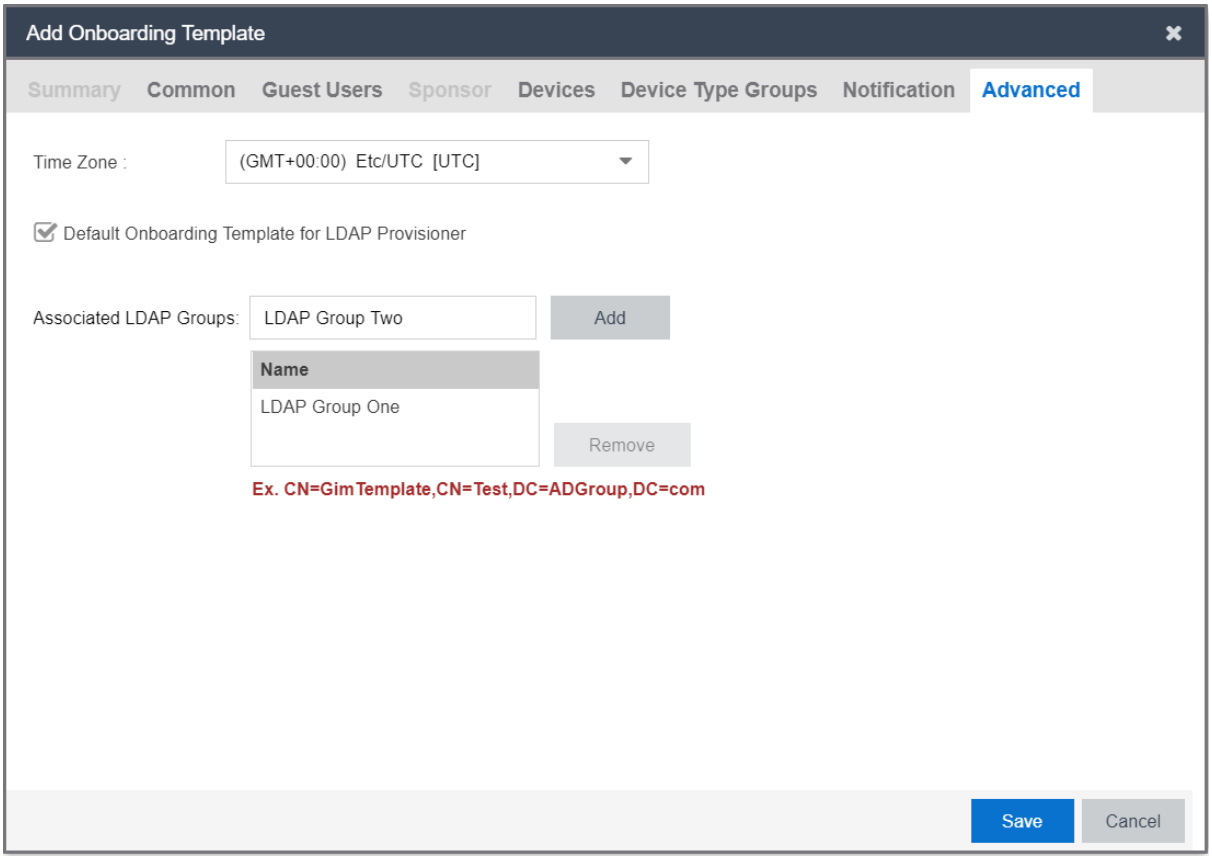
Configuring Advanced Details

Use this procedure to configure advanced details for the Onboarding Template.

Procedure

1. In the navigation pane, click **Onboarding Template** > **Add** > **Advanced** tab.

   The Advanced screen is displayed.



2. In the **Time Zone** drop-down list, select the required zone.
3. Select **Default Onboarding Template for LDAP Provisioner** to send the Onboarding Template as default for Provisioners who are not associated with any Onboarding Template(s).
4. In the **Associated LDAP Groups** section, **Add** or **Remove** the required LDAP Groups to be associated with the Onboarding Template(s).
5. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Field Descriptions

Use the data in the following table to use the **Advanced** tab.

Name	Description
Time Zone	Configures the time zone.
Default Onboarding Template for LDAP Provisioner	Enables or disables the default Onboarding Template for LDAP Provisioner. By default, it is enabled.

Table continues…

Name	Description
	Note: If you log in as a Provisioner: • **Case Scenario**: The group that you are part of is not associated with any Onboarding Template. • **Result**: The Onboarding Template(s) marked as default is / are sent to you.
Associated LDAP Groups	Configures the LDAP group(s) associated with the Onboarding Template. **Note:** If the logged in Provisioner is a part of any of the specified group(s), then the created Onboarding Template must be sent to the Provisoner. You can define the same group for multiple Onboarding Templates.

Managing Onboarding Templates

Onboarding Template is a collection of settings that establishes the administrative rights and account settings of the Provisioners that associate with it.

Use this procedure to manage an Onboarding Template.

Procedure

1. In the navigation pane, Click **Onboarding Templates**.
2. Click the required Onboarding Template to manage.
3. Click **Add** to create a new Onboarding Template. For more information, see Creating an Onboarding Template on page 64.
4. Click **Edit** to modify and view the existing Onboarding Template. For more information, see Modifying and Viewing an Onboarding Template on page 98.
5. Click **Copy** to create a copy of the existing Onboarding Template. For more information, see Copying an Onboarding Template on page 99.
6. Click **Delete** to delete the selected Onboarding Templates, Onboarding Template Members, and Expired Guest Accounts. For more information, see Deleting Onboarding Templates and Guest Accounts on page 99.

   Tip:

   Use Ctrl / Shift to select multiple records to delete.

Modifying and Viewing an Onboarding Template

Use this procedure to edit and view an existing Onboarding Template.

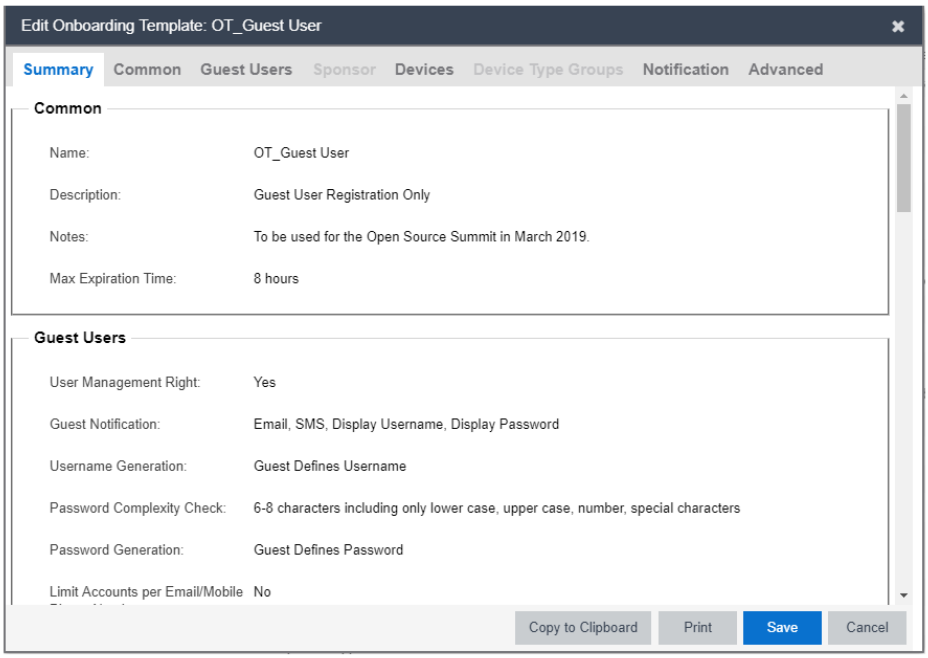
Procedure

1. In the navigation pane, Click **Onboarding Templates**.
2. Select the required Onboarding Template from the list.
3. Click **Edit** > **Summary** tab to view an Onboarding Template summary.

   Note:

   You can also view by double-clicking the required Onboarding Template from the list.

   The Edit screen is displayed.



4. In the Edit Onboarding Template screen, modify the changes in the required tabs.
5. Click **Copy to Clipboard** to copy the Onboarding Template summary to clipboard.
6. Click **Print** to print the Onboarding Template.
7. Click **Save** to save the configuration or **Cancel** to cancel the changes.

Copying an Onboarding Template

Use this procedure to create a copy of an existing Onboarding Template.

Note:

Copy option in the Onboarding Template only creates a new Onboarding Template. The Provisioner(s) or Guest User(s) or Device(s) associated with the source Onboarding Template is / are not added to the copied Onboarding Template.

Procedure

1. In the navigation pane, click **Onboarding Templates**.
2. Click the required Onboarding Template from the list.
3. Click **Copy**.
4. In the Onboarding Template Name field, enter the name, description and notes for the new Onboarding Template.
5. Modify the required changes in all the tabs for the new Onboarding Template.
6. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Deleting Onboarding Templates and Guest Accounts

Use this procedure to delete Onboarding Template(s), Onboarding Template Member(s) and Expired Guest User(s).

Procedure

1. In the navigation pane, Click **Onboarding Templates**.
2. Select the required Onboarding Template(s).
3. In the **Delete** drop-down list, click an option as required.
4. Click **Yes** or **No** in the confirmation message to delete the selected Onboarding Template(s), Onboarding Template Member(s), and Expired Guest User(s).

Field Descriptions

Use data in the following table to use **Delete** option.

Name	Description
Delete Onboarding Template(s)	Deletes the selected Onboarding Template(s).

Table continues…

Name	Description
	Note: You cannot delete an Onboarding Template, if it is associated with the Guest User(s) or Device(s) or Provisioner(s). Use Delete **Onboarding Template Member(s)** Option to proceed in such scenarios. In case of failure, appropriate error message is displayed.
Delete Onboarding Template Member(s)	Deletes all the Internal Provisioner(s) or Self Service Provisioner(s), or Guest User(s), or Device(s) of the selected Onboarding Template. If you select this option, the Guest and IoT Manager displays a screen that allows you to select the type of records to delete. If this option is selected, you need to select the required selection in the Delete Member screen.
Delete Expired Guest User(s)	Deletes all the expired Guest User accounts of the selected Onboarding Template(s).

Configuring Custom Attributes

The **Custom Attributes** tab in Onboarding Templates menu allows the Administrator to specify human readable labels for **Custom Field** (1-6). You can set custom labels differently for Guest User and Device in their respective tabs.

The Administrator configures custom labels, whereas the Provisioner and Self-Service guest configures values for these custom labels.

For more information, see Configuring Guest User Custom Attributes on page 100 and Configuring Device Custom Attributes on page 102.

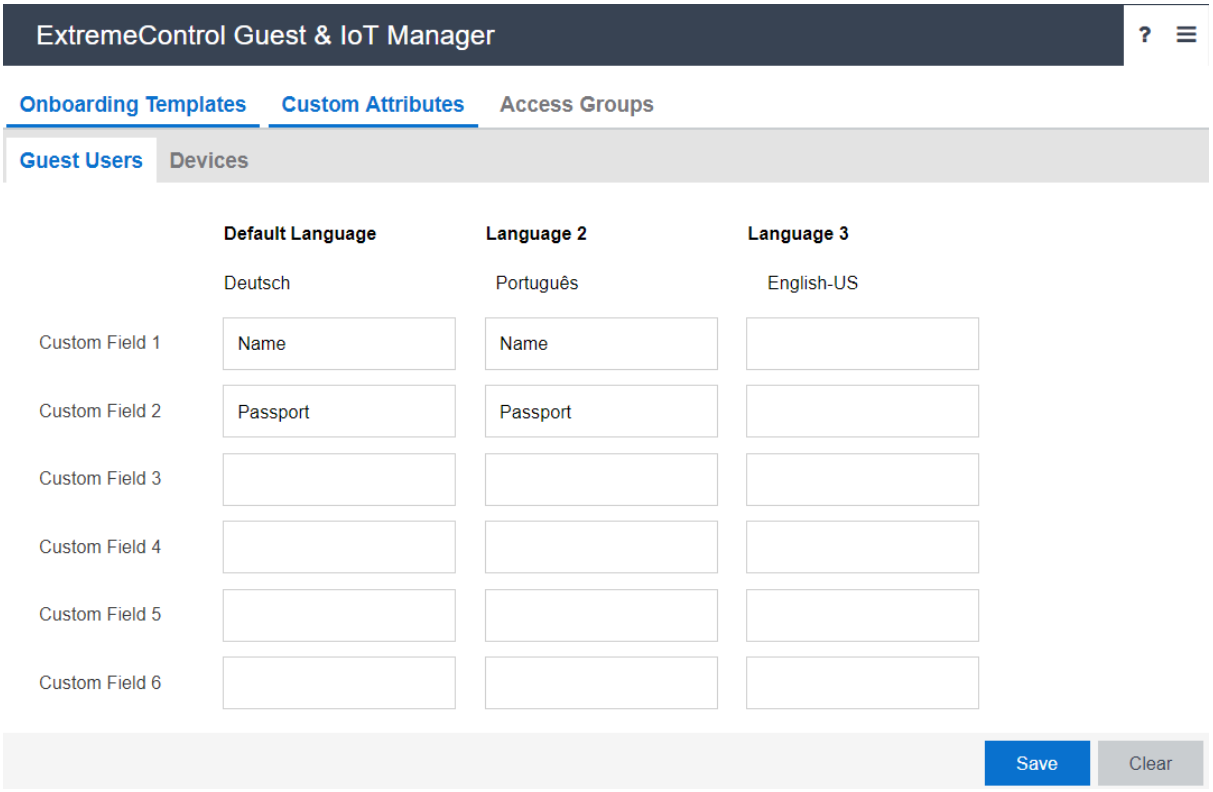
Configuring Guest User Custom Attributes

Use this procedure to configure Guest User Custom Attributes.

Procedure

1. In the navigation pane, click **Onboarding Templates** > **Custom Attributes** > **Guest User** tab.

   The Guest User screen is displayed.



The languages displayed are based on the locales configured in **Preferences** tab. For more information, see Setting the Locales on page 35.

2. In the **Custom Field**, enter one or more labels as required in the (1-6) fields.
3. Click **Save** to save the configuration or click **Clear** to clear the configuration.

   You cannot clear the default and other languages available in this screen.

Field Descriptions

Use the data in the following table to use **Guest User** tab.

Name	Description
Custom Field	Specifies the labels for the custom fields to be displayed during Guest User Registration. For example, if Administrator specify "**Country Code**" as the label for "**Custom Field 1**" for the language "**English-US**" and when the Provisioner or Self Service Guest User selects "**English-Us**" as the language to be displayed, then country code need to be specified during Guest User registration depending on the Onboarding Template settings. For more information, see Registering a New Guest User on page 154 and *ExtremeControl Guest and IoT Manager Configuration*.

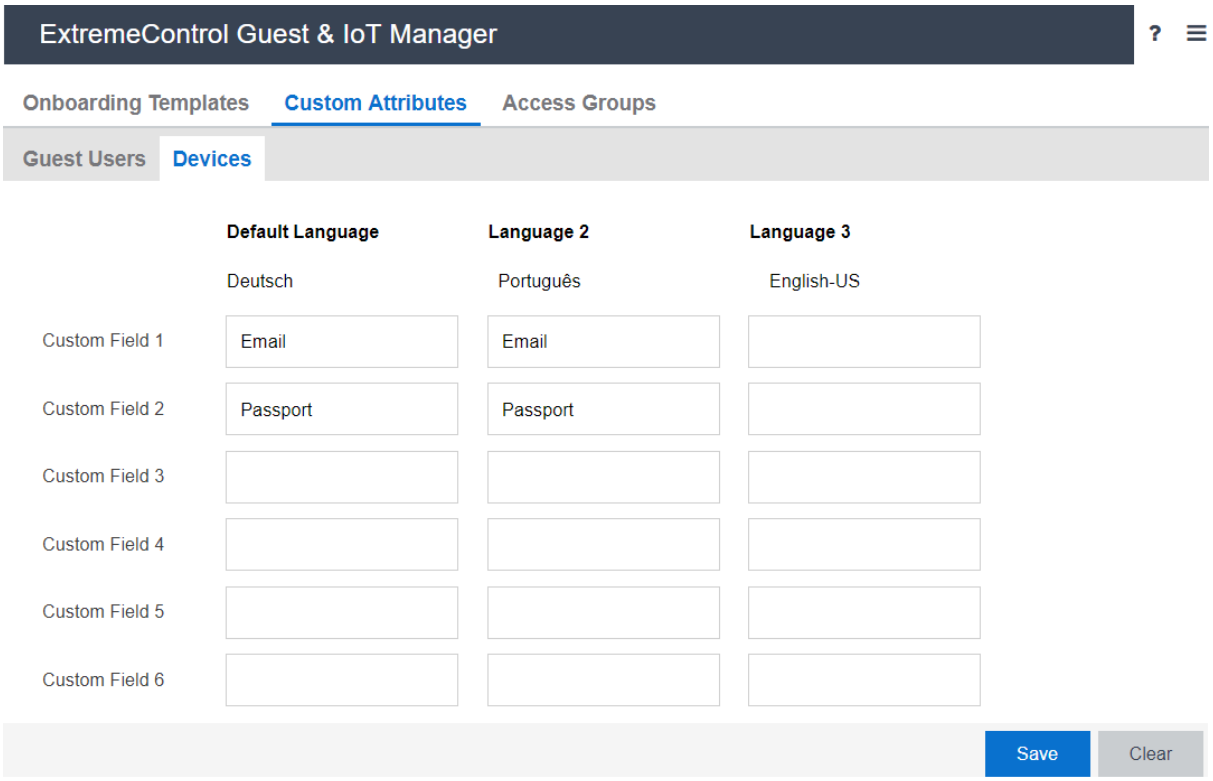
Configuring Device Custom Attributes

Use this procedure to configure Device Custom Attributes.

Procedure

1. In the navigation pane, click **Onboarding Templates** > **Custom Attributes** > **Device** tab.

   The Devices screen is displayed.



   The languages displayed are based on the locales configured in **Preferences** tab. For more information, see Setting the Locales on page 35.

2. In the **Custom Field** field, enter one or more labels as required in the (1-6) fields.
3. Click **Save** to save the configuration or click **Clear** to clear the configuration.

   Note:

   You cannot clear the default and other languages available in this screen.

Field Descriptions

Use the data in the following table to use **Device** tab.

Name	Description
Custom Field	Specifies the labels for the custom fields to be displayed during Guest User Registration. For example, if Administrator specify "**Location**" as the label for "**Custom Field 1**" for the language "**English-US**" and when the Provisioner or Self Service Guest User selects "**English-Us**" as the language to be displayed, then location need to be specified during Guest User registration depending on the Onboarding Template settings. For more information, see Registering a New Guest User on page 154 and *ExtremeControl Guest and IoT Manager Configuration*.

Configuring Access Groups

The **Access Groups** tab in Onboarding Templates menu allows the Administrator to map the **Access Groups** as Single and Multiple Memberships that are available to the Provisioner during Guest User Registration as per the Onboarding Template settings.

There are two types of Access Groups. The Extreme Management Center Administrator needs to create "User Groups - Single Membership" and "User Groups - Multiple Memberships" types of accounts in the server prior Provisioner provides network access to the users at your facility. These groups are customized for your site; the Administrator structure the fields that needs to be available during Guest User creation.

- **User Groups - Single Membership**: Configures the specific network to which the Guest User has access. The Provisioner may select only one **Single Membership** as the user must be assigned to one segment of the network. For example, you can select south east regional sales department VLAN as the Single Membership for the people belonging to the sales department of the south east region.
- **User Groups - Multiple Memberships**: Configures wired, wireless or secured wireless and typically the location of a switch or access point.

You can set Access Groups differently for Guest User and Device in their respective tabs. The User Groups configured on Extreme Management Center are available to the Guest and IoT Manager Administrator to map as Single and Multiple Memberships. For more information on configuring User Groups, see User Groups in Extreme Management Center.

