



DashBoard Server and User Rights Management User Guide

Version 8.8

Thank You for Choosing Ross

You've made a great choice. We expect you will be very happy with your purchase of Ross Technology. Our mission is to:

1. Provide a Superior Customer Experience
 - offer the best product quality and support
2. Make Cool Practical Technology
 - develop great products that customers love

Ross has become well known for the Ross Video Code of Ethics. It guides our interactions and empowers our employees. I hope you enjoy reading it below.

If anything at all with your Ross experience does not live up to your expectations be sure to reach out to us at solutions@rossvideo.com.



David Ross
CEO, Ross Video
dross@rossvideo.com

Ross Video Code of Ethics

Any company is the sum total of the people that make things happen. At Ross, our employees are a special group. Our employees truly care about doing a great job and delivering a high quality customer experience every day. This code of ethics hangs on the wall of all Ross Video locations to guide our behavior:

1. We will always act in our customers' best interest.
2. We will do our best to understand our customers' requirements.
3. We will not ship crap.
4. We will be great to work with.
5. We will do something extra for our customers, as an apology, when something big goes wrong and it's our fault.
6. We will keep our promises.
7. We will treat the competition with respect.
8. We will cooperate with and help other friendly companies.
9. We will go above and beyond in times of crisis. *If there's no one to authorize the required action in times of company or customer crisis - do what you know in your heart is right. (You may rent helicopters if necessary.)*

DashBoard Server and URM DashBoard Server and User Rights Management User Guide

- Ross Part Number: **8351DR-004A-01-8.8**
- Publication Date: December 18, 2019. Printed in Canada.
- Software Issue: **8.8**

The information contained in this Guide is subject to change without notice or obligation.

Copyright

© 2019 Ross Video Limited. Ross® and any related marks are trademarks or registered trademarks of Ross Video Limited. All other trademarks are the property of their respective companies. PATENTS ISSUED and PENDING. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording, or otherwise, without the prior written permission of Ross Video. While every precaution has been taken in the preparation of this document, Ross Video assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Patents

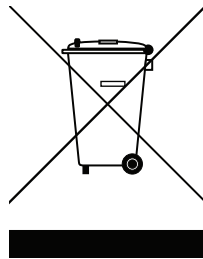
Ross Video products are protected by patent numbers US 7,034,886; US 7,508,455; US 7,602,446; US 7,802,802 B2; US 7,834,886; US 7,914,332; US 8,307,284; US 8,407,374 B2; US 8,499,019 B2; US 8,519,949 B2; US 8,743,292 B2; GB 2,419,119 B; GB 2,447,380 B. Other patents pending.

Environmental Information

The equipment that you purchased required the extraction and use of natural resources for its production. It may contain hazardous substances that could impact health and the environment.

To avoid the potential release of those substances into the environment and to diminish the need for the extraction of natural resources, Ross Video encourages you to use the appropriate take-back systems. These systems will reuse or recycle most of the materials from your end-of-life equipment in an environmentally friendly and health conscious manner.

The crossed-out wheeled bin symbol invites you to use these systems.



If you need more information on the collection, reuse, and recycling systems, please contact your local or regional waste administration.

You can also contact Ross Video for more information on the environmental performances of our products.