The End System Groups configured on Extreme Management Center are available to Guest and IoT Manager Administrator to map as Single and Multiple Memberships. For more information on configuring End System Groups, see End-System Groups in Extreme Management Center.

Note:

The **Access Groups** settings are optional. If you do not map the Access Groups as Single and Multiple Memberships, then a link to the Access Groups tab is displayed while creating an Onboarding Template.

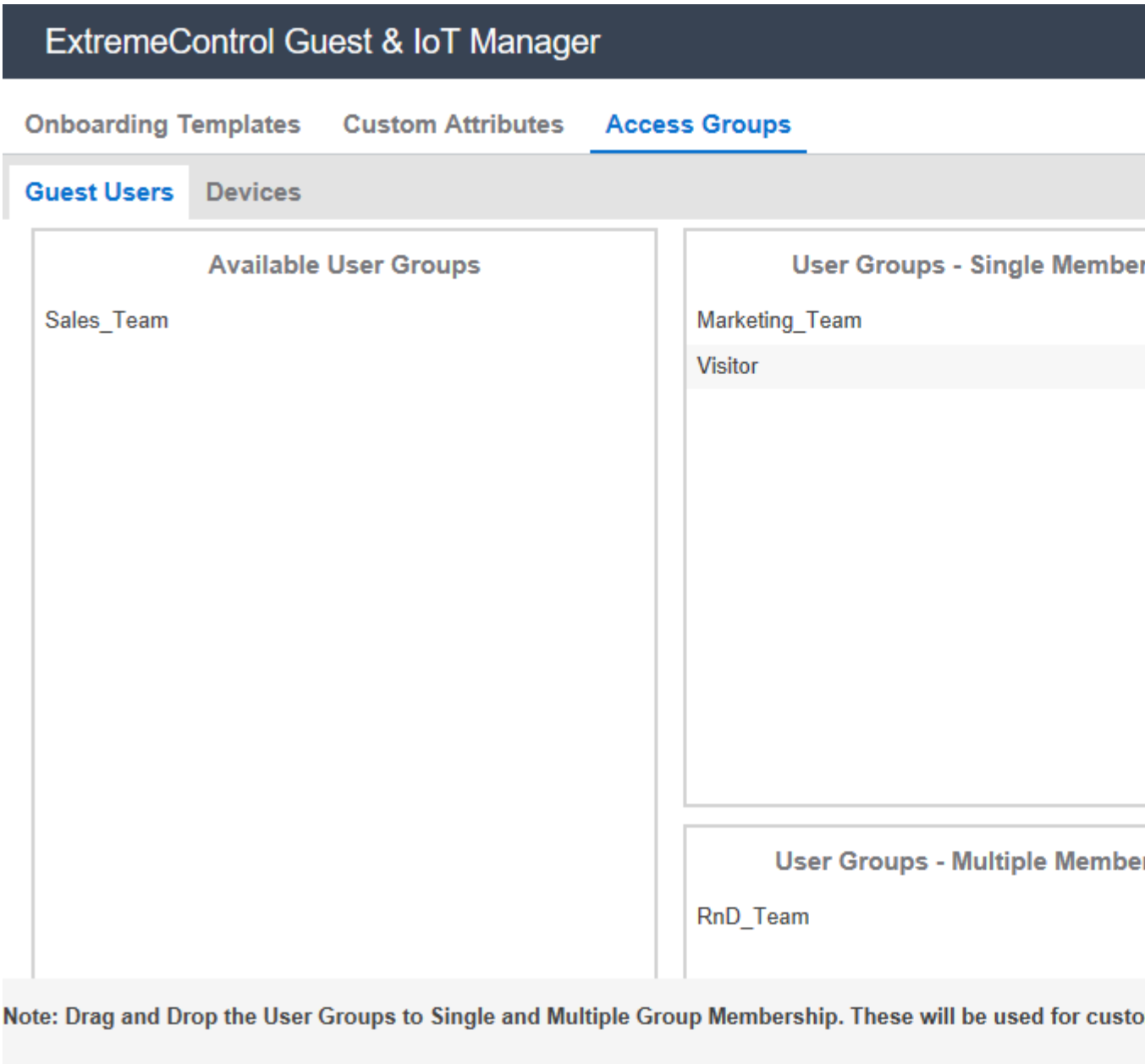
Configuring Guest User Access Groups

Use this procedure to configure Guest User access groups.

Procedure

1. In the navigation pane, Click **Onboarding Templates** > **Access Groups** > **Guest Users** tab.

   The Guest Users screen is displayed.



2. In the **Available User Groups** section, drag and drop the required *User Groups* to **Single** and **Multiple Group Memberships**. This can be used for customizing the Onboarding Templates.

   You can also perform the same action in reverse order.

3. Click **Save** to save the configuration.

Field Descriptions

Use the data in the following table to use **Guest Users** tab.

Name	Description
Available User Groups	Specifies the list of User Groups available for mapping with Single or Multiple Memberships.
User Groups - Single Membership	Specifies the list of User Groups that provide specific network access to the Guest User.
User Groups - Multiple Memberships	Specifies the User Groups that provide general network access to the Guest User.

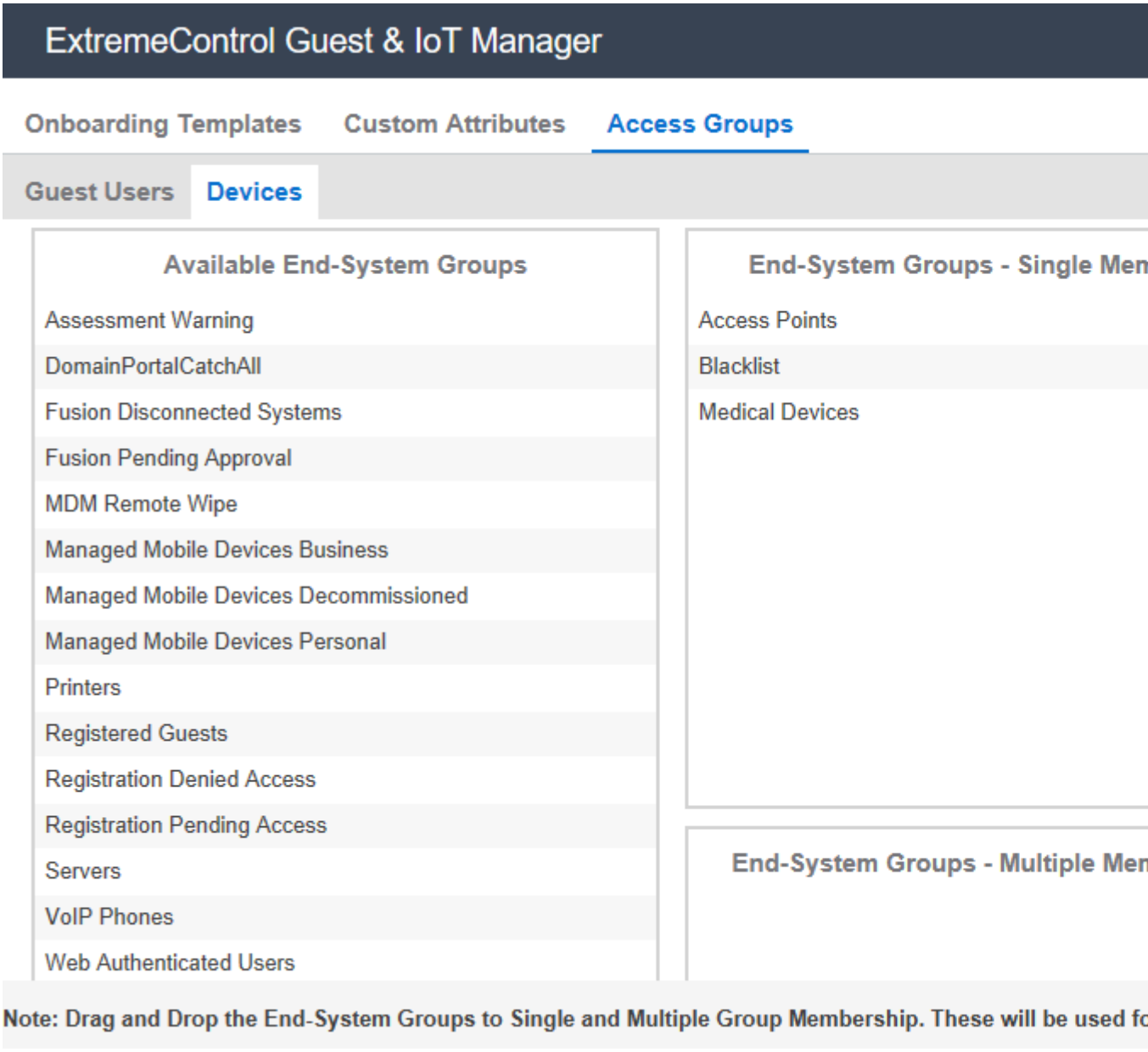
Configuring Device Access Groups

Use this procedure to configure Device access groups.

Procedure

1. In the navigation pane, Click **Onboarding Templates** > **Access Groups** > **Device** tab.

   The Devices screen is displayed.



2. In the **Available End-System Groups** section, drag and drop the required *End-System Groups* to **End-System Groups - Single Memberships** or **End-System Groups - Multiple Memberships**.
3. Click **Save** to save the configuration.

Field Descriptions

Use the data in the following table to use **Device** tab.

Name	Description
Available End-System Access Groups	Specifies the list of End-System Groups available for mapping as Single and Multiple Groups.
End-System Groups - Single Memberships	Specifies the list of End-System Groups that provide specific network access to the Guest User.
End-System Groups - Multiple Memberships	Specifies the End-System Access Groups that provide general network access to the Guest User.

Chapter 7: Configuring Provisioners

This module is intended for Guest and IoT Manager Administrator to perform operations on Provisioner accounts that are stored in the Access Control Engine local password repository. A Provisioner is a member of the organization whose account is stored either in the Access Control Engine or in LDAP. These internally stored Provisioners are referred as **Internal Provisioners**.

If the Administrator desires to create Guest User accounts to test policies, it is essential to have a Provisioner account. Administrator can only set up rules to place the Guest Users in the appropriate Onboarding Template and not modify the Guest Users. For more information, see Configuring Advanced Details on page 95.

Prerequisite for Provisioner Function

The Administrator must ensure that the following criterion is met before the Provisioners start functioning.

- **Provisioner Accounts:** Each provisioner must have a Provisioner Account stored in Access Control Engine or mapped via Access Control Engine to your LDAP store.
- **Access to the Provisioner Application**: Each provisioner must be able to connect to the Provisioner Application via the web browser.
- **Connection to an Access Control Engine**: The Guest and IoT Manager Application must have connectivity to the Access Control Engine in order to save and retrieve guest data.
- **Configurations**: The Access Control Engine must have the *Single Membership Access Group* and *Multiple Memberships Access Groups* that form the set of assignable access constraints for Guest Users.
- **Notification Settings**: The Guest and IoT Manager Application must have configuration to send Email and SMS notifications to the Guest Users. For more information, see Enabling E-mail Notification on page 55 and Configuring SMS Gateway / Provider on page 57.

Note:

Ensure that you have created an Onboarding Template to which the new Internal Provisioner belongs. For more information, see Creating an Onboarding Template on page 64.

It is necessary to train the Provisioners to use the Guest and IoT Manager Provisioner Application. For more information, see *ExtremeControl Guest and IoT Manager Configuration*.

Internal Provisioner Operations

The **Internal Provisioners** tab in Provisioners menu allows you to create and manage Internal Provisioners. You can also view and reassign the Internal Provisioner to one or more Onboarding Template(s). For more information, see Prerequisite for Provisioner Function on page 108.

Creating an Internal Provisioner

Use this procedure to create an Internal Provisioner account in the local password repository.

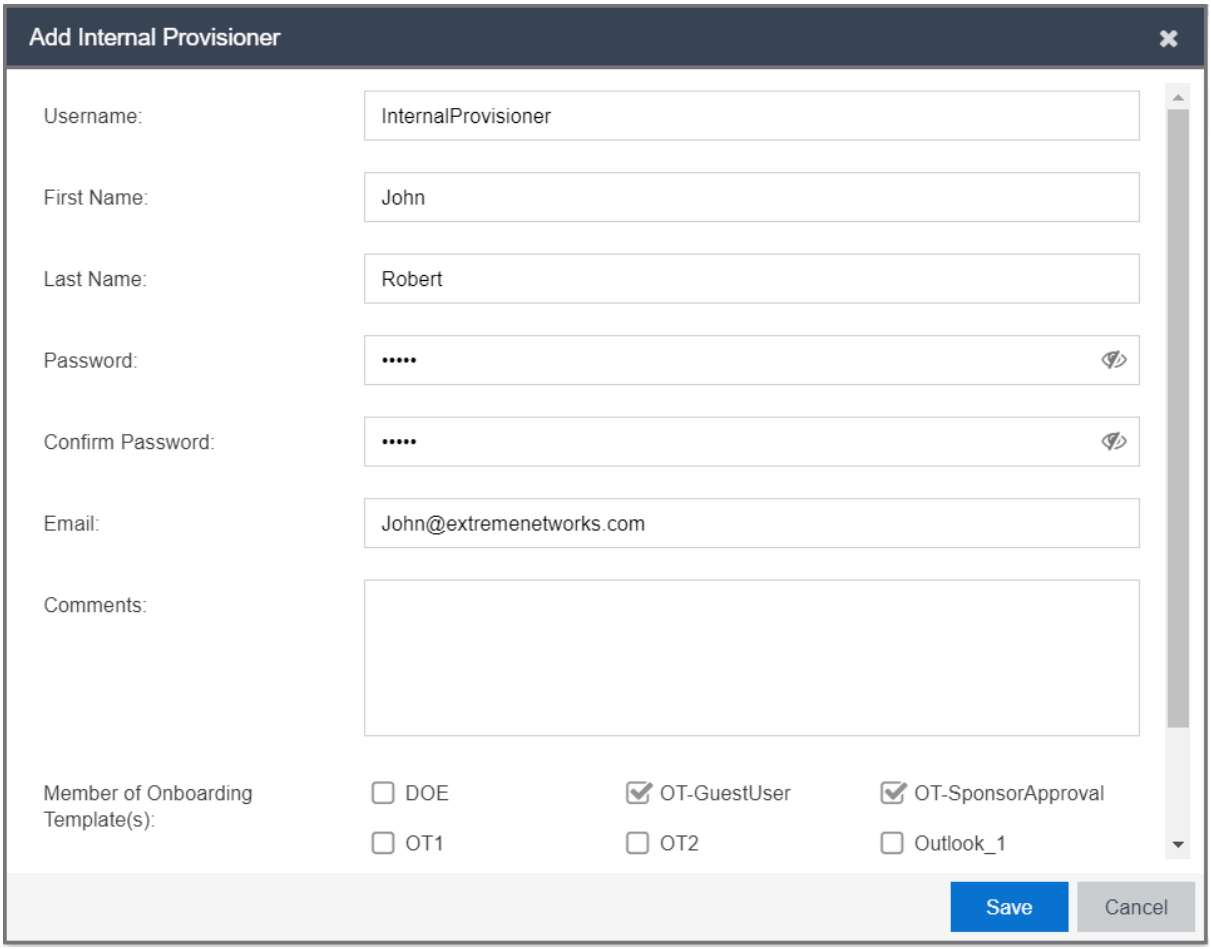
Procedure

1. In the navigation pane, click **Provisioner** > **Internal Provisioners** tab.

   The Internal Provisioners screen is displayed.

2. In the Internal Provisioners screen, click **Add** to add the internal provisioners.

   The Add Internal Provisioner screen is displayed.



3. Configure the Provisioner login credentials details in the respective fields as required.
4. In the **Member of Onboarding Templates(s)** section, select the Onboarding Template(s) that needs to be associated with the Provisioners.
5. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   The added Internal Provisioners details are displayed in Internal Provisioners screen along with all the specified information.

   The URL to access the Provisioner application is "`https://<Guest Manager & IOT Manager IP/Host Name>/GIM/provisioner/`"

   Provisioner URL can be also access through IP address or host name. For example: `https://<Guest Manager & IOT Manager IP / Host Name>`.
6. **(Optional)** Select the required Provisioner account and click **Edit**, to modify a provisioner account. For more information, see Modifying Internal Provisioner Account on page 111.
7. **(Optional)** Click  **Show Filter** to narrow the search parameters and quickly find all similar Provisioner accounts. For more information, see Filtering Internal Provisioners on page 113.
8. **(Optional)** Select the required Internal Provisioner(s) and click **Delete**, to remove the created Internal Provisioner(s).

   Tip:

   Use Ctrl / Shift to select multiple records to delete.

   When you delete a Provisioner(s), the application retains all Guest Users and Device Accounts that were provisoned by the deleted Provisioner.

Field Descriptions

Use data in the following table to use Add Provisioner screen.

Name	Description
Username, **First Name**, and **Last Name**	Configures the username, first name, and last name of the Provisioner account details. The length of the name can be 30 characters or less. **Note:** These fields should only contain letters, number, hyphen, and underscore.
Password and **Confirm Password**	Configures the password of the Provisioner. Since Guest and IoT Manager encrypts the password, ensure that you make a note of the password for future reference. **Note:** These fields should only contain alphanumeric and special characters. Only these special characters are allowed : `! @ # $ % ^ & * ( ) + - .`

Table continues…

Name	Description
Email	Configures the email address of the Provisioner.
Comments	Configures the additional information.
Member of Onboarding Template(s)	Configures the Onboarding Template that needs to be associated with the Provisoner. Select the required Onboarding Template and ensure that Provisioner must be part of atleast one Onboarding Template.

Modifying Internal Provisioner Account

Use this procedure to modify a Internal Provisioner account.

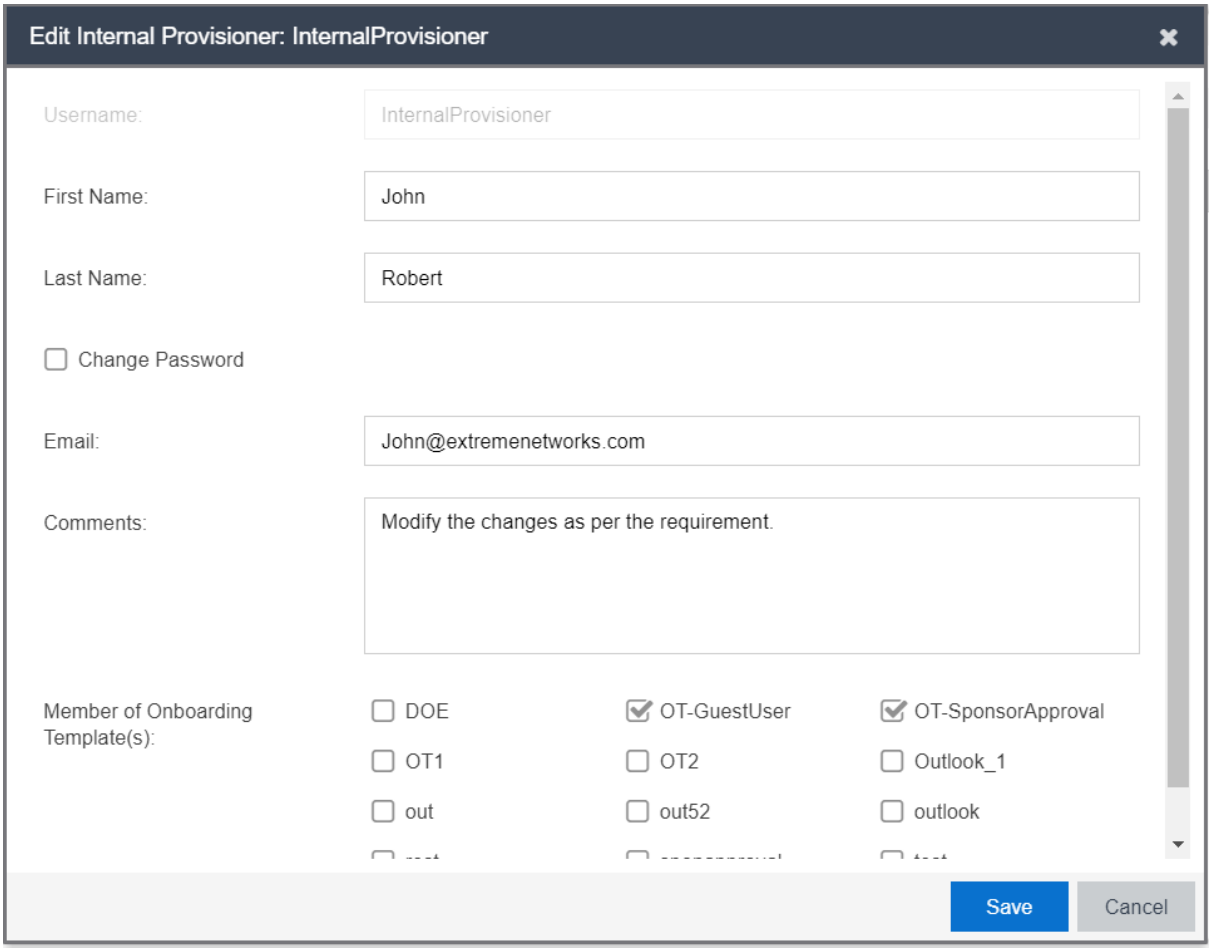
Procedure

1. In the navigation pane, click **Provisioner** > **Internal Provisioner** tab.

   The Internal Provisioners screen is displayed with the list of provisioners currently authorized to set up Guest access.