Company Address



Ross Video Limited

8 John Street
Iroquois, Ontario
Canada, K0E 1K0

Ross Video Incorporated

P.O. Box 880
Ogdensburg, New York
USA 13669-0880

General Business Office: (+1) 613 • 652 • 4886

Fax: (+1) 613 • 652 • 4425

Technical Support: (+1) 613 • 652 • 4886

After Hours Emergency: (+1) 613 • 349 • 0006

E-mail (Technical Support): techsupport@rossvideo.com

E-mail (General Information): solutions@rossvideo.com

Website: <http://www.rossvideo.com>

Contents

Introduction	1
Product Summary	1-1
DashBoard Server.....	1-1
DashBoard URM.....	1-1
Functional Overview.....	1-1
Licensed Number of Users	1-2
Permissions.....	1-2
Users	1-2
Roles	1-3
Devices	1-3
Applications	1-3
Before You Begin.....	1-3
Types of Applications.....	1-4
Installation Overview.....	1-5
Simplified Block Diagram.....	1-5
Documentation Terms and Conventions.....	1-7
 Interface Basics	 2
Additions to the DashBoard Client Interface.....	2-1
Configure DashBoard Server Interface.....	2-3
Configure DashBoard URM Interface	2-4
Configure User Rights Dialog Overview.....	2-6
Devices Tab Overview.....	2-7
Users Tab Overview	2-9
Tools Tab Overview	2-12
 Installation	 3
Before You Begin	3-1
System Requirements for the DashBoard Server	3-1
Installing the DashBoard Server Software.....	3-2
Creating a Backup of the Settings and Licensed Features	3-2
Installing the DashBoard Server Software	3-2
Uninstalling the DashBoard Server Software.....	3-2
Verifying the DashBoard Server.....	3-3
Licensing the DashBoard URM.....	3-3
Configuring the DashBoard URM.....	3-4
Configuring for an Embedded LDAP Server	3-4
Configuring for an External LDAP Server.....	3-5
 Configuring Roles and Accounts	 4
User Permissions Overview.....	4-1
Using an External LDAP Server.....	4-3
User Accounts and Roles.....	4-3
Permissions for Devices	4-3
Configuring the Administrators Role	4-3
Configuring the Basic Users Role	4-6
Creating a New Role.....	4-8
Configuring the Default User Account.....	4-9
Creating a New User Account	4-10
Assigning Users to Roles	4-12

Managing Permissions	4-12
Login Settings	4-13
Copying Permissions	4-13
Deleting User Roles and Accounts	4-15
Disabling User Roles and Accounts	4-16
Changing Passwords for Accounts	4-16
Managing Devices	5
Device Management Overview	5-1
Updating the List of Devices.....	5-2
Updating the Device List	5-2
Updating Device Information	5-2
Configuring Permissions for openGear Devices	5-3
Configuring Permissions for a Device	5-4
To configure permissions for a device:	5-4
To configure permissions for a specific menu of a device:	5-5
Managing Device Permissions.....	5-5
Copying Permissions	5-5
Deleting Permissions	5-6
Maintenance	6
Managing Inactive Devices.....	6-1
Deleting Inactive Devices.....	6-1
Copying Permissions for Inactive Devices.....	6-2
Adding Users and Roles to an Inactive Device	6-3
Reviewing User Permissions.....	6-3
Appendix A. Applications	7
Configuring an Open Application.....	7-1
Configuring a Closed Application	7-3
Configuring a Custom Application	7-6

Introduction

In This Chapter

This chapter provides an introduction to the DashBoard Server and User Rights Management (URM) features, and includes general information on functions and possible applications.

The following topics are discussed:

- Product Summary
- Functional Overview
- Applications
- Installation Overview
- Documentation Terms and Conventions

Product Summary

The DashBoard client has the ability to detect devices on a subnet and can enable complete control of all settings on all devices. The DashBoard Server and User Rights Management (URM) is designed to enable administrators to assign and manage user permissions, and determine the level of access for those users. For example, one user is responsible for adjusting the network settings for one type of device, while another user manages the input and outputs of another device type.



Note — *Other control mechanisms, such as SNMP, are not managed by the DashBoard URM.*

DashBoard Server

Users must now log on to the DashBoard client with a user name and password before gaining access to the devices on their network. Access to devices is now configured using the options available in the DashBoard URM. You have the option of connecting DashBoard URM to an external LDAP Server to use your existing users and roles, or this information can be managed completely internal to the DashBoard Server with its built-in LDAP Server.

DashBoard URM

The DashBoard URM licensed feature enables administrators to manage how users access devices communicating with the DashBoard client. Until the DashBoard URM licensed feature is installed, the DashBoard URM assumes a default license where configurations can be saved for up to two users/roles. Once the DashBoard URM licensed feature is installed, the number of accounts you can configure is based on the license key you installed.

Functional Overview

The DashBoard Server and URM operates as a form of hierarchical database where user permissions are organized into a tree-like format. As outlined in the section, “**Functional Overview**” on page 1-1, you can install the

DashBoard Server and URM to be an embedded LDAP Server or to use the corporate (external) LDAP Server for users and roles only.

The DashBoard Server and URM is composed of:

- **Properties** — Define specific tasks for which permissions can be set.
- **Users and roles** — Define who has access to the options in the DashBoard client, the DashBoard Server and URM.
- **Devices** — Define access to physical devices and the applicable settings that are displayed in the DashBoard client.