2. In the Internal Provisioners screen, select the Provisioner account that you wish to modify.
3. Click **Edit**, to view the Provisioner account details.

   The Edit Internal Provisioner screen is displayed.



Note:

You can also view by double-clicking the required Provisioner account from the list. By default, the **Username** field is disabled.

4. In the Edit Internal Provisioner screen, modify the fields required.
5. **(Optional)** Select **Change Password** to modify the Internal Provisioner's password. You must specify **New Password** and **Confirm New Password**.
6. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   The modified internal provisioners details are displayed in the Internal Provisioners screen.

Field Descriptions

Use data in the following table to use Edit Provisioner screen.

Name	Description
First Name and **Last Name**	Modify the First Name, and Last Name of the Provisioner account details. The length of the name can be 30 characters or less. **Note:** These fields should only contain letters, number, hyphen, and underscore.
Change Password	Select this to modify the current password details. If selected, you must also specify New Password and Confirm New Password. Change Password is optional.
New Password and **Confirm New Password**	Configures a new password for the Provisioner account. Since Guest and IoT Manager encrypts the password, ensure that you make a note of the password for future reference. **Note:** These fields should only contain alphanumeric and special characters. Only these special characters are allowed : `! @ # $ % ^ & * ( ) + - .`
Email	Modify the email address of the Provisioner, if required.
Comments	Modify the additional information, if required.
Member of Onboarding Template(s)	Reassign the Internal Provisioner to one or more Onboarding Template, if required.

Filtering Internal Provisioners

Use this procedure to filter Internal Provisioner account.

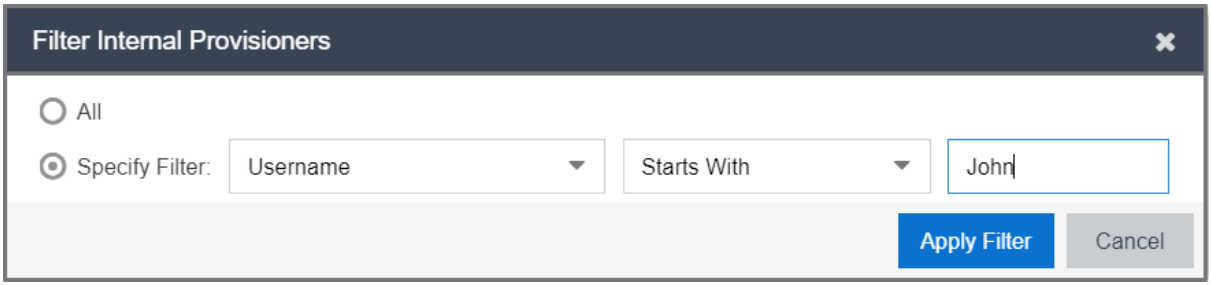
Procedure

1. In the navigation pane, click **Provisioner** > **Internal Provisioner** tab.

   The Internal Provisioners screen is displayed with the list of provisioners currently authorized to set up Guest access.

2. In the Internal Provisioners screen, click **Show Filter** to narrow the search parameters and quickly find all similar provisioners.

   The Filter Internal Provisioner screen is displayed.



3. In the Filter Internal Provisioner screen, do the following:
   a. Select **All**, and click **Apply Filter** to view all the Internal Provisioners.
   b. Select **Specify Filter**; include the additional fields to narrow the quick search and click **Apply Filter**.
   c. Click **Cancel** to cancel the changes.

   Use the paging control at the bottom of the list to move forward or backward by one page, or to the first or last page of the list. You can control number of records to be displayed per page and also click an individual page number to navigate to the specific page. Click **Refresh** icon to refresh the view.

Field Descriptions

Use data in the following table to use Filter Internal Provisioner screen.

Name	Description
All	Displays the list of all the Internal Provisioner account data.
Specify Filter	Simplifies the search parameters to quickly find the selected search criterion that includes specified parameters. Additionally you can also enter the operator conditions to match the selected search criteria to obtain precise search results of each Provisioner. The search conditions are: • **Username** • **First Name** • **Last Name** • **Email** The search conditions operators are: • **Starts with** • **Ends with** • **Contains** • **Equals** • **Not Equals**

Chapter 8: Configuring Self-Services

This module is intended for Guest and IoT Manager Administrator to create Self-Service Provisioner. A Self-Provisioned Guest User and Devices that appears as a Guest User account and Devices is managed similar to other Guest User account and Devices. For more information, see *ExtremeControl Guest and IoT Manager Configuration*.

Configuring Self-Service Provisioners

The **Self-Service Provisioners** tab in Self-Services menu allows you to select the Service Type and Onboarding Template to create Self-Service URLs and also creates a dedicated Provisioner account for each Self-Service. The dedicated Provisioner owns the Guest User and Devices created through the Self-Service. You can direct arriving Guests to these Self-Service URLs to use the self-registering feature.

Generally, an arriving Guest uses a kiosk computers / BYOD devices to fill out the Self-Provisioning information. When their account is created, this service sends the login credentials to the user through email, SMS message, or to a front desk personal who can print it as hard copy.

Note:

Ensure that you have configured email and / or SMS gateway details to send account access details. For more information, see Enabling E-mail Notification on page 55 and Adding SMS Gateway on page 57.

Creating Self-Service Provisioners

Use this procedure to create a Self-Service Provisioners.

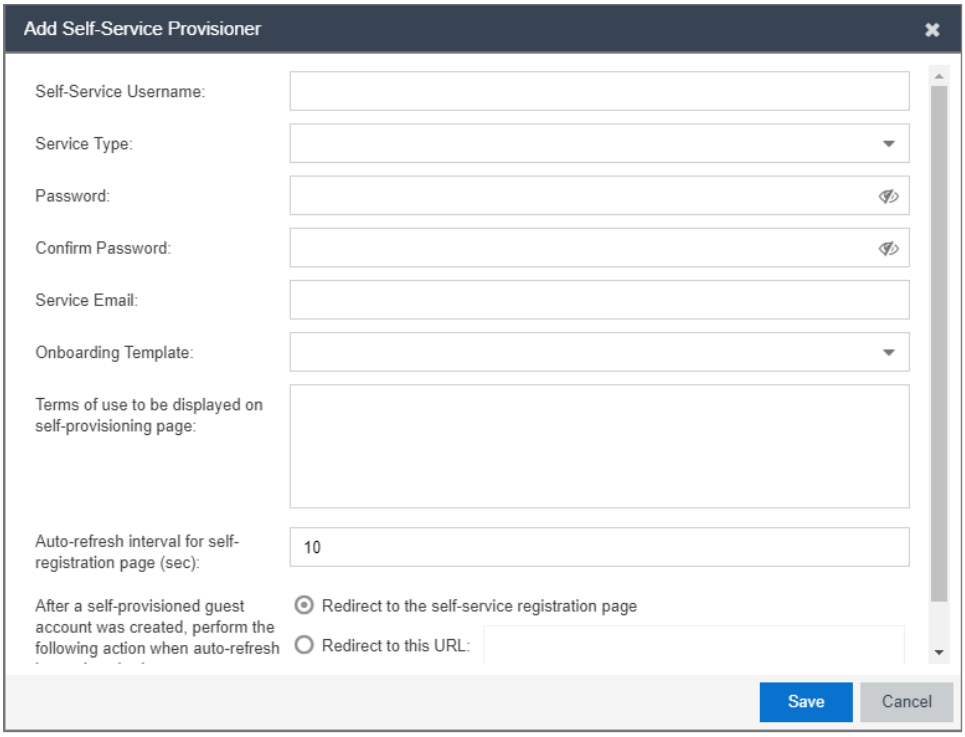
Procedure

1. In the navigation pane, click **Self-Services** > **Self-Service Provisioners** tab.

   The Self-Service Provisioners screen is displayed.

2. In the Self-Service Provisioners screen, click **Add** to add a Self-Service Provisioner.

   The Add Self-Service Provisioner screen is displayed.



3. In the **Self-Service Username** field, enter the name of the Provisioner account.
4. In the **Service Type** field, select the required service type from the drop-down list.

   If you select **Device** option as **Service Type**, the **User account with provisioning rights must be successfully authenticated to create a device account** and **Confirmation Template** fields are enabled.

   - Select **User account with provisioning rights must be successfully authenticated to create a device account**, to allow the successfully authenticated Provisioners to create a Device account.
   - Use the **Confirmation Template** field, to specify how the confirmation messages needs to be displayed.
5. In the **Password**, **Confirm Password** and **Service Email** fields, configure the Provisioner login credentials.
6. In the **Onboarding Template** field, select the required Onboarding Template from the drop-down list to set the access restrictions.
7. In the **Terms of use to be displayed on self-provisioning page** field, enter the terms of use to be displayed on the Self-Provisioning page.

8. In the **Auto-refresh interval for self-registration page (sec)** field, enter the value for the refresh interval and select the required auto refresh option in the **After a self-provisioned guest account is created, perform the following action when auto-refresh interval expired** field.
9. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   The created Self-Service Provisioner is displayed in the Self-Service Provisioners screen with all the added details.
10. **(Optional)** Select the required Self-Service Provisioner and click **Edit** to modify a Self-Service Provisioners. For more information, see Modifying Self-Service Provisioners on page 119.
11. **(Optional)** Select the required Self-Service Provisioner(s) and click **Delete** to delete the Self-Service and its Provisioner account.

    Tip:

    Use Ctrl / Shift to select multiple records to delete.

    When you delete a Self-Service Provisioner(s), the application retains all Guest Users and Device Accounts that were provisoned by the deleted Self-Service Provisioner.

Field Descriptions

Use data in the following table to use Add Self-Service Provisioner screen.

Name	Description
Self-Service Username	Configures the name of the Provisioner account that manages the Self-Service and also used in URL of the Self-Service. The length of the name can be 30 characters or less. **Note:** These fields should only contain letters, number, hyphen, and underscore.
Service Type	Configures basic properties of Self-Provisoning Service. The Registration Page does not exist until you specify the options. The two options are: • **Guest User** If you select **Guest User** option as **Service Type** and the **Onboarding Template** of the type as **Guest User**, the users can create their account directly. If the **Onboarding Template** is of type **Sponsor**, then Sponsor Approval is required. For more information, see Configuring Sponsor Approval on page 74. The Guest User has to provide basic information such as first name, last name, email, mobile number and so on in the New User Registration Page. The information collected in based on the associated Onboarding Template.

Table continues…

Name	Description
	In addition, if the Sponsor approval is required then user must specify the Sponsor details or it will be auto-populated based on the type of the Sponsor selected in the associated Onboarding Template. The Sponsor receives an email with Guest User's details and option to Approve or Deny Guest User's access request. **Note:** Guest User is granted access only after the Sponsor has approved the access request. • **Devices** If you select **Device** option as **Service Type**, then you must select **Onboarding Template** of the type a **Devices** only.
Password and **Confirm Password**	Configures the password of the Provisioner. Since Guest and IoT Manager encrypts the password, ensure that you make a note of the password for future reference. **Note:** These fields should only contain alphanumeric and special characters. Only these special characters are allowed : `! @ # $ % ^ & * ( ) + - .`
Service Email	Configures the email address of the Provisioner.
Onboarding Template	Associates this Onboarding Template to the Self-Service Provisioner.
User account with provisioning rights must be successfully authenticated to create a device account	Select to provision a Device only after successful authentication of the Provisioner. This field is enabled, if the selected Service Type is Device only.
Confirmation Template	Specifies the confirmation message format and also contains the variables to display the Username and MAC address as part of the confirmation message. You can also specify variables to display the start time and end time of the Device account in the confirmation message. This field is enabled, if the selected Service Type is Device only. **Note:** If you have not provided any information in this field, then the default template will be used.
Terms of use to be displayed on self-provisioning page	Displays terms and condition information in the Self-Service Provisioning page.
Auto-refresh interval for self-registration page (sec)	Configures the time value for the refresh interval of the Self-Service Provisioning page. Default value is 10 seconds.
After a self-provisioned guest account is created, perform the following action	Specifies the actions that needs to be performed after the Guest account creation. The options are: • **Redirect to the self-service registration page**

Table continues…

Name	Description
when auto-refresh interval expired	• **Redirect to the specified URL** • **Don't do anything**

Modifying Self-Service Provisioners

Use this procedure to modify a Self-Service Provisioners.

Procedure

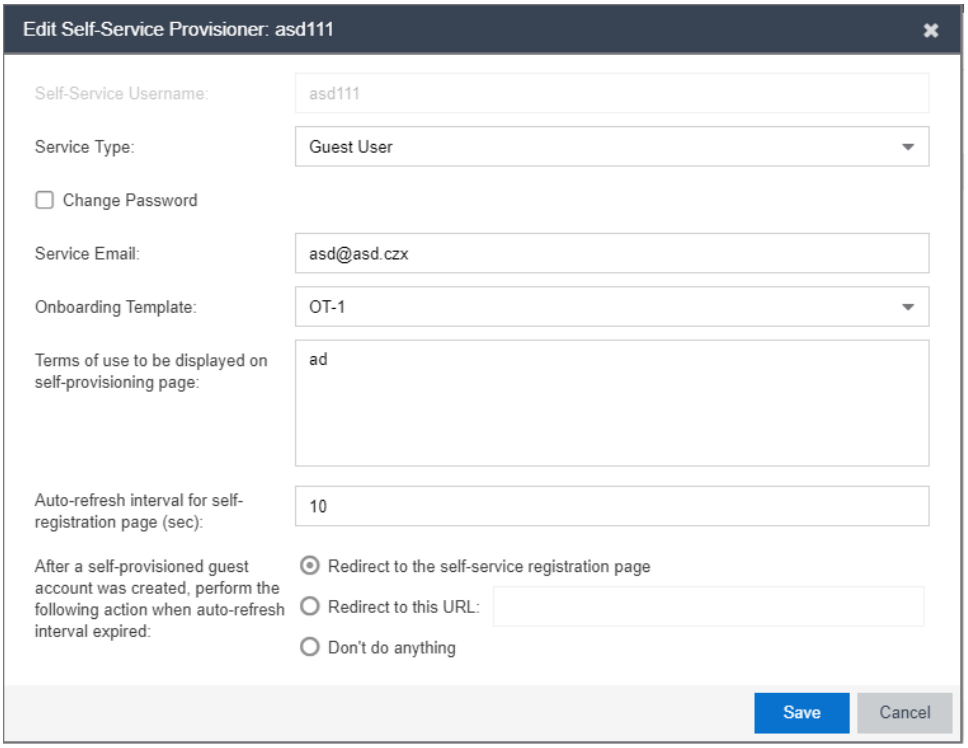
1. In the navigation pane, click **Self-Services** > **Self-Service Provisioners** tab.

   The Self-Service Provisioners screen is displayed with list of Self-Service Provisioners and their accounts.

2. In the Self-Service Provisioners screen, select the Self-Service Provisioners account that you wish to modify.

3. Click **Edit**, to view the Provisioner account details.

   The Edit Self-Service Provisioner screen is displayed.



Note:

You can also edit by double-clicking the required Self-Service Provisioner account from the list. By default, the **Self-Service Username** field is disabled.

4. In the Edit Self-Service Provisioner screen, modify the fields required.
5. **(Optional)** Select **Change Password** to modify the Self-Service Provisioner's password. You must specify New Password and Confirm New Password.
6. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   The modified Provisioners details are displayed in the Self-Service Provisioners screen.

Field Descriptions

Use data in the following table to use Edit Self-Service Provisioner screen.

Name	Description
Service Type	Modify the Service Type. The Options are : Guest User and Device. Device option enables **User account with provisioning rights must be successfully authenticated to create a device account** and **Confirmation Template** field.
Change Password	Select this to modify the current password details. If selected, you must also specify New Password and Confirm New Password. Change Password is optional.
New Password and **Confirm New Password**	Modify the password and reconfirm. Since Guest and IoT Manager encrypts the password, ensure that you make a note of the password for future reference. **Note:** These fields should only contain alphanumeric and special characters. Only these special characters are allowed : ! @ # $ % ^ & * ( ) + - .
Service Email	Modify the email address of the Provisioner, if required.
Onboarding Template	Select the different Onboarding Template from the drop-down list to associate, if required.
User account with provisioning rights must be successfully authenticated to create a device account	Select to provision a Device only after successful authentication of the Provisioner. This field is enabled, if the selected Service Type is Device only.
Confirmation Template	Modify the confirmation message, if required This field is enabled, if the selected Service Type is Device only. **Note:** If you have not provided any information in this field, then the default template will be used.

Table continues…

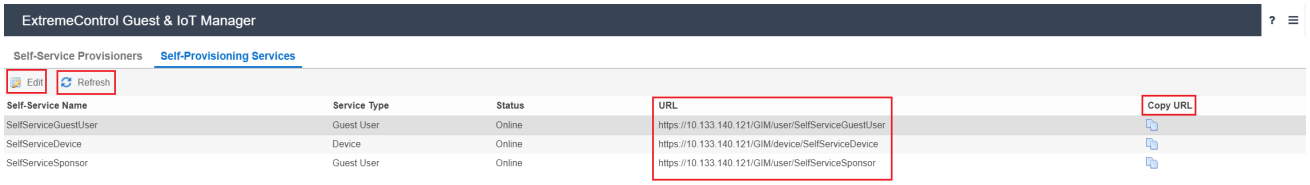
Name	Description
Terms of use to be displayed on self-provisioning page	Modify the terms of use message, if required.
Auto-refresh interval for self registration page (sec)	Modify the auto refresh value, if required.
After a self-provisioned guest account is created, perform the following action when auto-refresh interval expired	Specifies the options that needs to be performed once the Self-Provisioners Guest account is created. The options are: • **Redirect to the self-service registration page** • **Redirect to the specified URL** • **Don't do anything**

Viewing Self-Provisioning Services

The **Self-Provisioning Services** tab in Self-Services menu allows you to view and identify Self-Provisioning Services that you have created. The created Self-Provisioning Services are displayed along with Self-Service Name, Service Type, Status, and the URL. The different URL represents the particular service type pages that has been generated for registering the Guest Users and Devices.

You can also copy these URLs to access the Self Service page. For more information on using Self-Provisioning page, see Using Self-Provisioning Services on page 154.

Self Provisioning Services



Chapter 9: Managing Guest Users

This module is intended for Guest and IoT Manager Administrator to manage and carry out bulk Guest User operations. A Guest User account can be permanent, temporary, automatically expiring account with specific limited rights to use the network based on the associated Onboarding Template.

Accessing Guest Users

The **Guest Users** tab in the Guest Users menu allows you to view and manage all the users created by the Provisioner(s).

Using Guest User Features

Use this procedure to manage the Guest User Administrator features.