This section provides a functional overview of the DashBoard Server and URM to help you configure and manage your user database.

Licensed Number of Users

The DashBoard Server and URM allows for licenses that stipulate the number of users that can be configured. The **Configure DashBoard Server** and the **Configure DashBoard URM** interfaces display the maximum number of users that can be configured (as defined by your license key) and how many of those accounts are currently configured.

When the number of users is limited, settings can only be configured for that number of licensed users/roles. However, if there are more users/roles with configured settings than the license allows, no users/roles can have their settings configured until you purchase a license for more users or by reducing the current number of configurable users.

Permissions

Permissions are configured using the options in the **Configure User Rights** dialog. Permissions can be tailored to your facility needs.

Allow, Deny, Inherit

There are three permission settings: Allow, Deny, and Inherit. These options are applicable to device and setting properties, and can be configured for individual users and/or roles.

- **Allow** — This option enables the role or user to perform the specific task.
- **Deny** — This option prevents the role or user from performing the specific task.
- **Inherit** — This option assumes the permission settings from the hierarchy. Setting a property to Inherit causes DashBoard to search higher in its hierarchy for a setting of Allow or Deny for the same property. At any given level in the hierarchy, an Allow takes precedence over a Deny. You can see the value that the property inherits as a green checkbox in either the Allow or Deny column. For example, selecting Inherit for a specific card will apply the permissions as set in the frame that the card is installed in.

Users, roles, and devices that have neither had permissions set nor confirmed to be “wide open” are indicated with an asterisk in the tree view of the **Configure User Rights** dialog, enabling you to quickly see which devices and settings still need to be configured.

Users

Users must be given a unique ID name and an associated password. User IDs are forced to be an E-mail address. This information can be used to log into the DashBoard client. One user account, **Default User**, comes automatically configured with the DashBoard Server and URM. The same user account can be active on multiple DashBoard clients. For example, the Default User account can be used by multiple people to log in from separate desktops.

You can choose to create individual accounts for each person accessing devices via a DashBoard client, have a single Default User account that is used by everyone, or enable an external LDAP Server to define user accounts. This is dependent on your facility requirements.

Users can have permissions defined based on their individual account, membership in a role, or based on a specific device, a device type, or menu(s) for a device. Keep in mind that users assigned to roles assume the permissions as defined by that specific role.

Roles

A role is a group of users that share the same permissions because they belong to that specific role. By default, when using the internal LDAP Server, the DashBoard URM includes two roles: Administrator and Basic User. You can configure additional roles, based on any number of parameters, as required. For example, you may want to create a role that grants card upgrade permissions, but read-only access to all other parameters. If you are using an external LDAP Server, only the roles defined by that LDAP are used.

The difference between a role and a user is that an account is assigned to a specific user, while a role can be assigned to multiple users. Note that if any role that a user is a member of has the permissions to perform a task, that user also has the permissions to perform that task. Objects that have neither had permissions set nor confirmed to be “wide open” are displayed in the **Configure User Rights** dialog with an asterisk so that they can have permissions set.

You need at least one Administrator who can modify server and URM settings. The DashBoard Server and URM automatically includes an Administrator role and a Basic Users role.

- **Administrator** role — You can use this role to set permissions for configuring server and URM settings, network settings, and/or to perform software upgrades. Assign the users that you wish to grant such permissions to this role.
- **Basic Users** role — You can use this role to assign permissions that might apply to a wide range of users who do not need full access. For example, if you wish to limit most of your users to read-only access for server and URM settings, configure the Basic Users role to Deny all tasks except Read for the server and URM.

Devices

Devices are objects that communicate with the DashBoard client and appear in the Tree Views and are arranged in a hierarchy. The method for configuring device permissions depends on how specific you want to be. Permissions for devices can be tied to the system (global), the device itself, the type of device, or menu items for that device. Note that any given permission is always tied to a user or role.

For example, if you are configuring an openGear card, you can configure permissions based on one or more of the following:

- that specific card
- a specific menu for that card
- the openGear frame that the card is installed in
- copying permission from a similar card to your specific card

Applications

This section outlines possible applications of the DashBoard Server and URM. Your requirements may differ from what is presented.

Before You Begin

You can start your approach to configuring and managing users in DashBoard URM by asking the following questions:

1. Will user information and permissions be defined by an external LDAP Server or will this information be managed internally by the DashBoard Server and URM?
2. How will you define the purpose of an Administrator? For example, one Administrator only upgrades the software on devices and a second configures and manages the DashBoard Server and URM.

3. How many administrators will you need?
4. How many user accounts will you need to create?
5. Will each user accessing the DashBoard client need a unique account?
6. What type of access is required for each user? Will users have specific permissions, or will all users have the same permissions?
7. Will you need to group users based on tasks or devices?
8. Are there many users with different tasks or similar tasks?
9. How do the users need to access the devices in DashBoard? For example, will specific users need to change parameters frequently, view card information only, or have access to a select set of device parameters?
10. Is there a need to lock access to devices so that only an Administrator, or a specific set group of users, can modify device parameters?
11. Is there a need to add password protection to your frames?

Types of Applications

If the DashBoard URM service derives user information from an external LDAP Server, such as the one that defines your corporate user data, users and/or roles is defined by that LDAP Server (including password authentication). However, if the DashBoard URM service is to be managed as an isolated database, there are three basic applications for DashBoard URM: open, closed, or custom.



Operating Tip — *The Server Configuration menu enables you to select the system default settings to Allow or Deny for properties that have no permissions set all the way up the hierarchy.*

For more information on configuring examples of a specific type of application and the steps required, refer to the applicable section in “**Appendix A. Applications**”.

Open Application

An open application assumes that all users are granted full permissions for all devices. An open application is useful in situations where the users require full access to all devices, or the majority of users will be assigned to a single role. In either of these situations, you can create user accounts and assign them to a single role (Basic Users), all with the same permissions.



Operating Tip — *For an open application, consider setting your default permission to Allow in the Configure DashBoard URM tab.*

This application may include one or more of the following:

- All users log in with the Default User account. This account is assigned to the Basic User role which has all read/write permissions set to Allow.
- Granting the Basic Users role full access to all devices while an Administrator account manages the permissions for all devices, the DashBoard Server, and the DashBoard URM.
- Configuring all user accounts permissions to “Allow” at the highest levels of the hierarchy for the Default User and Basic User role. You would only deny specific permissions where required.
- Configuring roles that enable different groups of users the same permissions.

Closed Application

A closed application assumes that users are either restricted to read access only and have no permissions for any devices on the subnet. Specific devices, such as an openGear frame, may or may not be locked with a password. This application may include one or more of the following:



Operating Tip — *For a closed application, consider setting your default permission to Deny in the Configure DashBoard URM tab.*

- Limiting the users access to all devices listed in the DashBoard client by setting permissions to “Deny” at the highest levels of the hierarchy for the Default User and Basic User role. You would only specify permissions where required.
- Configuring all user accounts to read-only access.
- The frames are password protected.

Custom Application

A custom application assumes that each user is granted specific permissions and belong to one or more roles. A single user can belong to many roles, each role with specific permissions, and be allowed to access any number of devices. Each user account may have specific permissions that apply only to that account. The advantage to using roles is that an Administrator can update the permissions for that one role and the change automatically affects the individual users assigned to that role.

In a custom application, some users may have only read access, other users may have read/write access for specific devices, or other users may have a combination of permissions. The configurations can be as complex or as simplistic as you need. Keep in mind that permissions assignment can be a multi-layered where access can be granted based on the user type, the role(s) they are assigned, and the device(s) they work with.

Installation Overview

The DashBoard Server and URM enables you to select how to manage user data: using your facility LDAP Server or setting up an isolated (embedded) database. Depending on how you have decided to manage the user data, you can assign permissions to individual users or groups of users, define user groups (roles) based on a variety of parameters, and manage access to devices on a single subnet.

This section provides a brief overview of the installation stages for the DashBoard Server and URM, and a summary of the DashBoard Server and URM features.

Simplified Block Diagram

Figure 1.1 provides a simplified workflow of the set up for the DashBoard Server and URM. Basic descriptions of each stage are provided below.