Procedure

1. In the navigation pane, click **Guest Users** > **Guest Users** tab.

   The Guest Users screen is displayed along with the user details created by the Provisioner(s). By default, 25 users are displayed and you can extend up to 75 users.

   You can also click the column headers to sort the list view by that column. Click the column header a second time to reverse the direction of the sort.

2. Select the required user and click **View** to view the selected user information.
3. **(Optional)** Select the required Guest User(s) and click **Extend Expiration** to extend the validity of Guest User(s) account. The validity is extended based on the duration specified during the creation.

   The duration of each selected Guest User is calculated as:

   DURATION = END_TIME – START_TIME

   Then the account is modified to :

   START_TIME = CURRENT_TIME

END_TIME = START_TIME + DURATION

Extend Expiration Example:

Consider two Guest Users, User 1 valid for a duration of one month and User 2 is valid for a duration of two months, both are expiring tomorrow and the current time is 02:00 P.M. When you select these two accounts and click **Extend Expiration** option, their expiry is extended as follows:

a. User 1 is extended as Start Time = 02:00 P.M. today and End Time = 02:00 P.M. today + 1 month.

b. User 2 is extended as Start Time = 02:00 P.M. today and End Time = 02:00 P.M. today + 2 months.

Note:

The Provisioners can use **Extend Expiration** option to extend the duration of expiry for expired Guest User account(s) also.

Expiry of First Login Pending and Permanent Guest User accounts cannot be extended.

4. **(Optional)** Select the required user and click **Resend Password** to send the password to Guest Users.

   When multiple Guest Users are selected to resend the password, the application validates the following prior sending the password:

   - Notification options has either SMS / Email or both enabled.
   - Account is not locked / expired.

5. **(Optional)** Select the required user account(s) and click **Delete** to remove the selected Guest User account(s).

   Tip:

   Use Ctrl / Shift to select multiple records to delete.

6. **(Optional)** In the Guest Users screen, click **Show Filter** to specify the search parameters and quickly find all similar records. The filter is applied to all columns displayed in the list view. For more information, see Searching Specific Guest Users on page 123.

   Note:

   Use the paging control at the bottom of the list to move forward or backward by one page, or to the first or last page of the list. You can control number of records to be displayed per page and also click an individual page number to navigate to the specific page. Click **Refresh** icon to refresh the view.

Searching Specific Guest Users

Use this procedure to retrieve specific Guest Users based on the search parameters.

Procedure

1. In the navigation pane, click **Guest Users** > **Guest Users** tab.

   The Guest Users screen is displayed along with the user details created by the Provisioner. By default, 25 users are displayed and you can extend up to 75 users.

2. In the Guest User screen, click **Show Filter** to specify the search parameters and quickly find all similar records.

   The Filter Guest Users screen is displayed:

3. To retrieve specific Guest Users, do the following:
   a. For Guest Users added by the Provisioner:
      a. In the **Specify Filter** section, select **Provisioner** from the drop-down list.
      b. Enter the operation (Starts with, Equals, Not Equals, Contains, Ends With) and the name of the Provisioner.
      c. Click **Apply Filter**. A list of Guest Users provisioned by the selected Provisioner are displayed.
   b. For Guest Users that belong to an Onboarding Template:
      a. In the **Specify Filter** section, select **Onboarding Template** and required template of the selected Onboarding Template from the drop-down list.
      b. Click **Apply Filter**. A list of guest users that belong to the selected Onboarding Templates are displayed.
   c. For Guest Users First Login Pending Accounts:
      a. In the **Specify Filter** section, select **First Login Pending and Created Before** and the required search conditions operator from the drop-down list.
      b. Enter the date in YYYY/MM/DD format or click the calendar icon to select a date.
      c. Enter the **Time** and select AM or PM from the drop-down list.
      d. Select the **Time Zone** from the drop-down list.
      e. Click **Apply Filter**. The list of all the first login pending accounts created before the specified date as entered are displayed.
   d. For Guest Users based on Sponsor Response:
      a. In the **Specify Filter** section, select **Sponsor Response** and the required search values from the drop-down list.

         The search values are:

         - Approved
         - Denied
         - Pending
         - Auto-Approved

- Auto-Denied
- Not Applicable

b. Click **Apply Filter**. The list of all the Guest Users that have the selected Sponsor Response are displayed.

e. For Guest Users activated in last X number hours:

a. In the **Specify Filter** section, select **Guest Users Activated in the Last** from the drop-down list and enter number of hours in the Hours field. You can search up to a maximum of two years from the current time.

b. Click **Apply Filter**. The list of all the Guest Users activated in last X number hours are displayed.

f. For expired Guest User account details:

a. In the **Specify Filter** section, select **Expired Guest Users** from the drop-down list.

b. Click **Apply Filter**. The list of all the expired Guest Users accounts are displayed.

Tip:

When Guest User accounts are expired, the affected accounts cannot access the network. You can also use this procedure to delete all the expired Guest User accounts.

c. **Optional**: Select the required expired Guest User(s) and click **Delete** to remove the guest account.

Note:

Use Ctrl / Shift to select multiple records to delete.

Chapter 10: Managing Devices

This module is intended for Guest and IoT Manager Administrator to carry out bulk operations on the Device records. A Device record can be permanent, temporary, automatically expiring record with specific limited rights to use the network based on the associated Onboarding Template.

Accessing Devices

The **Devices** tab in the Devices menu allows you to view and manage all the Device actions created by the Provisioner(s).

Using Devices Features

Use this procedure to manage the Device Administrator features. The Administrator can also perform bulk operations of Devices.

Procedure

1. In the navigation pane, click **Devices** > **Devices** tab.

   The Devices screen is displayed along with the Device details created by the Provisioner(s). By default, 25 Devices are displayed and you can extend up to 75 Devices.

   You can also click the column headers to sort the list view by that column. Click the column header a second time to reverse the direction of the sort.

2. Select the required Device record and click **View** to view the Device record summary.
3. **(Optional)** Select the required Device record(s) and click **Extend Expiration** to extend the validity duration of the Device record(s). The validity is extended based on the duration specified during the creation.

   The duration of expiry of each selected Devices is calculated as:

   DURATION = END_TIME – START_TIME

   Then the account is modified to :

   START_TIME = CURRENT_TIME

END_TIME = START_TIME + DURATION

Extend Expiration Example:

Consider two Devices, Device 1 valid for a duration of one month and Device 2 is valid for a duration of two months, both are expiring tomorrow and the current time is 02:00 P.M. When you select these two Devices and click **Extend Expiration** option, their expiry is extended as follows:

a. Device 1 is extended as Start Time = 02:00 P.M. today and End Time = 02:00 P.M. today + 1 month.

b. Device 2 is extended as Start Time = 02:00 P.M. today and End Time = 02:00 P.M. today + 2 months.

Note:

The Provisioners can use **Extend Expiration** option to extend the duration of expiry for expired Device record(s) also.

Expiry of First Login Pending and Permanent Device record(s) cannot be extended.

4. **(Optional)** Select the required Device record(s) and click **Delete** to remove Device record(s).

Tip:

Use Ctrl / Shift to select multiple records to delete.

5. **(Optional)** In the Devices screen, click **Show Filter** to specify the search parameters and quickly find all similar records. The filter is applied to all columns displayed in the list view. For more information, see Searching Specific Devices on page 127.

Note:

Use the paging control at the bottom of the list to move forward or backward by one page, or to the first or last page of the list. You can control number of records to be displayed per page and also click an individual page number to navigate to the specific page. Click **Refresh** icon to refresh the view.

Searching Specific Devices

Use this procedure to retrieve specific Device record summary based on the search parameters

Procedure

1. In the navigation pane, click **Devices** > **Devices** tab.

   The Devices screen is displayed along with the Device details created by the Provisioner. By default, 25 Devices are displayed and you can extend up to 75 Devices.

2. In the Devices screen, click **Show Filter** to specify the search parameters and quickly find all similar records.

The Filter Devices screen is displayed:

3. To retrieve the specific Devices, do the following:
    a. For Devices added by the Provisioner:
        a. In the **Specify Filter** section, select **Provisioner** from the drop-down list.
        b. Enter the operation (Starts with, Equals, Not Equals, Contains, Ends With) and the name of the Provisioner.
        c. Click **Apply Filter**. A list of Devices provisioned by the selected Provisioner are displayed.
    b. For Devices that belong to an Onboarding Template:
        a. In the **Specify Filter** section, select **Onboarding Template** and required template of the selected Onboarding Template from the drop-down list.
        b. Click **Apply Filter**. A list of Devices that belong to the selected Onboarding Templates are displayed.
    c. Devices activated in last X number of hours:
        a. In the **Specify Filter** section, select **Devices Activated in the Last** and enter the number of hours in the **Hours** field. You can search up to a maximum of two years from the current time.
        b. Click **Apply Filter**. The list all the selected Devices activated in last X number hours are displayed. Here, X represents the number of hours as entered in **Hours** field are displayed.
    d. For pending Devices list:
        a. In the **Specify Filter** section, select **First Login Pending and Created Before** and the required search conditions operator from the drop-down list.
        b. Enter the date in YYYY/MM/DD format or click the calendar icon to select a date.
        c. Enter the **Time** and select AM or PM from the drop-down list.
        d. Select the **Time Zone** from the drop-down list.
        e. Click **Apply Filter**. The list of all the first login pending Device records created before the specific date as entered are displayed.
    e. For Device record expiring in limited hours:
        a. In the **Specify Filter** section, select **Devices Expiring in the Next** and enter the number of day in the **Days** field. You can search up to a maximum of two years from the current time.
        b. Click **Apply Filter**. The list of all the Device records expiring in next few days are displayed.
    f. For expired Device record:
        a. In the **Specify Filter** section, select **Expired Devices** from the drop-down list.

b. Click **Apply Filter**. The list of all the expired Device records are displayed.

c. **Optional**: Select the required expired Device and click **Delete** to remove the Device record(s).

Note:

You can also use this procedure to delete all the expired Device records.

Chapter 11: Configuring Guest and Devices

This module is intended for Guest and IoT Manager Provisioner to create and manage Guest User and Device account(s). Your Provisioner account is part of one or more Onboarding Templates that establish rights, such as the maximum lifetime of accounts you create, and which “Single Membership” and “Multiple Memberships” Access groups you can provide to those accounts.

A Guest User is a visitor, or other temporary user, to whom you grant specific, limited rights to use your network. As a Provisioner you can set the duration of access for the Guest User. The account can be valid for only a few minutes, hours, for a number of weeks, or permanent. The account expires automatically after a specified period of time. However, if the account expires, you can renew it, if needed.

When a Guest User is created, you can determine how and when the user can use your network. These are the groups that can be configured in Access Control Engine. You can:

- 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.
- Determine the network ports or access points the user can connect. That is, you can specify the access points or conference room network jacks that allows the user to connect.
- Specify the segments of your network the user can reach once connected. For example, you can give a user only Internet access or you can give access to the corporate Intranet.

Configuring Guests

The **Guest Users** tab in Guest Users menu provides complete control over the user account creation process. Guest User features for managing guest accounts allows you:

- Create guest accounts
- View and manage guest accounts
- Handle the account activation time for network access usage and the duration.
- Remove the guest accounts automatically after expiration.

Note:

The assigned Onboarding Template needs to permit the Guest User management operations to the Provisioner.

Guest User Connections

When guests have their temporary Username and Password, they can connect in one of two ways:

- **Standard Login**: In most networks, the Guest User plugs in their Device into the wired network or connects to an open wireless access point. The networking client (known as the “supplicant”) on the user’s Device brings up a login dialog. The user can provide the login credentials for the configuration.
- **Captive Portal**: If the captive portal tool is used, the user plugs in their Device into the wired network or connects to an open wireless access point and launch web browser. The captive portal intercepts the user’s web traffic and displays a login page in the browser. The user can provide the login credentials.

Creating Guest User Account

Use this procedure to create a Guest User account.

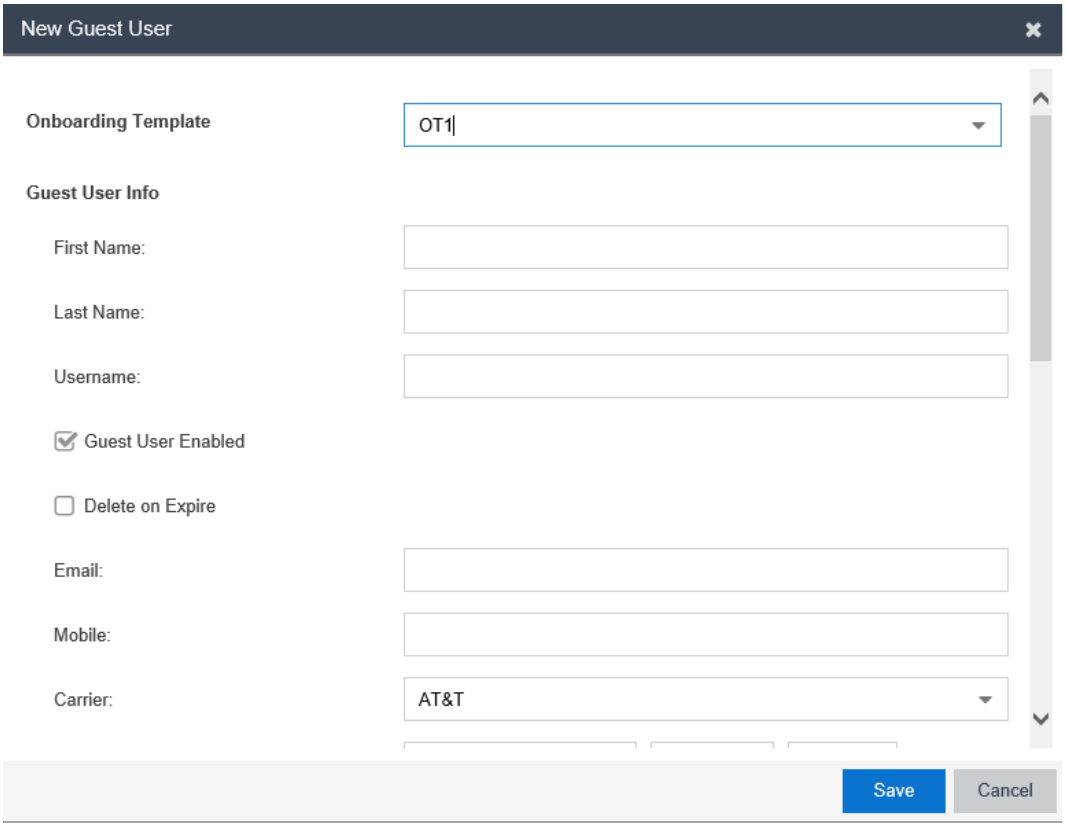
Procedure

1. In the navigation pane, click **Guest Users** > **Guest Users** tab.

   The Guest User screen is displayed.

2. In the Guest User screen, click **Add** to create a new Guest User.

   The New Guest User screen is displayed.



3. In the **Onboarding Template** field, select the required Onboarding Template the Guest User is to be associated with from the drop-down list.

   To associate the Guest User Account with Vouchers, select Creating Guest User Account using Vouchers on page 136.

4. In the **Guest User Info** section, configure the account details as required.
5. In the **Send Notification** section, configure the notification conditions as required.
6. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   The *Successful Guest Creation* message is displayed along with Username and Password details if specified in the Onboarding Template.

   The added new user is displayed in the Guest User screen along with all the specified information and also sends Email / SMS notifications to the user.

7. **(Optional)** Select the required Guest User(s) and click **Extend Expiration** to extend the validity of Guest User(s) account. The validity is extended based on the duration specified

during the creation. For more information, see Extending Expiry of Guest User Account on page 142.

8. **(Optional)** Select the required Guest User(s) and click **Resend Password** when Guest User(s) need to recover the account password.

   The password is shared via email / SMS or both depending on the notification options of the Onboarding Template to which the user is associated with.

   The following checks are performed prior the password is shared when one or more users are selected:

   - Notification options has either SMS / Email or both enabled
   - Account is not locked / expired

9. **(Optional)** Select the required Guest User and click **Edit** to modify Guest User accounts. For more information, see Modifying Guest User Account on page 139.
10. **(Optional)** Select the required Guest User(s) and click **Delete**, to remove accounts.

    Tip:

    Use Ctrl / Shift to select multiple records to delete.

11. **(Optional)** Click **Show Filter** to specify the search parameters and quickly find all similar records. The filter is applied to all columns displayed in the list view. For more information, see Finding Guest User Account on page 140.
12. **(Optional)** Select the Guest User and click **Print**, to print the account summary.

    Note:

    Use the paging control at the bottom of the list to move forward or backward by one page, or to the first or last page of the list. You can control number of records to be displayed per page and also click an individual page number to navigate to the specific page. Click **Refresh** icon to refresh the view.

Field Descriptions

Use data in the following table to use New Guest User screen. The fields are enabled based on the associated Onboarding Template settings.

Name	Description
Onboarding Template	Specifies the list of Onboarding Templates that the Provisioner is a member of. The provisioner can add the Guest User to any one of the available Onboarding Templates. The Onboarding Templates imposes certain account guidelines (for example, prompt the Username, auto-generation of the password, maximum validity period, allowable access groups, and so on), according to how the Administrator has configured the Guest User account details for

Table continues…

Name	Description
	the particular selected Onboarding Template. As a result, the fields and defaults of the screen changes when you select a Onboarding Template. **Note:** Onboarding Template limits the rights that can be granted to the user.
First Name and Last Name	Configures the first and last name of the Guest User. The length of the name can be 30 characters or less. **Note:** These fields should only contain letters, number, hyphen, and underscore.
Username	Generates Username for the created users first name. Ensure that the first name entered does not have any spaces. The length of the name can be 30 characters or less. **Note:** You can edit the Username and provide a unique name, if the Administrator has selected **Generate Username with** option while creating an Onboarding Template. User Name is auto-generated, if the Administrator has selected **Random Generated Password** option while creating an Onbarding Template. This field should only contain alphanumeric and special characters. Only these special characters are allowed : `! @ # $ % ^ & * ( ) + - .` For more informaiton about configuring the guest user account details, see *ExtremeControl Guest and IoT Manager Configuration*.
Password	Specifies the password for the Guest User login. The password must meet the specified complexity checks. If the Onboarding Template is configured to auto-generate password, this field does not appear while creating a new Guest User.
Delete on Expire	Deletes the Guest User from the Access Control Engine. Select this option to automatically remove expired guest account. If you do not select this option, you need to manually remove the guest account after it expires. The expired user accounts remains in the Access Control Engine. As a Provisioner you can renew or remove the expired accounts at any point of time. The account validity is indicated in RED color in the **End Time** column of Guest User screen attributes.
Email	Configures the email address of the Guest User.

Table continues…

Name	Description
	When this account is created, you can instruct Guest and IoT Manager Application to send a notification to specified or another address. For more information, see **Send Notification** row beneath.
Mobile	Configures the contact number of the Guest User. Guest and IoT Manager Application uses this number is to send account notification via SMS messaging.
Carrier / Provider	Specifies the list of phone carrier and provider service details.
Activate Account On	Configures the date and time at which the Guest User account is activated. The value in these fields defaults to the current date and time on the Guest and IoT Manager. You can also view the time zone that has been set to the current Onboarding Template. • **Date:** Enter the start date for activating Guest User account. The date should be in YYYY/MM/DD format. • **Time:** Enter the time in hours and minutes based on a 12-hour setting. The time should be in hh:mm:ss format. • **AM / PM:** Select the time of the day.
Activate On First Login	Specifies that guest account will be valid only after the first login. **Note:** This field is available only if the Administrator has selected **First Login** option while creating an Onboarding Template and the Provisioner selects the same Onboarding Template during Guest User account creation from the **Onboarding Template** drop-down list. The **Activate Account On** option is replaced by **Activate on First Login: Yes** option.
Duration	Configures the duration validity of the guest account. The account validity period starts from the activation time and lasts for the specified duration. By default, the application sets the durations to the maximum time period specified in the **Temporary Account Validity** field during creation of Onboarding Template. Specify the period as an integer and set the units by selecting minutes, hours, and days.
Single Membership Access Group	Specifies one of the access group that has been configured in the Onboarding Template.
Multiple Memberships Access Group	Configures the access to the Guest User. You can select multiple options. For example, if the access has to be provided for a specific department, the Administrator defines which access group are available for you.
Custom Fields: 1 to 6	Specifies the label values configured for Guest Users.
Send Notification	Specifies the address / number that is required to share the account notification details. The application automatically sends the notification via Email or SMS to the Guest and / or others to provide the new guest account details.