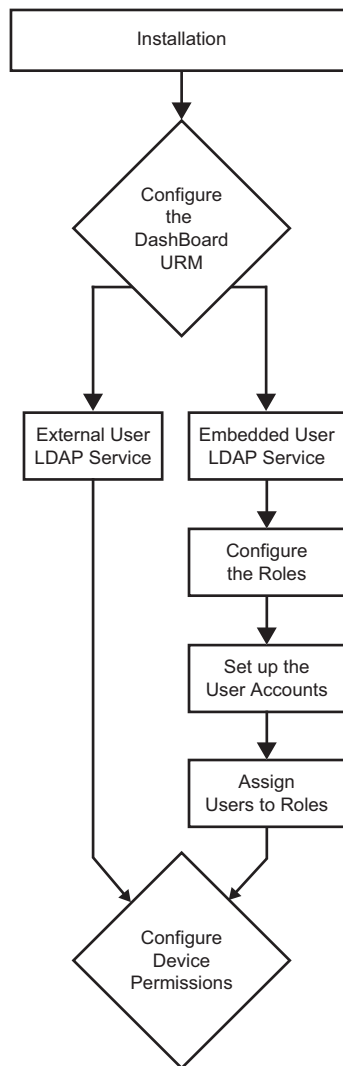


Figure 1.1 *Simplified Workflow Diagram*

Installation

1. Verify that the computer you wish to install the DashBoard Server meets the requirements described in the section “**System Requirements for the DashBoard Server**” on page 3-1.
2. Create a backup of your DashBoard client and settings.
3. Install the DashBoard Server software as described in the procedure “**Installing the DashBoard Server Software**” on page 3-2.
4. Verify the software installed correctly and that your server is running. Refer to the section “**Verifying the DashBoard Server**” on page 3-3 for details.

Configuring the DashBoard URM

1. Install a license key for the DashBoard URM feature.
2. Determine the type of database service you wish to run:
 - **Embedded LDAP Server** — By default, the DashBoard Server and URM is configured to operate as an isolated system where the DashBoard URM service maintains its own database for user information and

permissions. Therefore, no additional set up is required to use this type of system unless you wish to re-name your server. Proceed to step 3.

- **External LDAP Server** — DashBoard URM service to retrieve user data and permissions from an external LDAP Server. Proceed to step 4.

3. If you have chosen to use an **Embedded LDAP Server:**

- Configure the Administrators Role(s)
- Configure the Basic Users Role
- Create new role(s) as needed
- Configure the Default User Account
- Create new user accounts as needed
- Assign users to roles

4. If you have chosen to use an **External LDAP Server:**

- Configure the permissions database
- Configure the user accounts and roles database

Configuring the Device Permissions

1. Configure the DashBoard URM.
2. Update the list of devices.
3. To configure permissions for a device, refer to the section “**Configuring Permissions for a Device**” on page 5-4.

Documentation Terms and Conventions

The following terms and conventions are used throughout this manual:

- “**Administrator**” refers to a user that is allowed to configure and manage user accounts and permissions in the DashBoard Server and URM.
- “**Card**” refers to openGear terminal devices within openGear frames, including all components and switches.
- “**DashBoard client**” refers to the DashBoard Control System™ interface itself.
- “**DashBoard Server and URM**” refers to the DashBoard Server and the DashBoard URM licensed feature.
- “**DashBoard URM**” refers to the DashBoard User Rights Management licensed feature.
- “**Device**” refers to an object that displays in the tree views of the DashBoard client and the DashBoard Server and URM.
- “**Device information**” refers to data that records the names of tabs and associated menu items that display in the DashBoard client for that device. For example, device information for the FDR-6603 card would list the Signal tab, Product tab, Hardware tab, Setup tab, and Alarms tab as separate nodes under the card tab.
- “**External LDAP**” refers to a system that uses the external Lightweight Directory Access Protocol Server (LDAP) to manage a user database.
- “**Frame**” refers to any openGear frames that house the openGear cards.
- “**Operating Tip**” and “**Note**” boxes are used throughout this manual to provide additional user information.
- “**Role**” refers to a group of users that share the same permissions to perform tasks in the DashBoard Server and URM.
- “**User account**” identifies a specific user by name and includes information on that user such as log in name, password, and permissions set for the account. A user logs in to the DashBoard client using their ID and password as defined by their user account.
- “**Unauthenticated mode**” refers to instances where the DashBoard client is functioning without the DashBoard Server and URM enabled.

Interface Basics

In This Chapter

This chapter provides an overview of the menus available for the DashBoard Server and URM. Refer to the specific chapters for detailed information and procedures on how to configure your DashBoard Server and URM, set up user accounts, roles, and assign permissions.

The following topics are discussed:

- Additions to the DashBoard Client Interface
- Configure DashBoard Server Interface
- Configure DashBoard URM Interface
- Configure User Rights Dialog Overview
- Devices Tab Overview
- Users Tab Overview
- Tools Tab Overview

Additions to the DashBoard Client Interface

The Basic Tree View of the DashBoard client displays nodes specific to the DashBoard Server and URM. Expanding the nodes and selecting the options enables you to access the Configure User Rights dialog and begin configuring permissions for users and devices. Each time you launch the DashBoard client, you are prompted to log in with an user account and password.

This section provides an overview of the nodes now available in the Basic Tree View of DashBoard specific to the DashBoard Server and URM. For more information on using the Basic Tree View, refer to the ***DashBoard Control System User Manual***.

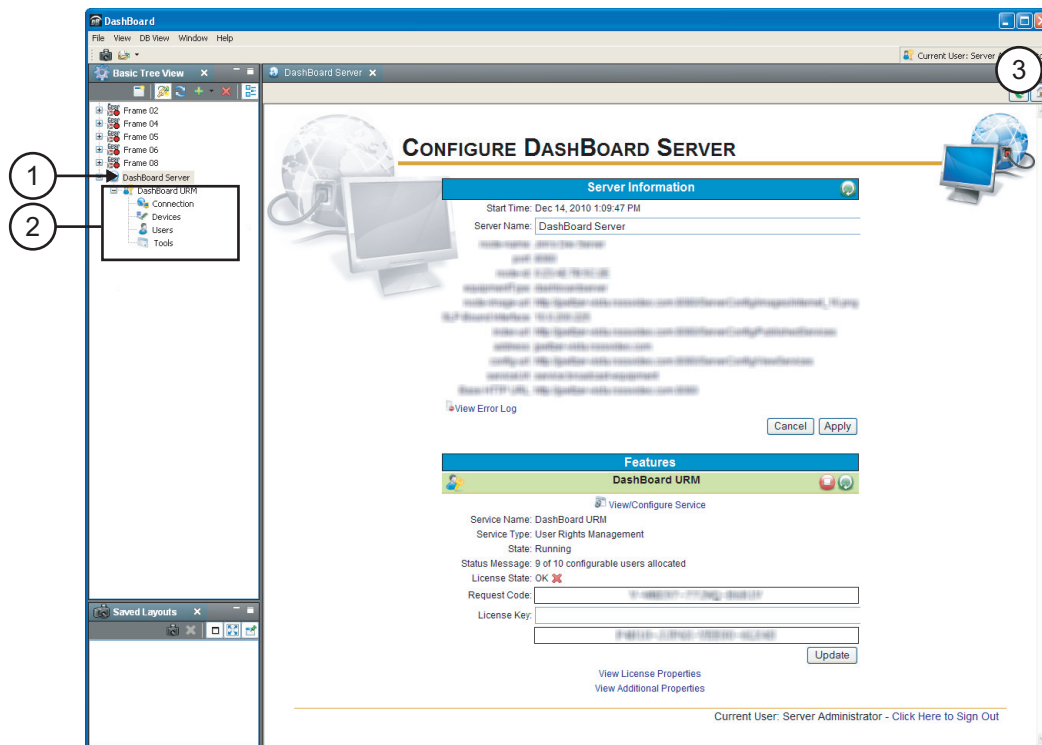






Figure 2.1 Basic Tree View — DashBoard Server Nodes





1. DashBoard Server Node

All services hosted by a specific DashBoard Server instance are displayed under that server's node in the DashBoard client tree view. Expand this node to view a list of the server plug-ins. Right-click the DashBoard Server node to display a menu with the following options:

-  **Open** — Select this option to display the **Configure DashBoard Server** tab in the DashBoard client. From this tab you can view server setup information, access the server error log, and install licenses for the server plug-ins.
-  **Permissions** — Select this option to display the **Configure User Rights** dialog in a separate window from the DashBoard client. From this dialog you can configure user accounts, roles, and devices, for the DashBoard Server and URM.
-  **Refresh** — Select this option to update the information for the DashBoard Server.
-  **Remove** — Select this option to delete the DashBoard Server and URM from the DashBoard client tree view.

2. DashBoard URM Node

This is a licensed feature of the DashBoard Server that provides options for configuring and monitoring user accounts, roles, and devices for the DashBoard Server and URM Service.