Table continues…

Name	Description
	A notification message has the format of Email / SMS template configured in the Onboarding Template of which the Guest User is a member. For more information about configuring account notification templates, see *ExtremeControl Guest and IoT Manager Configuration*. The options available are: • **Guest User Email**: Sends an email to guest with account details. The variables specified in the guest's **Onboarding Template** > **Email Template** field are sent. • **Other Email**: Sends the guest's account details to the address specified. The variables specified in the guest's **Onboarding Template** > **Email Template** field are sent. • **Password to Guest User Mobile Phone**: Sends an SMS message to guest with account details. The variables specified in the guest's **Onboarding Template** > **SMS Template** fields are sent. The options are available only if the Guest and IoT Manager Administrator has configured the Application to send messages. For more information about enabling e-mail notifications and configuring the SMS gateway or provider, see *ExtremeControl Guest and IoT Manager Configuration*.

Note:

Different types of Guest User accounts created based on the validity are:

- Permanent
- Temporary - Time Based
- Temporary - First Login

Creating Guest User Account using Vouchers

Use this procedure to create Guest User account(s) in bulk using vouchers.

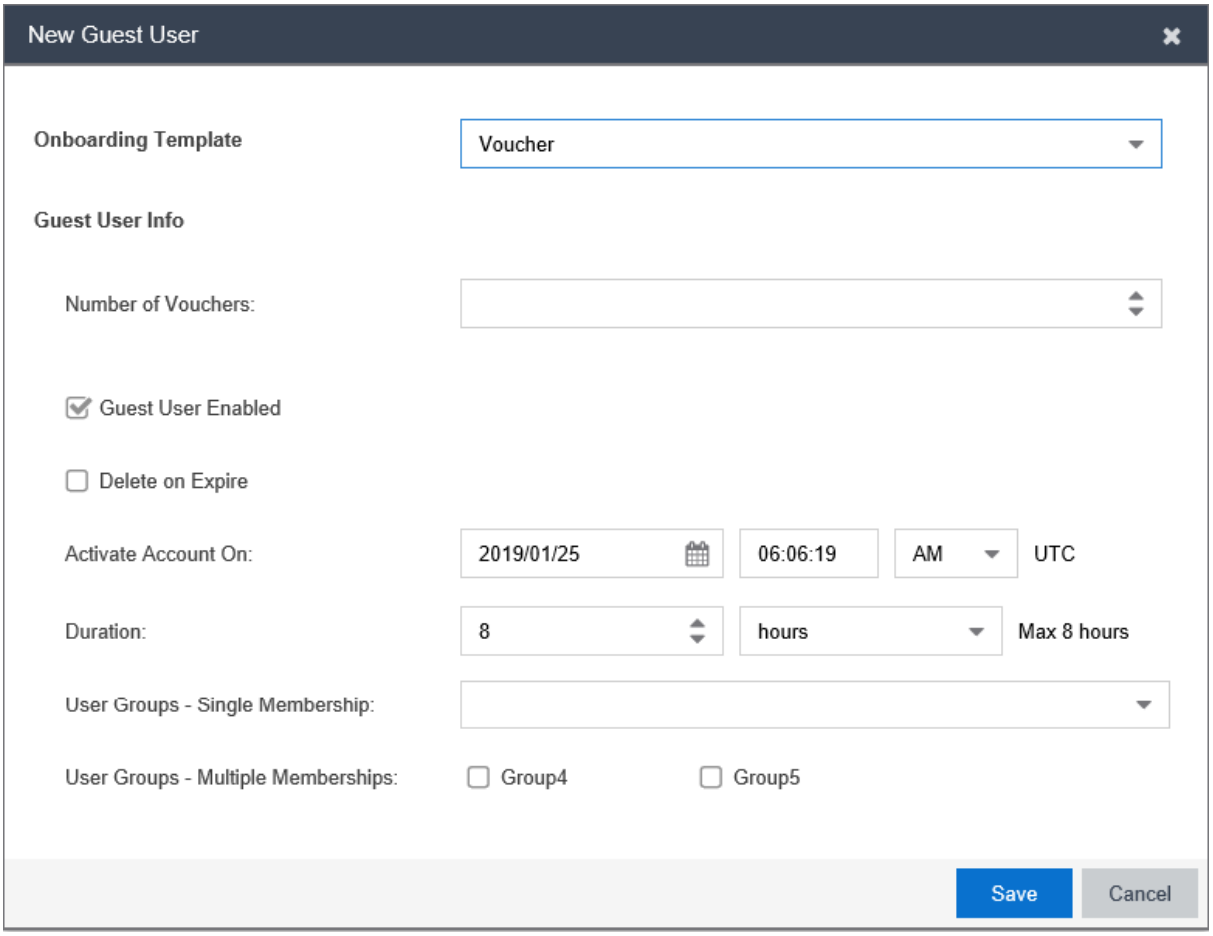
Procedure

1. In the navigation pane, click **Guest Users** > **Guest Users** tab.

   The Guest User screen is displayed.

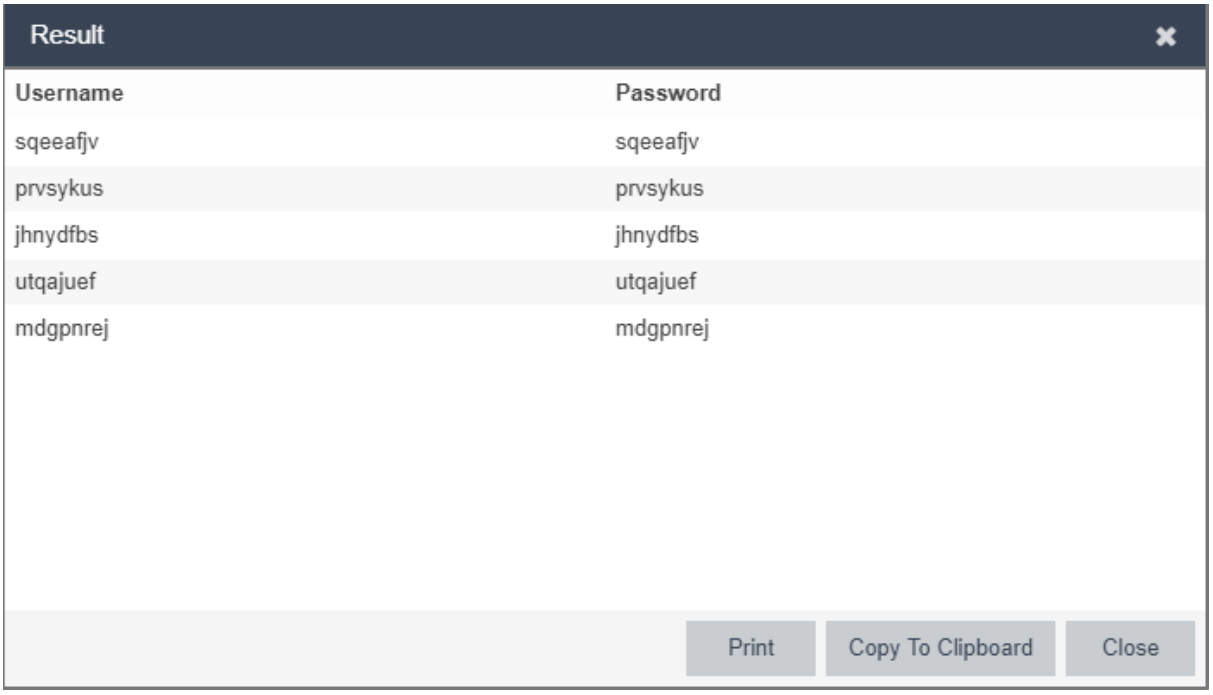
2. In the Guest User screen, click **Add** to create new Guest User(s).

   The New Guest User screen is displayed.



3. In the **Onboarding Template** field, select the required Voucher Onboarding Template the Guest User is to be associated with from the drop-down menu.
4. In the **Guest User Info** section, configure the account details as required.
5. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   The *Successful Guest Creation* message is displayed along with Username and Password details. The Provisioner can copy these details to the clipboard in the supported browsers or print them.



Field Descriptions

Use data in the following table to use New Guest User screen. The fields are enabled based on the associated Onboarding Template settings.

Name	Description
Onboarding Template	Specifies the list of Onboarding Templates that the Provisioner is a member of. The provisioner can add the Guest User to any one of the available Voucher type Onboarding Templates. The Onboarding Templates imposes certain account guidelines (for example, prompt the Username, auto-generation of the password, maximum validity period, allowable access groups, and so on), according to how the Administrator has configured the Guest User account details for the particular selected Onboarding Template. As a result, the fields and defaults of the screen changes when you select a Onboarding Template. **Note:** Onboarding Template limits the rights that can be granted to the user.
Number of Vouchers	Enter the number of vouchers as required. The maximum number of vouchers is 200.
Guest User Enabled	The option is selected by default and can be disabled by the Provisioner.
Delete on Expire	Deletes the Guest User from the Access Control Engine. Select this option to automatically remove expired guest account.

Table continues…

Name	Description
	If you do not select this option, you need to manually remove the guest account after it expires. The expired user accounts remains in the Access Control Engine. As a Provisioner you can renew or remove the expired accounts at any point of time. The account validity is indicated in RED color in the **End Time** column of Guest User screen attributes.
Activate Account On	Configures the date and time at which the Guest User account is activated. The value in these fields defaults to the current date and time on the Guest and IoT Manager. You can also view the time zone that has been set to the current Onboarding Template. • **Date:** Enter the start date for activating Guest User account. The date should be in YYYY/MM/DD format. • **Time:** Enter the time in hours and minutes based on a 12-hour setting. The time should be in hh:mm:ss format. • **AM / PM:** Select the time of the day.
Duration	Configures the duration validity of the guest account. The account validity period starts from the activation time and lasts for the specified duration. By default, the application sets the durations to the maximum time period specified in the **Temporary Account Validity** field during creation of Onboarding Template. Specify the period as an integer and set the units by selecting minutes, hours, and days.
User Groups - Single Membership	Specifies one of the access group that has been configured in the Onboarding Template.
User Groups - Multiple Memberships	Configures the access to the Guest User. You can select multiple options. For example, if the access has to be provided for a specific department, the Administrator defines which access group are available for you. This option is not mandatory and depends on the Provisioner to select this option.

Modifying Guest User Account

Use this procedure to modify Guest User accounts.

Procedure

1. In the navigation pane, click **Guest Users** > **Guest Users** tab.

   The Guest User screen is displayed with list of Guest User accounts created by the Provisioner.

2. Select the required user account to be modified and click **Edit**.

   You can also edit by double-clicking the required user account from the list.

The **Onboarding Template** field is editable only during creating an Guest User.

3. In the Guest User Info section, modify the fields required.
4. In the Send Notification section, select the required fields.

   Note:

   Guest User account(s) that was created using Voucher type Onboarding Template will not have this option.

5. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   The modified Guest User details are displayed in the Guest User screen.

6. **(Optional)** To modify the validity of a Guest User account, do the following:
   a. Select the required user account and scroll left to view the **Start Time** and **End Time** Guest User attributes column. The RED text indicates expired account.
   b. Double-click the user account to view the Edit Guest User screen.
   c. Modify the duration period in **Duration** field or modify the **Activate Account On** field to change the validity period to desired time frame.

   For more information, see Creating Guest User Account Field Descriptions on page 133.

Finding Guest User Account

Use this procedure to find a Guest User account.

Note:

Use the paging control at the bottom of the list to move forward or backward by one page, or to the first or last page of the list. You can control number of records to be displayed per page and also click an individual page number to navigate to the specific page. Click **Refresh** icon to refresh the view.

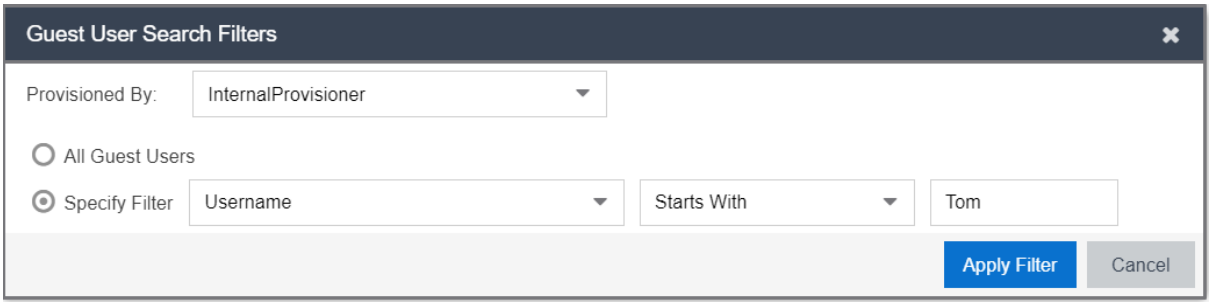
Procedure

1. In the navigation pane, click **Guest Users** > **Guest Users** tab.

   The Guest User screen is displayed with the list of Guest Users created by the Provisioner.

2. In the Guest User screen, click **Show Filter** to specify the search parameters and quickly find all similar user records.

   The Filter Guest Users screen is displayed.



3. In the **Provisioned By** field, select the required Onboarding Template or the Provisioner who has created the guest account from the drop-down list.
4. To search the Guest Users:
   - Select **All Guest Users** to view all the Guest Users.
   - Select **Specify Filter**; include the additional fields to specify the quick search.
5. Click **Apply Filter**.

   The corresponding records are displayed in the Guest User screen table.

   In the Guest User screen, select the required Guest User and scroll towards left to view the permanent access user accounts. The **End Time** Guest User attributes column status is displayed as blank **(–)**.

Field Descriptions

Use data in the following table to use Filter Guest User screen.

Name	Description
Provisioned By	Specifies the Provisioner name or the Onboarding Template(s) that the Guest User belongs to. The Provisioner can add the Guest User to any one of the available Onboarding Templates.
All Guest Users	Displays the list of all the users available for the selected option in the **Provisioned By** field.
Specify Filter	Simplifies the search parameters to quickly find the selected search criterion that includes specified parameters. Additionally you need to enter the operator conditions to match the selected search criteria to obtain precise search results of the selected Onboarding Template. The search conditions are: • **User Name** • **First Name** • **Last Name** • **Email** • **SMS Address** • **Start Time**

Table continues…

Name	Description
	• **End Time** • **Guest User Activated in the Last**: Fetches all the Guest User records activated in the last X number of hours. • **First Login Pending and Created Before**: Fetches all the Guest User records that have been created before the X date entered and awaiting first login. • **Guest Users Expiring in the Next**: Calculates and fetches the users according to: CURRENT_TIME < END_TIME < CURRENT_TIME + X days 'X' is a variable here. So, if you want to filter all Guest Users expiring tomorrow, you can select this filter condition. • **Expired Guest Users**: Fetches all the expired Guest User records. • **Sponsor Response** • **Sponsore Email** The search conditions operators depends on the selected search conditions. Some conditions have multiple condition operators. For example, you can search for multiple values when using the equal (=) or not equal !=) operators.

Extending Expiry of Guest User Account

Use this procedure to extend the duration of expiry of a Guest User account(s) at one go.

Procedure

1. In the navigation pane, click **Guest Users** > **Guest Users** tab.

   The Guest User screen is displayed with the list of users provisioned.

2. Select the required Guest User(s) and click **Extend Expiration** to extend the validity of Guest User(s) account. The validity is extended based on the duration specified during the creation.

   The duration each selected Guest User is calculated as:

   DURATION = END_TIME – START_TIME

   Then the account is modified to :

   START_TIME = CURRENT_TIME

   END_TIME = START_TIME + DURATION

   Extend Expiration Example:

Consider two Guest Users, User 1 valid for a duration of one month and User 2 is valid for a duration of two months, both are expiring tomorrow and the current time is 02:00 P.M. When you select these two accounts and click **Extend Expiration** option, their expiry is extended as follows:

a. User 1 is extended as Start Time = 02:00 P.M. today and End Time = 02:00 P.M. today + 1 month.

b. User 2 is extended as Start Time = 02:00 P.M. today and End Time = 02:00 P.M. today + 2 months.

Note:

The Provisioners can use **Extend Expiration** option to extend the duration of expiry for expired Guest User account(s) also.

Expiry of First Login Pending and Permanent Guest User accounts cannot be extended.

3. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

Configuring Devices

The **Devices** tab in Devices menu provides complete control over the Device records creation process. Device features allows you:

Devices feature allows you:

- Adding device records
- View and manage devices

Note:

The assigned Onboarding Template need to permit the Device management operations to the Provisioner.

Adding a Device Record

Use this procedure to add a Device record.

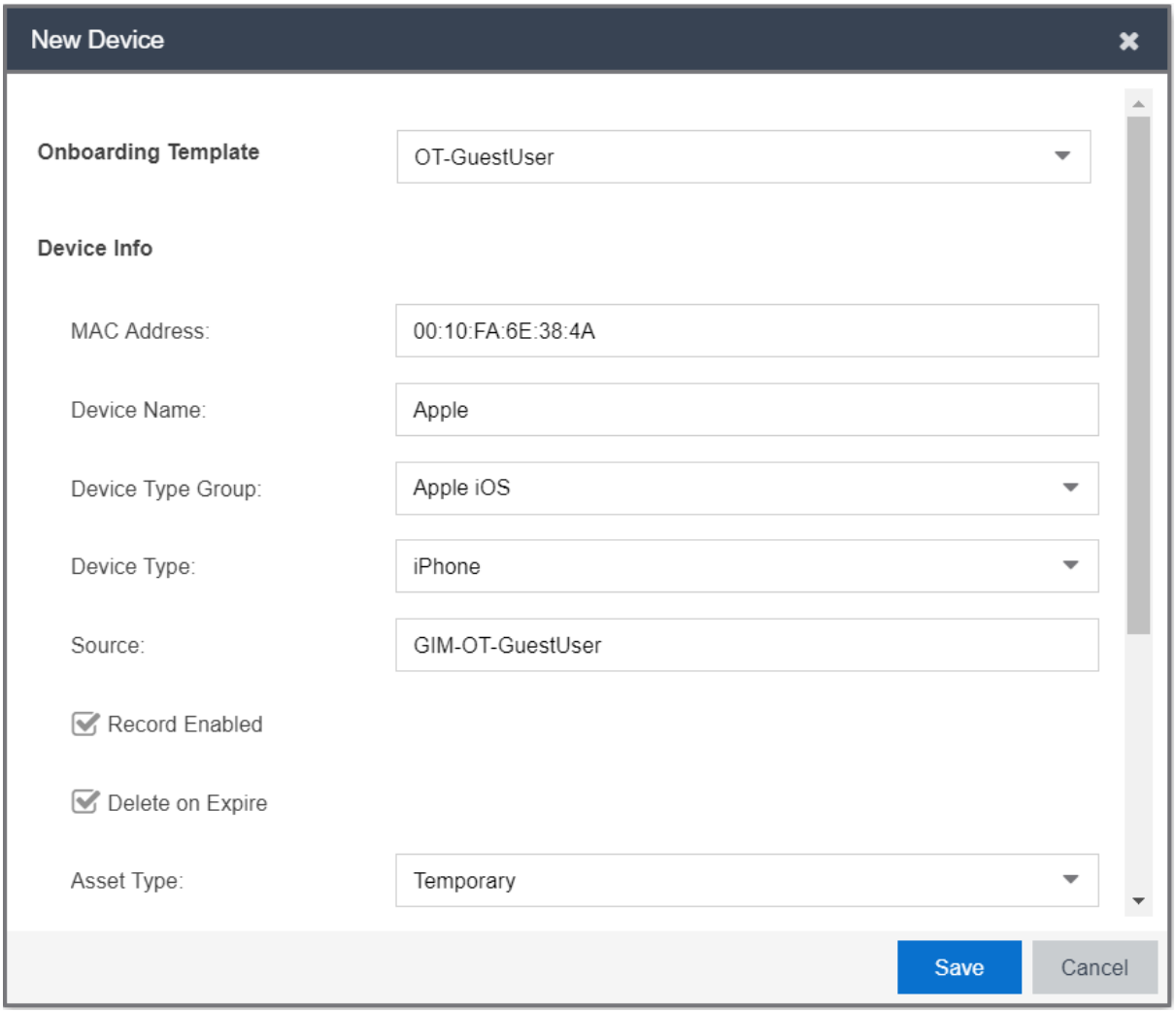
Procedure

1. In the navigation pane, click **Devices** > **Devices** tab.

   The Devices screen is displayed.

2. In the Devices screen, click **Add** to create a new Device record.

   The New Device screen is displayed.



3. In the **Onboarding Template** field, select the required Onboarding Template the Device is to be associated with from the drop-down list.
4. In the **Device Info** section, configure the Device details as required.
5. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   The added new Device record is displayed in the Devices screen along with all the specified information.
6. **(Optional)** Select the required Device record(s) and click **Extend Expiration** to extend the validity duration of the Device record(s). The validity is extended based on the duration specified during the creation. For more information, see Extending Expiry of a Device on page 149.
7. **(Optional)** Select the required Device record(s) and click **Delete** to remove the Device record(s).

Tip:

Use Ctrl / Shift to select multiple records to delete.

8. **(Optional)** Click **Show Filter** to specify the search parameters and quickly find all similar records. The filter is applied to all columns displayed in the list view. For more information, see Finding Device Records on page 147.

Note:

Use the paging control at the bottom of the list to move forward or backward by one page, or to the first or last page of the list. You can control number of records to be displayed per page and also click an individual page number to navigate to the specific page. Click **Refresh** icon to refresh the view.

Field Descriptions

Use data in the following table to use New Device screen. The fields are enabled based on the associated Onboarding Template settings.

Name	Description
Onboarding Template	Specifies the list of Onboarding Template(s) that the Provisioner is a member of. The Provisioner can add the Device using any one of the available Onboarding Template(s).
MAC Address	Configures the MAC address of the Device. Format of MAC address: xx:xx:xx:xx:xx:xx. For example: 10:00:01:02:21:10.
Device Name	Configures the name of the Device.
Source	Displays the source of the Device. By default, the information is available.
Device Type Groups	Specifies the list of Device type groups available for the selected Onboarding Template.
Device Type	Specifies the list of Device types available for the selected Device type group.
Records Enabled	Select to enable the record. If you do not select this option, the Device is disabled.
Delete on Expire	Deletes the Devices from the Access Control Engine. Select this option to automatically remove expired Device records. If you do not select this option, you need to manually remove the Device records after it expires. The expired Device records remains in the Access Control Engine. As a Provisioner you can renew or remove the expired records at any point of time.
Assest Type	Specifies the list of assets types to configure the record duration.

Table continues…

Name	Description
	The options available are: • **Permanent** • **Temporary** If the **Asset Type** is selected as **Permanent**, the Application creates a permanent record for the Device and the **End Time** column displays "—". If the **Asset Type** is selected as **Temporary**, the Application creates a temporary record for the Device and allows you to specify the record validity details in **Activate Account On** field.
Activate Account On	Configures the date and time at which the Device record is activated. The value in these fields defaults to the current date and time on the Guest and IoT Manager. You can also view the time zone that has been set to the current Onboarding Template. • **Date:** Enter the start date for activating Device records . The date should be in YYYY/MM/DD format. • **Time:** Enter the time in hours and minutes based on a 12-hour setting. The time should be in hh:mm:ss format. • **AM / PM:** Select the time of the day.
Activate on First Login	Specifies that guest account will be valid only after the first login. **Note:** This field is available only if the Administrator has selected **First Login** option in **Account Validity Period** section while creating an Onboarding Template and the Provisioner selects the same Onboarding Template during Device record creation from the **Onboarding Template** drop-down list. The **Activate Account On** option is replaced by **Activate on First Login: Yes** option.
Duration	Configures the duration validity of the Device record. The record validity period starts from the activation time and lasts for the specified duration. By default, the application sets the durations to the maximum time period specified in the **Temporary Account Validity** field during creation of Onboarding Template. Specify the period as an integer and set the units by selecting minutes, hours, and days.
Single Membership Access Group	Specifies one of the access groups that has been configured in Onboarding Template
Multiple Memberships Access Group	Configures the access to the Devices. You can select multiple options. For example, if the access has to be provided for a specific department, the Administrator defines which access group are available for you.
Custom fields: 1 to 6	Specifies the label values configured for Device records.

Modifying Device Record

Use this procedure to modify Device records.

Procedure

1. In the navigation pane, click **Devices** > **Devices** tab.

   The Devices screen is displayed with list of Device records created by the Provisioner.

2. Select the required Device record to be modified and click **Edit**.

   You can also edit by double-clicking the required Device record from the list.

   The **Onboarding Template** field is editable only during creating an Device.

3. In the Device Info section, modify the fields required.

4. Click **Save** to save the configuration or click **Cancel** to cancel the changes.

   The modified Device record details are displayed in the Devices screen.

5. **(Optional)** To modify the validity of a Device record, do the following:

   a. Select the required Device record and scroll left to view the **Start Time** and **End Time** Device attributes column. The RED text indicates expired record.

   b. Double-click the Device record to view the Edit Device screen.

   c. Modify the duration period in **Duration** field or modify the **Activate Account On** field to change the validity period to desired time frame.

   For more information, see Adding a Device Record Field Descriptions on page 145 .

Finding Device Records

Use this procedure to find a Device record summary.

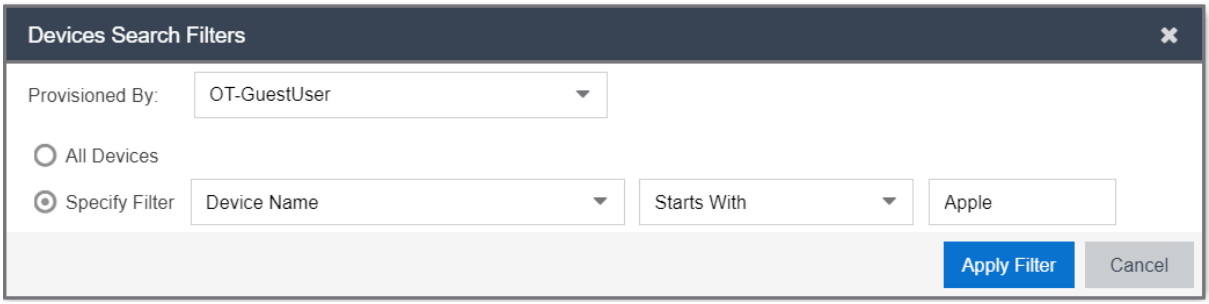
Procedure

1. In the navigation pane, click **Devices** > **Devices** tab.

   The Devices screen is displayed with the list of Devices created by Provisioner.

2. In the Devices screen, click  **Show Filter** to specify the search parameters and quickly find all similar Device records.

   The Filter Devices screen is displayed.



3. In the Filter Devices screen, do the following:
   a. Select the required Onboarding Template or the Provisioner who has created the guest account from the **Provisioned By (Provisioner)** drop-down list.
   b. Select **All Devices**, and click **Apply Filter** to view all the Devices.
   c. Select **Specify Filter**; include the specific Device attributes from the drop-down list to specify the quick search and click **Apply Filter**.

      The corresponding Device records are displayed in the Devices screen table.
   d. Click **Cancel** to cancel the changes.

   Use the paging control at the bottom of the list to move forward or backward by one page, or to the first or last page of the list. You can control number of records to be displayed per page and also click an individual page number to navigate to the specific page. Click **Refresh** icon to refresh the view.

Field Descriptions

Use data in the following table to use Filter Devices screen.

Name	Description
Provisioned By (Provisioner)	Specifies the list of Onboarding Templates that owns the Device record available for the Provisioner along with logged in Provisioner name.
All Devices	Displays the list of all the devices available for the selected Provisioned By (Provisioner). By default, this option is selected.
Specify Filter	Simplifies the search parameters to quickly find the selected search criterion that includes specified parameters. Additionally you need to enter the operator conditions to match the selected search criteria to obtain precise search results of the selected Onboarding Template. The search conditions are: • **MAC Address** • **Name** • **Type** • **Source** • **Start Time**

Table continues…

Name	Description
	• **End Time** • **Devices Activated in the Last**: Fetches all the Device records activated in the last X number of hours. • **First Login Pending and Created Before**: Fetches all the Device records that have been created before the X date entered and awaiting first login. • **Devices Expiring in the Next**: Calculates and fetches the Devices according to: CURRENT_TIME < END_TIME < CURRENT_TIME + X days 'X' is a variable here. So, if you want to filter all Devices expiring tomorrow, you can select this filter condition. • **Expired Devices**: Fetches all the expired Device records. The search conditions operators depends on the selected search conditions. For example, you can provide explicit operations such as Start With, Equal, Not Equal, Contains, Ends With and the name of the search value. Some conditions have multiple condition operators. For example, you can search for multiple values when using the equal (=) or not equal !=) operators.

Extending Expiry of a Device

Use this procedure to extends the duration of expired Device(s) by "X" days at one go.

Procedure

1. In the navigation pane, click **Devices** > **Devices** tab.

   The Devices screen is displayed with the list of Devices provisioned.

2. Select the required Device record(s) and click **Extend Expiration** to extend the validity duration of the Device record(s). The validity is extended based on the duration specified during the creation.

   The duration of expiry of each selected Devices is calculated as:

   DURATION = END_TIME – START_TIME

   Then the account is modified to :

   START_TIME = CURRENT_TIME

   END_TIME = START_TIME + DURATION

   Extend Expiration Example:

Consider two Devices, Device 1 valid for a duration of one month and Device 2 is valid for a duration of two months, both are expiring tomorrow and the current time is 02:00 P.M. When you select these two Devices and click **Extend Expiration** option, their expiry is extended as follows:

a. Device 1 is extended as Start Time = 02:00 P.M. today and End Time = 02:00 P.M. today + 1 month.

b. Device 2 is extended as Start Time = 02:00 P.M. today and End Time = 02:00 P.M. today + 2 months.

Note:

The Provisioners can use **Extend Expiration** option to extend the duration of expiry for expired Device(s) also.

Expiry of First Login Pending and Permanent Device accounts cannot be extended.

Managing Sponsor Actions

The **Sponsor** tab in Sponsor menu allows a Sponsor to manage guest accounts that require Sponsor's attention. A Sponsor can either be an internal Provisioner or a Provisioner belonging to a Sponsor LDAP.

Sponsor feature allows you:

- View all the sponsored Guest Users
- Manage Sponsor actions

Viewing and Providing Guest Access

Use this procedure to view all sponsored Guest Users and allow actions such as approve, bulk approve, bulk deny / lock,bulk extend expiration, send email, and print the Guest Users.

Procedure

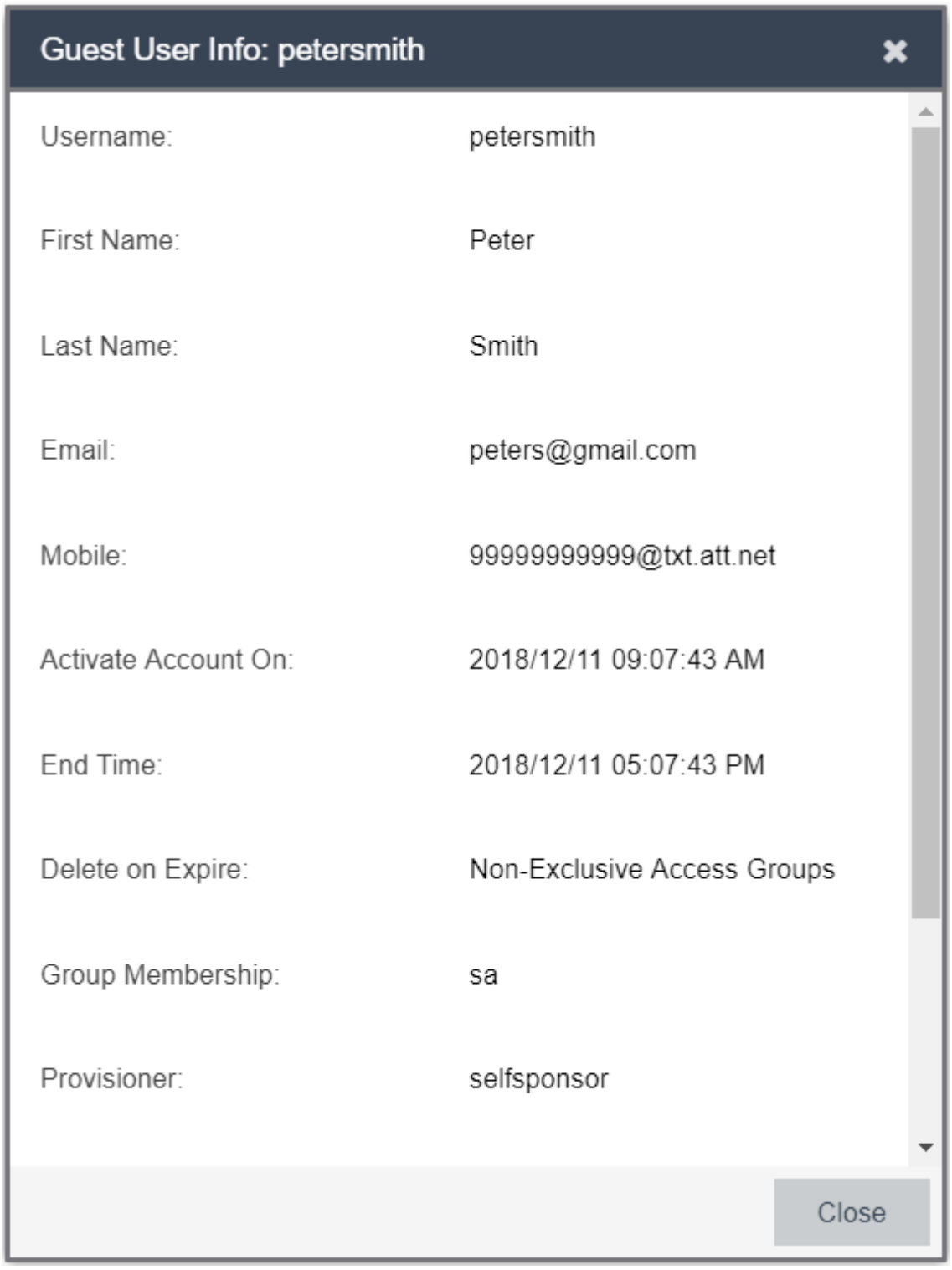
1. In the navigation pane, click **Sponsor** > **Sponsor** tab.

   The Sponsor screen is displayed with all the list of guests for which the Provisioner is a Sponsor.

   You can also click the column headers to sort the list view by that column. Click the column header a second time to reverse the direction of the sort.

2. Select the required user and click **View** to view the selected user information.

   The Guest User Info screen is displayed.


Guest User Info: petersmith
Username:
petersmith
First Name:
Peter
Last Name:
Smith
Email:
peters@gmail.com
Mobile:
99999999999@txt.att.net
Activate Account On:
2018/12/11 09:07:43 AM
End Time:
2018/12/11 05:07:43 PM
Delete on Expire:
Non-Exclusive Access Groups
Group Membership:
sa
Provisioner:
selfsponsor
Close

Note:

The view functionality is available only if the following conditions are met:

- If a valid Email ID is present for the Sponsor.
- LDAP Sponsor Username must be mentioned along with the complete domain. Though Guest and IoT Manager-LDAP authentication is not case sensitive, the Sponsor view functionality is case sensitive. For example, if the Provisioner Username in LDAP is <<name>> and the domain is `test.local`, then the Sponsor managing Guest Users view works only if the Provisioner logs in as `<<name>>@test.local`.

3. Select the required user accounts and click **Approve** to approve the access.

   The Approve screen is displayed. You can include a message that needs to be sent as part of the approval email.

4. Select the required user accounts and click **Deny/Lock** to deny the access.

   The Deny / Lock screen is displayed. You can include a message that needs to be sent as part of the denial email.

5. Select the required user accounts and click **Extend Expiration** to extend the duration of Guest User account.

   The Extend Expiration screen is displayed and enables you to extend the validity of Guest User(s) account. The validity is extended based on the duration specified during the creation.

   The duration of each selected Guest User is calculated as:

   DURATION = END_TIME – START_TIME

   Then the account is modified to :

   START_TIME = CURRENT_TIME

   END_TIME = START_TIME + DURATION

   Extend Expiration Example:

   Consider two Guest Users, User 1 valid for a duration of one month and User 2 is valid for a duration of two months, both are expiring tomorrow and the current time is 02:00 P.M. When you select these two accounts and click **Extend Expiration** option, their expiry is extended as follows:

   a. User 1 is extended as Start Time = 02:00 P.M. today and End Time = 02:00 P.M. today + 1 month.

   b. User 2 is extended as Start Time = 02:00 P.M. today and End Time = 02:00 P.M. today + 2 months.

   Note:

   Expiry of First Login Pending and Permanent Guest User accounts cannot be extended.

6. Select the required user and click **Send Email**.

The Email screen is displayed. You can include a message that needs to be sent as part the email.

7. Select the required user and click **Print** the information, if required.
8. **(Optional)** Click  **Show Filter** to specify the search parameters and quickly find all similar records.

   The filter is applied to all columns displayed in the list view. Additionally you can also enter the operator conditions to match the selected search criteria to obtain precise search results.

   For more information about how to search specific guest users, see *ExtremeControl Guest and IoT Manager Configuration*.

Chapter 12: Using Self-Provisioning Services

This chapter is intended for Guest Users to understand the Self-Provisioning Services functionality that offers guest the ability to create an account or register their devices.

The available service types are:

- Guest User on page 154 : A Self-Provisioning Service that allows users to self-register to create their own accounts.
- Devices on page 158: A Self-Provisioning Service that allows users to register a Device.

Registering a New Guest User

Use this procedure to create a new Guest User using the Self-Provisioning Services.

Before you begin

Ensure that you have the URL that is available in the Self-Provisioning Services tab.

The URL's are different for each service type. For Guest User: `https://<server_name>/GIM/user/<service_name>`

Procedure

1. In the Register New Guest User screen, enter the Guest User details in the respective fields as required.
2. If the Onboarding Template type is Sponsor Approval, users has to enter the Sponsor details. The Sponsor details need to be entered depends on the associated Onboarding Template setting. The possible scenarios are:
   - Sponsor Details on page 156
   - Fixed Sponsor on page 157
   - Predefined Sponsor on page 157
   - LDAP Sponsor on page 158

3. Click **Submit** / **Request Approval** to create the guest account.
   - If the Sponsor approval is not required, the Guest User account is created and the credentials are shared with the user via email / SMS or displayed. If the associated Onboarding Template has settings that requires Sponsor approval, then the **Request Approval** option is displayed. The Sponsor must approve for the account to be activated.
4. **(Optional)** Click **Clear**, to clear the configuration.
5. **(Optional)** Click **Resend Password** only when Guest User needs to recover the forgotten account password. This option is available as per the associated Onboarding Template configuration.

   The password is shared via email / SMS or both depending on the notification options of the Onboarding Template to which the user is associated.

   The following checks are performed prior the password is shared:

   - Notification options has either SMS / Email or both enabled
   - Account is not locked / expired

   Important:

   We strongly recommend that Administrator must disable unnecessary features in the web browser that displays in the Self-Service Provisioning service. Disable all menus, tool bars, and the URL.

   Guest and IoT Manager must be connected to the Access Control Engine all the times for the Self-Service Provisioning service to operate.

Field Descriptions

Use data in the following table to use Register New Guest User screen. The fields are displayed based on the associated Onboarding Template settings.

Name	Description
First Name and **Last Name**	Specifies the first name, and last name of the Guest User account details. The length of the name can be 30 characters or less. **Note:** These fields should only contain letters, number, hyphen, and underscore.
Username	Specifies the Username or auto populates based on the user input and associated Onboarding Template settings.

Table continues…

Name	Description
	Note: These fields should only contain alphanumeric and special characters. Only these special characters are allowed : ! @ # $ % ^ & * ( ) + – .
Email	Specifies the email address of the Guest User to send the account access details.
Mobile Phone	Specifies the contact number of the Guest User to send the account access details.
Carrier	Specifies the list of phone carriers that are available.
Custom Fields : 1 to 6	Specifies the label values configured for Guest Users. The Custom fields are available to collect specific data from the user. This information can be shared with Sponsor via email during the approval / deny flow.
Terms of Use	Displays the terms of use provided to the Guest Users.

Sponsor Details

Use this procedure to add the sponsor details manually while registering Guest Users.

Procedure

1. In the **Register New Guest User** > **Sponsor** section, enter the Sponsor contact details in the respective fields as required.
2. Click **Request Approval** to create the Guest User.

   For more information, see *ExtremeControl Guest and IoT Manager Configuration*.
3. **(Optional)** Click **Clear**, to clear the configuration.
4. **(Optional)** Click **Resend Password** only when Guest User needs to recover the forgotten account password. This option is available as per the associated Onboarding Template configuration.

Field Descriptions

Use data in the following table to use **Sponsor** section in Register New Guest User screen.

Name	Description
First Name and Last Name	Specifies the first and last name of the Sponsor.
Email	Specifies the email ID and allows to select the domain from the drop-down list.

Table continues…

Name	Description
	You can either select the email ID from the drop-down list, or enter the corresponding name to search and select the appropriate Sponsor.
Mobile Phone	Specifies the Sponsor contact number that is required to send SMS notification.

Fixed Sponsor

Use this procedure to send the request to the fixed Sponsor.

Procedure

1. In the **Register New Guest User** > **Sponsor** section, Sponsor details are not visible in the Self-Service Provisioning service. The email notification is sent to the defined Fixed Sponsor to approve or deny the user account approval request.
2. Click **Request Approval** to obtain the Guest User request approval from the Sponsor specified in the associated Onboarding Template.
3. **(Optional)** Click **Clear**, to clear the configuration.
4. **(Optional)** Click **Resend Password** only when Guest User needs to recover the forgotten account password. This option is available as per the associated Onboarding Template configuration.

Predefined Sponsors

Use this procedure to send the request to the Predefined Sponsor.

Procedure

1. In the **Register New Guest User** > **Sponsor** section, the options are available based on the associated Onboarding Template. You can perform any one of the following actions:
   a. Select the predefined sponsor from the drop-down list.

      OR

   b. Enter the email ID of the Sponsor in the text field.

      Ensure that the provided email address match with the predefined sponsor list in the Onboarding Template.
2. Click **Request Approval** to create the Guest User.
3. **(Optional)** Click **Clear**, to clear the configuration.
4. **(Optional)** Click **Resend Password** only when Guest User needs to recover the forgotten account password. This option is available as per the associated Onboarding Template configuration.

LDAP Sponsor

Use this procedure to select the Sponsors from pre populated list in Self-Service Provisioning service.

Procedure

1. In the **Register New Guest User** > **Sponsor** section, click on the **Search** icon to select the Sponsor details.

   The **Sponsor** field lists all the available Sponsors. When you select the required Sponsor, the Sponsor details are auto populated in the **First Name**, **Last Name** and **Email** fields.
2. Click **Request Approval** to create the Guest User.
3. **(Optional)** Click **Clear**, to clear the configuration.
4. **(Optional)** Click **Resend Password** only when Guest User needs to recover the forgotten account password. This option is available as per the associated Onboarding Template configuration.

Registering New Devices

Use this procedure to create a new Device using the Self-Provisioning Services.

Before you begin

Ensure that you have the URL that is available in the Self-Provisioning Services tab.

The URL's are different for each service type. For new Devices: `https://<server_name>/GIM/device/<service_name>`

Procedure

1. In the Register New Guest User screen, enter the Device details in the respective fields as required.
2. Click **Submit** to create the Device record.
3. **(Optional)** Click **Clear**, to clear the configuration.

Field Descriptions

Use data in the following table to use Register New Device screen. The fields are displayed based on the associated Onboarding Template settings.

Name	Description
Username and Password	Provides the valid Username and Password to obtain access to the Device.
MAC Address	Provides the MAC address of the Device.
Device Type Groups	Specifies the Device Type Groups.
Device Type	Specifies the list of pre populated device types that are included in the drop-down list based on the selected Device Family.
Custom Fields : 1 to 6	Specifies the label values configured for Devices. The Custom fields are specified to collect data from the user.
Terms of Use	Displays the terms of use provided to the Devices.

Chapter 13: Guest and IoT Manager Add-In for Outlook

The Guest and IoT Manager Add-in provosions and provides guest access credentials to meeting invitees. You can download the add-in from both Administrator and Provisioner login page.

This section provides information on how to install Add-in for Outlook that works with Windows and Macintosh computers (Outlook 2016 for Windows and Mac) and also on how to provision guest access using the installed Add-in.

Installing Guest and IoT Manager Add-In

Use this procedure to install Guest and IoT Manager Add-In for Outlook 2016 for Windows and Mac that helps in automating tasks when you view or create meetings.

Before you begin

Internet Explorer must be installed and needs to be enabled in the **Turn Windows features on or off** screen for an Outlook Add-in to work.

Procedure

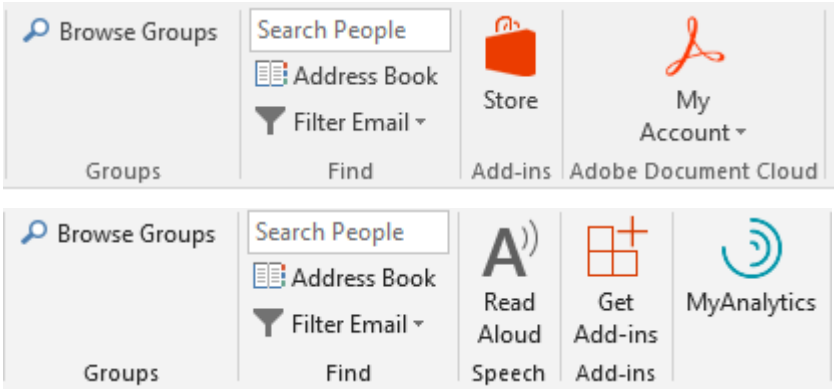
1. In the Guest and IoT Manager Administrator / Provisioner login page, click **Download GIM Outlook Add-in** to download the installer and store it in the local drive.
2. In the local folder, extract the files. You can see the following files in the folder:
   - GIM Certificate File: Guest and IoT Manager certificate is the HTTPD certificate bound to the HTTPD service.
   - GIM Manifest File
   - Readme File

   Note:

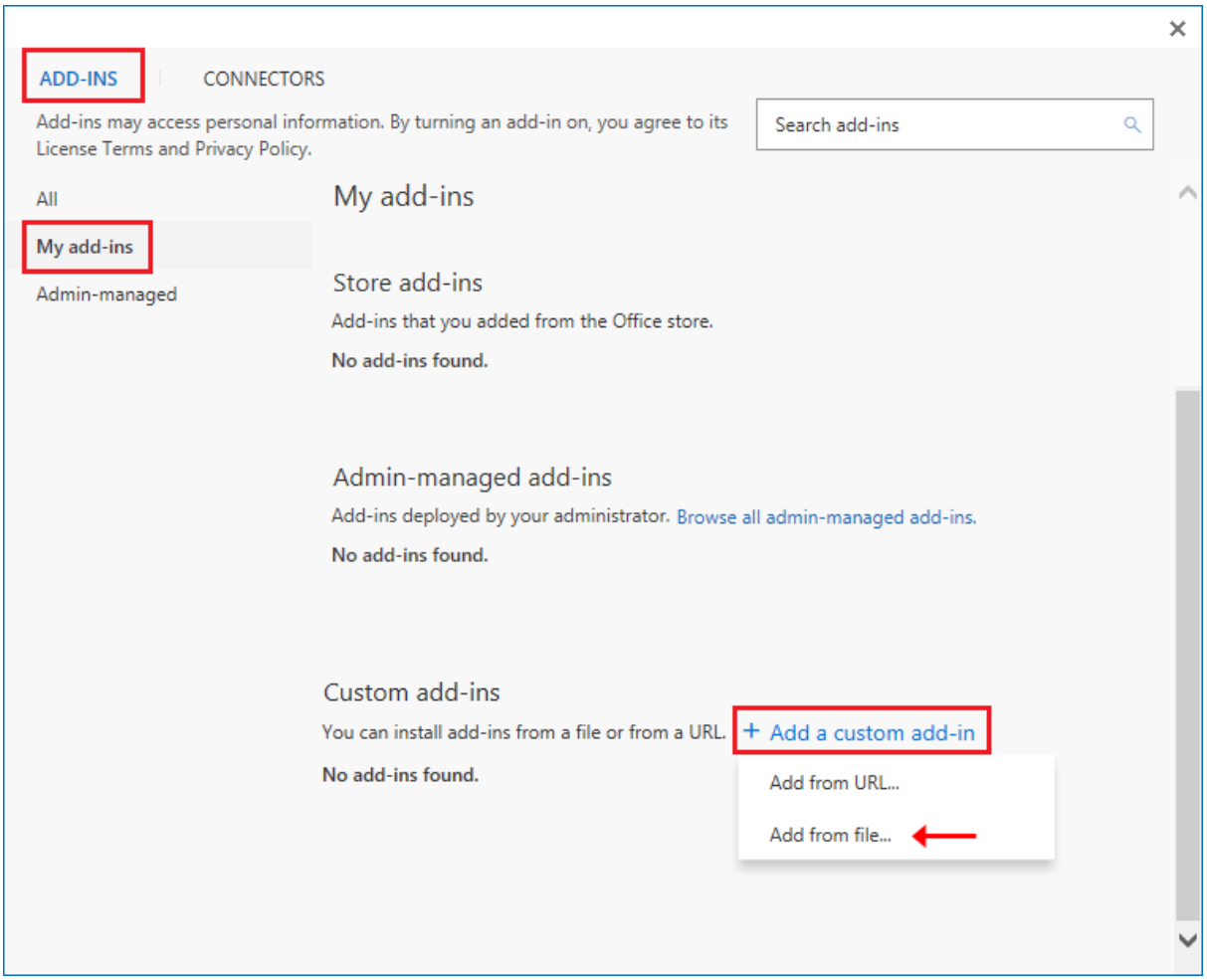
   The GIM certificate file contains a certificate to certify the identity and Readme file contains the instructions to install.

   Install the GIM certificate only if it is Self-Signed SSL certificate. For more information on certificate installation, refer `Readme` file.

3. Start the Outlook application and click **Store** or **Get Add-ins** in the **Home** menu.



The ADD-INS screen is displayed. In the ADD-INS screen, you can install the add-in either from the local drive or Administration can side-load this add-in to all the Provisioner(s).

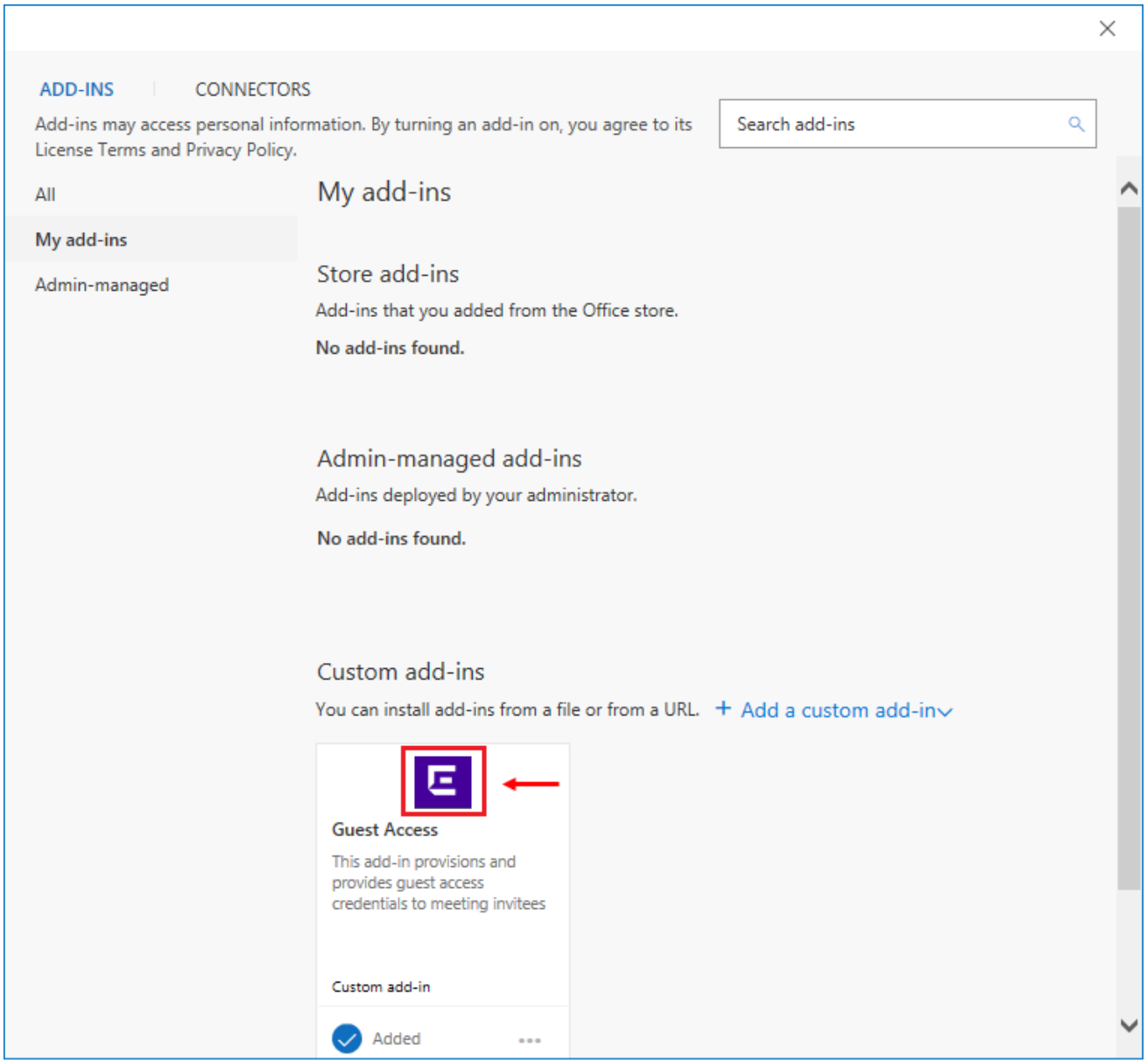


4. To install the add-in from the local drive, do the following:
   a. In the ADD-INS screen, click **My add-ins** > **+ Add a custom add-in** > **Add from file….** to import the add-in manifest file.
   b. Select **Browse** and navigate to the location of the add-in manifest file that you want to install.
   c. Select the "`gim-manifest.xml`" add-in file and click **Open**.
   d. Click **Install**.

      The added add-in is displayed in the **Custom add-ins** section of ADD-INS screen.
5. To side-load the add-in to the Provisioner(s) as an Administrator, use Exchange Administration Center (EAC).

   Side-loading add-ins requires at minimum the **My Custom Apps** role for your Exchange Server. For more information, see Install an Add-In for Outlook.

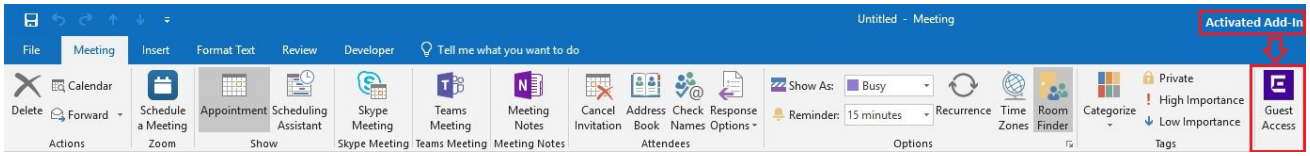
GIM Add-In



Note:

The added add-in is activated only when the Provisioner(s) wants to raise a meeting request. For more information, see Provisioning Guest Access on page 164.

An example of added add-in:



Provisioning Guest Access

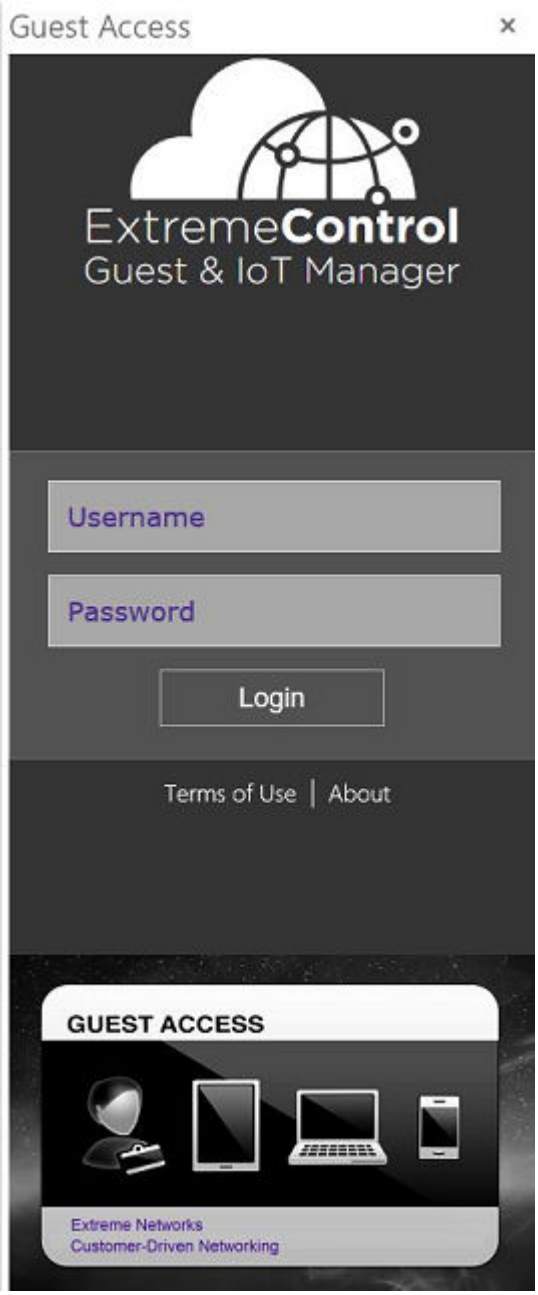
Use this procedure to provision Guest Users while scheduling the meeting.

Procedure

1. Start the **Outlook** application.
2. In the **Meeting** mode, select **Guest Access** add-in. If you do not see the Guest Access add-in, then you need to install. For more information, see Installing Guest and IoT Manager Add-In on page 160.

3. Click **Guest Access**.

   The task pane displays the Guest and IoT Manager Provisioner login page.

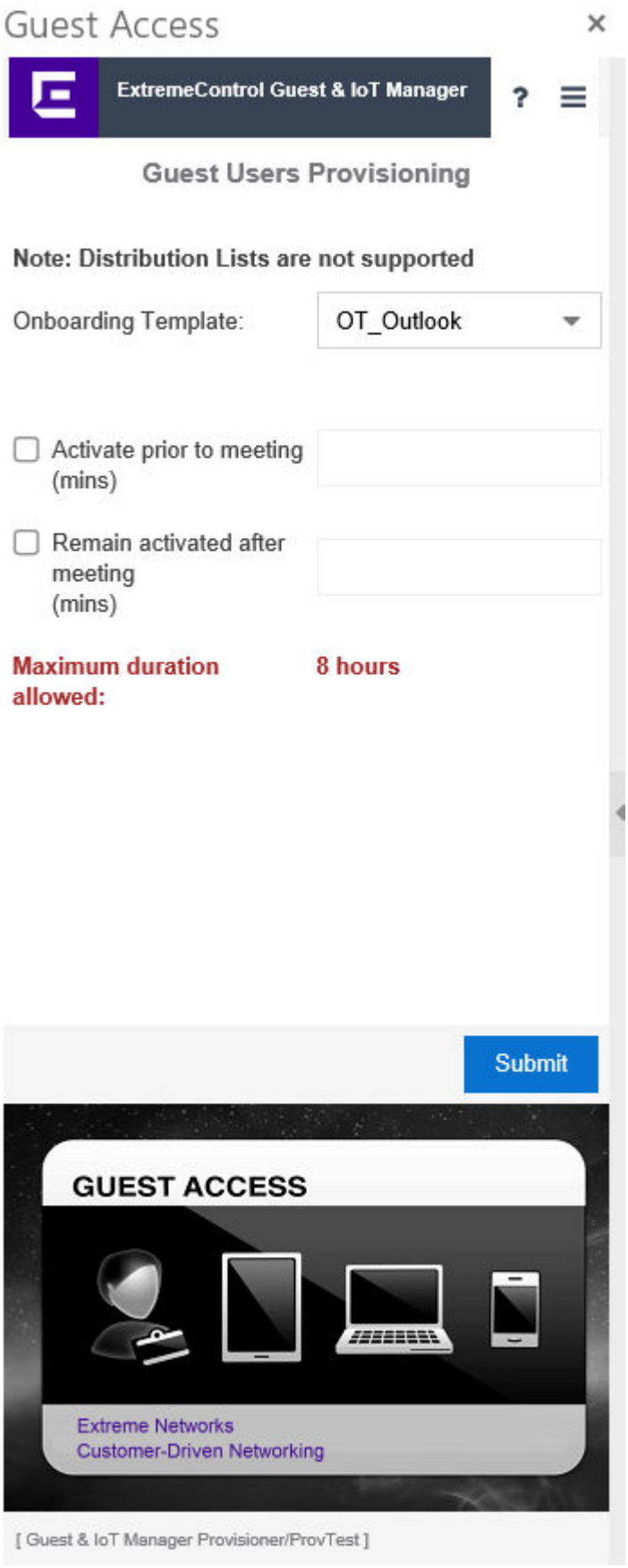


4. Login to the application using Provisioner credentials.

   The Guest User Provisioning screen is displayed on successful authentication and if the Provisioner being part of atleast one Onboarding Template of type Outlook.

   Note:

   Ensure that the Guest and IoT Manager Application is connected with Access Control Engine to authenticate.


Guest Access
ExtremeControl Guest & IoT Manager
Guest Users Provisioning
Note: Distribution Lists are not supported
Onboarding Template:
OT_Outlook
Activate prior to meeting (mins)
Remain activated after meeting (mins)
Maximum duration allowed:
8 hours
Submit
GUEST ACCESS
Extreme Networks
Customer-Driven Networking
[Guest & IoT Manager Provisioner/ProvTest]

5. Select the required **Onboarding Template** to which the users in the meeting needs to be associated from the drop-down list.
6. Select the required **Access Groups**.

   The Single and Multiple Memberships Access Groups are available based on the Onboarding Template configuration.
7. **(Optional)** Select the **Activate prior to meeting (mins)** or **Remain activated after meeting (mins)** and enter the minutes to add a buffer time between the scheduled guest access. The maximum buffer time is 30 minutes.

   The Guest Users obtain the access duration equal to scheduled duration along with buffer / padding duration. Whereas, the outlook calender shows only the scheduled meeting duration.
8. Set up the meeting as you typically do:
   a. In the **To** field, enter the email address of the Guest User(s), separated by semicolons.
   b. Select **Room...** to find a conference room if you need your Guest Users to be accommodated in one location.
   c. Select a **Start Time** and **End Time**; enter an agenda in the meeting area.
9. Click **Submit** in the Guest User Provisioning screen prior sending the meeting invite. Alternatively, you can also provision the Guest Users by reopening this meeting invite from the calender. The email sent summary is displayed.
   - If the Guest User is present in the database, then the invite is updated with the scheduled start and end time.
   - If a new Email ID is added, then the Guest User is created and confirmation email is sent to the corresponding Guest User.
   - If any Email ID is removed, then the corresponding Guest Users will also be removed from the Guest and IoT Manager Application.

   Note:
   - If the Administrator has excluded a domain during Guest User Onboarding Template creation, then the Guest User account is not created for any emails available in that particular domain.
   - Ensure that you always expand the distribution list.
   - You need to click **Submit** in the add-in once again, if there are any changes in the recipient list or meeting duration.
   - If the scheduled meeting duration along with added padding is greater than the maximum expiration time configured in the Onboarding Template, then the access duration will be reduced to maximum duration configured in the Onboarding Template.
   - Recurring meetings are not supported. Access will be provided only for the first occurrence.

Tip:

If you want to extend the access for the second occurrence, resubmit in the Guest and IoT Manager add-in when the first meeting is ended and so on.

10. **(Optional)** Click **Delete** in the Guest User Provisioning screen to remove all the Guest Users in the meeting. For example, if you need to cancel the guest access / meetings.

Note:

The application displays a warning message prior removing all the Guest Users.

The **Delete** option is available only if you have created the Guest Users for the current meeting schedule.

Chapter 14: Troubleshooting and FAQs

This chapter describes the basic concepts and general troubleshooting guidelines for problems that may occur when configuring and using the Guest and IoT Manager Application. The solutions to common questions helps you troubleshoot quires when you encounter errors.

Testing RADIUS Connection Settings

Use this procedure to test the RADIUS setup.

Procedure

1. Create a Provisioner. For more information, see Creating an Internal Provisioner on page 109.
2. Open your web browser and enter the URL of the Provisioner Application.

   `https://<Guest Manager machine>/GuestManager/provisioner/`
3. In the Login screen, enter the Provisioner login credentials.
4. Click **Login**. If your login attempt fails, see Problem: Provisioner Cannot Login on page 171.

Restarting Guest and IoT Manager

Use this procedure to restart Guest and IoT Manager Application.

Procedure

1. Log in to the Guest and IoT Manager Virtual Appliance console.
2. Enter the **Username** and **Password**.
3. Enter `tomcat restart`, to restart the web server.
4. Launch the Guest and IoT Manager Virtual Appliance console.

Problem: Virtual Appliance Troubleshooting

Condition

Problem in Guest and IoT Manager Virtual Appliance.

Guest and IoT Manager URL is not Accessible

1. Log in to the Guest and IoT Manager Virtual Appliance as Administrator.
2. From the CLI, enter command `tomcat 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 tomcat, do the following

1. Log in to Guest and IoT Manager Virtual Appliance as Administrator.
2. From the CLI, enter `tomcat restart`.

Guest and IoT Manager CLI

If you are not able to ping the Guest and IoT Manager Virtual Appliance after assigning the IP address and configure the route, enter `reboot` from the CLI.

Problem: Saving Access Control Engine Settings

Problem

Unable to save Access Control Engine details in Guest and IoT Manager.

Solution

1. Ensure that the DNS is configured correctly if hostname is used to connect
2. Ensure Extreme Management Center / Access Control Engine version is compatible with the Guest and IoT Manager version
3. Ensure that the Extreme Management Center administrative user has Guest and IoT Manager read and write permissions.
4. Ensure that the Access Control Engine is added in the required Engine Group in Extreme Management Center.

Problem: User Groups / End System Group Not Visible in Guest and IoT Manager

Problem

Any newly created User Groups / End System Groups created in Extreme Management Center is not visible in the Access Group tab of the Onboarding Template module.

Solution

1. User Groups of type Username and End System Groups of type MAC are only visible in the Guest and IoT Manager.
2. Ensure that the Groups created in Extreme Management Center are of the appropriate type.

Problem: Provisioner Cannot Login

Problem

No login button found.

Solution

1. If Access Control Engine or Extreme Management Center is not reachable, ensure that Access Control Engine and Extreme Management Center are up and reachable.
2. If invalid Extreme Management Center credentials are entered, ensure that Guest and IoT Manager is configured with valid Extreme Management Center administrator credentials which has Guest and IoT Manager read and write access.
3. Ensure that the Access Control Engine is added in the required Engine Group in Extreme Management Center.
4. If no valid Guest and IoT Manager license installed, ensure that the valid Guest and IoT Manager license is installed in the Extreme Management Center.

Problem

Provisioner login fails with an error stating “Server error please contact administrator”

Solution

1. If Access Control Engine or Extreme Management Center is not reachable, ensure that Access Control Engine and Extreme Management Center are up and reachable.
2. If Guest and IoT Manager is not configured in the Engine Group, ensure to add Guest and IoT Manager IP address and RADIUS shared secret in Engine details on Extreme Management Center.
3. If Guest and IoT Manager management IP address is changed but not updated the Guest and IoT Manager Server settings in the Engine Group, update the Guest and IoT Manager IP address in Engine details on Extreme Management Center.

4. If RADIUS shared secret mismatch, ensure that you have entered the same RADIUS shared secret on Guest and IoT Manager and in the Engine details on Extreme Management Center.
5. If Guest and IoT Manager is not licensed, install valid Guest and IoT Manager license on Extreme Management Center.
6. If the Provisioner is an LDAP Provisioner and is not associated with any Onboarding Template, ensure that an Onboarding Template is associated with that LDAP group or there is a default Onboarding Template present. For more information, see Configuring Onboarding Template on page 64.

Problem

Invalid credentials

Solution

1. If wrong credentials are entered, ensure a valid username and password is entered.
2. If Guest and IoT Manager domain LPR and Access Control Engine AAA LPR settings are not same, ensure that both are same.
3. If Internal Provisioner and AAA rule does not have local authentication selected in the AAA rule, ensure that the local authentication is selected with LPR same as GIM domain LPR
4. If LDAP Provisoner and AAA rule does not have LDAP authentication selected as the authentication type in the AAA configuration, ensure the LDAP authentication is selected and required LDAP details are provided.

Problem

If fall through is enabled in the AAA configuration and both “Local Authentication” and “LDAP Authentication” is enabled, then the fall through does not work as expected and the second rule is not evaluated.

Solution

Do not enable fall through option for Provisoner login.

Problem: Guest and IoT Manager Email / SMS Notification Failed

Problem

Unable to send Email / SMS notifications for Guest Users.

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

   Log in to the Guest and IoT Manager Administrator User Interface. In the navigation pane, click **Administration** > **Notification** > **Email** > **Enable Sending of Email Notification**. Check the details and click **Save**.

2. Log in to the Guest and IoT Manager Virtual Appliance console as Administrator.
   a. Enter command `show dns` to check if the dns is configured. If dns is not configured, configure dns. For more information, see dns on page 177.
   b. Enter `reboot`.
3. Send a test email using "Test" option. For more information, see Setting Notification Parameters on page 54.
4. Ensure that the **Guest User Email** and / or **Password to Guest User Mobile Phone** options are selected in the **Send Notification** section of the New Guest User screen.

Problem: Unable to Access Guest and IoT Manager Application URL

Problem

When the admin interface IP address is updated manually through CLI command, Guest and IoT Manager URL is not reachable.

Solution

Verify the route settings and make appropriate change if needed. For more information, see route on page 180.

Problem: User and Device Troubleshooting

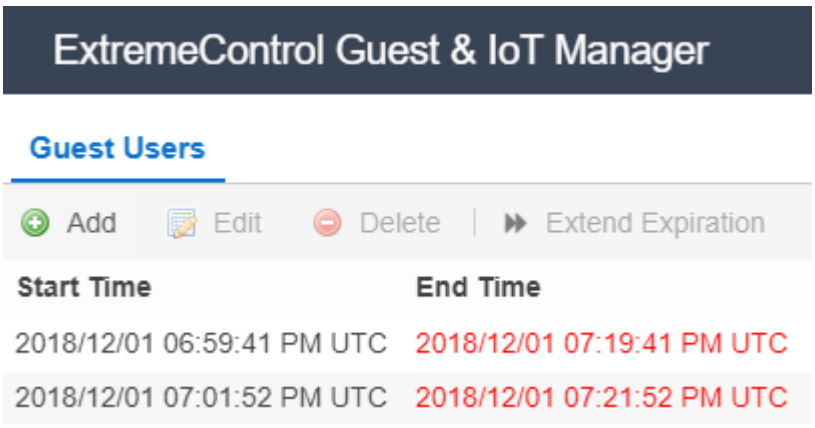
Problem

Newly created Guest Users / Devices from Guest and IoT Manager are not authenticated.

Solution

1. Ensure that the records are enabled.

   For more information, see *ExtremeControl Guest and IoT Manager Configuration*.
2. Ensure that the Guest User / Device is not expired. You can identify the expired record in the End Time attributes column that is highlighted in RED.



3. Ensure that the start time is not in the future.

Problem

Expired Guest User / Device record is not available Guest and IoT Manager.

Solution

Ensure that the **Delete on Expiry** option is unchecked while creating the new Guest User / Device.

Problem: Sponsor List is Not Available

Problem

“Sponsor list is not available” error is seen when logging to the self-service URL.

Solution

Ensure that the LDAP group which has the sponsors is correctly entered in the Onboarding Template setting. For more information, see Configure Sponsor LDAP Group on page 75.

Problem: Modification in Network Interface settings does not reflect post deployment

Problem

If Network Interface information is modified during the deployment, the changes will not get updated post deployment.

Solution

1. Delete the installed **OVA**.
2. Re-install the **OVA** with default Network Interface settings.

Retain the default Network interface settings on deployment of **OVA**. Any changes in the Network interface settings can be done post bring up.

Outlook Add-in Issues

Problem

Any changes to the meeting invite, either invitees or meeting time, is not reflecting in the Guest User records.

Solution

Ensure to click on submit after making the changes and before clicking “Send Update” in the meeting invite.

Problem

Outlook Add-in icon disappears from Outlook.

Solution

Restarting the Outlook application resolves this issue.

Service Unavailable in Browser

Problem

Post GIM reboot (manually from CLI) or post a config restore workflow, “Service Unavailable” message is observed in the browser while accessing GIM Application.

Solution

Restart tomcat service from the CLI. Enter command `tomcat restart`.

Chapter 15: Command Line Interface

This chapter describes the Command Line Interface (CLI) used in Guest and IoT Manager Application to operate the system and to perform specific tasks required by Administrator.

The Guest and IoT Manager CLI provides a limited set of administrative actions that you can perform on the Application. The CLI has a default timeout of 5 minutes.

The following section briefs the CLI commands available on Guest and IoT Manager.

certificate

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 [reset, reset-all]
```

Example

```
GIM>certificate
certificate [reset, reset-all]
            reset #reset will retain all custom certs / keys / chain and reset only to default
            reset-all # reset all will remove all custom certs / keys / chain and reset to default
GIM>_
```

clear

The **clear** command clears the terminal screen.

Syntax

```
clear
```

Example

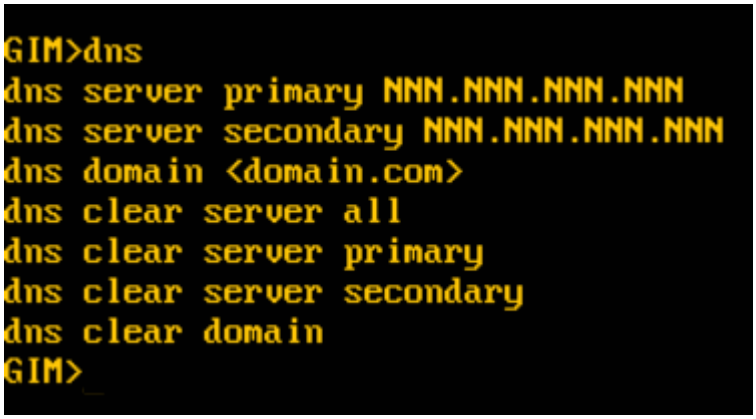
dns

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



exit

The **exit** command closes the current active session and logout the console.

Syntax

```
exit
```

halt

The **halt** command ends running system and power off the Guest and IoT Manager virtual machine.

Syntax

```
halt
```

help

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

Syntax

```
help
```

Example

```
GIM>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.
interface           : Configure interface settings.
ping                : Ping remote system.
reboot              : Reboot GuestManager Virtual Machine.
reinit              : Reinitialize GuestManager VM to
                    : factory defaults.
route               : Configure route settings.
show certificates   : Show Certificates.
show dns            : Show current dns settings.
show interface      : Show current interface settings.
show route          : Show current route settings.
sshd                : Enable/disable configure sshd service.
tomcat              : tomcat <start|stop|restart|status>
user                : user <user name> [enable|disable]
GIM>_
```

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

```
GIM>interface admin ipaddr 10.133.133.143/24
Generating new self-signed certificates for IP 10.133.133.143
tomcat restart completed successfully
Restarted the web services to listen on the new IP Address.
Please verify the route setting using the "route command"
GIM>
```

ping

The **ping** command pings a remote system to test the connection between ExtremeControl 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 is displayed 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

```
GIM>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=0.620126724243 ms
200 bytes from 10.133.133.10 icmp_seq=1 ttl=5 time=0.509977340698 ms
200 bytes from 10.133.133.10 icmp_seq=2 ttl=5 time=0.501871109009 ms
200 bytes from 10.133.133.10 icmp_seq=3 ttl=5 time=0.499963760376 ms
GIM>
```

reboot

The **reboot** command restarts the Guest and IoT Manager virtual machine instance.

Syntax

```
reboot
```

reinit

The **reinit** command restores the Guest and IoT Manager virtual machine instance to the factory default and reset all configurations.

Syntax

```
reinit
```

route

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

Syntax

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

Example

```
GIM>route
route add|delete <subnet>/<[prefix|netmask]> <gateway> [interface]
Adding a route:
route add 0.0.0.0/0 192.168.1.1 [<port>]
route add 192.168.10.0/24 192.168.1.1 [<port>]
route add 192.168.10.0 255.255.255.0 192.168.1.1 [<port>]
Deleting a route:
route delete 192.168.10.0/24 192.168.1.1
route delete 192.168.10.0 255.255.255.0 192.168.1.1
GIM>_
```

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

```
GIM>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
GIM>_
```

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

```
GIM>show dns
Domain               :  None
Primary DNS Server   :  134.141.162.20
Seconday DNS Server:  None
GIM>
```

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

```
GIM>show interface admin
NIC Name: Admin
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:95:c9:dd brd ff:ff:ff:ff:ff:ff
    inet 10.133.133.143/24 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe95:c9dd/64 scope link
       valid_lft forever preferred_lft forever

GIM>
```

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

```
GIM>show route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.133.133.1    0.0.0.0         UG    0      0        0 ens33
10.42.0.0       10.42.0.0       255.255.255.0   UG    0      0        0 flannel.1
10.42.1.0       10.42.1.0       255.255.255.0   UG    0      0        0 flannel.1
10.42.5.0       10.42.5.0       255.255.255.0   UG    0      0        0 flannel.1
10.133.133.0    *               255.255.255.0   U     0      0        0 ens33
172.17.0.0      *               255.255.0.0     U     0      0        0 docker0

GIM>
```

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 are supported in a future release.

Example

```
GIM>sshd
sshd <enable|disable> [<interface> <port>]
Note: <port> must be between 1 and 65535 inclusive.
sshd enable admin 22
sshd disable [<interface>]
     where interface is one of the following:
     Admin, ServiceA, ServiceB
     ens33, ens34, ens35
GIM>
```

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

```
GIM>tomcat
tomcat <start|stop|restart|status>
starts, stops, restart the tomcat service.

GIM>tomcat stop
tomcat stop completed successfully
GIM>tomcat start
tomcat start completed successfully
GIM>tomcat restart
tomcat restart completed successfully
GIM>_
```

user

The **user** command is used to enable / disable the root and debug users.

Syntax

```
user root enable
```

Example