-  **Connection** — Double-click this icon to display the **Configure DashBoard URM** tab in the Device View. Refer to the section “**Configure DashBoard URM Interface**” on page 2-4 for details on this tab.
-  **Devices** — Double-click this icon to display the **Configure User Rights** dialog with the **Devices** tab pre-selected. Refer to the section “**Devices Tab Overview**” on page 2-7 for details on this tab.
-  **Users** — Double-click this icon to display the **Configure User Rights** dialog with the **Users** tab pre-selected. Refer to the section “**Users Tab Overview**” on page 2-9 for details on this tab.
-  **Tools** — Double-click this icon to display the **Configure User Rights** dialog with the **Tools** tab pre-selected. Refer to the section “**Tools Tab Overview**” on page 2-12 for details on this tab.

3. Current User Field

This field, located in the top permission corner of the DashBoard client, indicates the user account currently logged in to the DashBoard client. Note that a user account can simultaneously be in use in several DashBoard clients. You can configure how long users remain logged in to the DashBoard client.

Configure DashBoard Server Interface

This tab displays in the DashBoard client when you right-click the DashBoard Server node and select Open. Use this tab to view server configuration information, update the server display name, and view information on available licensed features.

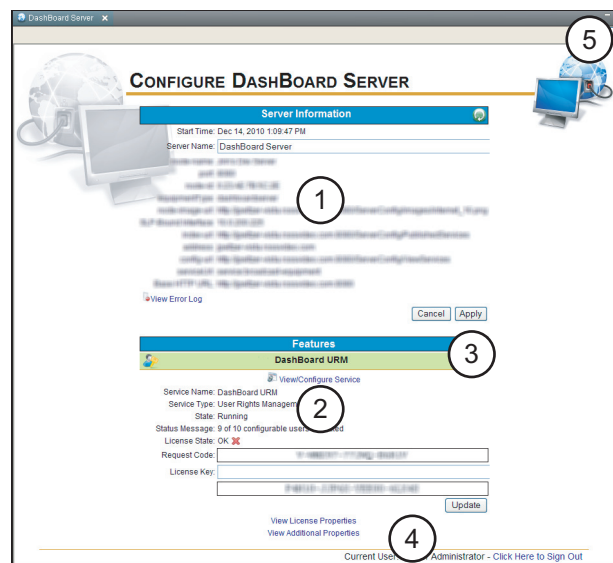


Figure 2.2 Configure DashBoard Server Tab

1. DashBoard Server Information


This area of the tab provides information about the DashBoard Server, including the number of users accounts currently configured or available. You cannot edit the set up information for the server or licensed features from this tab, but you can update the name of the server. You can also access the error log for your DashBoard Server by clicking the **View Error Log** link. For information on modifying or updating the server settings, refer to the section “**Installing the DashBoard Server Software**” on page 3-2.

2. Features Information

This area of the tab displays the licensed features of the DashBoard Server. For information on installing a licensed feature for the DashBoard Server, refer to the section “**Licensing the DashBoard URM**” on page 3-3.



- **View License Properties** — Select this link to display the read-only license information for your feature, including the number of users accounts currently configured or available.
- **View Additional Properties** — Select this link to display the read-only setup information for your DashBoard Server and URM.

For example, if you have installed a license key for the DashBoard URM feature, this area displays the name given to the feature that displays in all the DashBoard interfaces, request code, license key, number of configurable users allowed, and the status of the feature (as indicated by the background color of the feature header). The feature status ranges between the following:

- Red — A red background indicates an error condition for the license.
- Yellow — A yellow background indicates a possible error condition has occurred, but the license is still valid. This color may also indicate that your license is about to expire.
- Green — A green background indicates the license is valid and operational.
- Gray — A gray background indicates that the feature is unlicensed or the  button was clicked.

3. Stop and Re-Start Service Buttons

The header for the DashBoard URM licensed feature includes two buttons that function as follows:



-  — Click this button to stop running the DashBoard URM service. The DashBoard Server is now set to Unauthenticated mode. In this mode, permissions are ignored by the DashBoard clients communicating with the DashBoard Server and URM.
-  — Click this button to re-start the DashBoard URM service.

4. Current User and Sign Out Link

The **Current User** field displays the user name currently signed in to the DashBoard client. Select **Sign Out** to log out of the interface.

5. Refresh and Home Buttons

This toolbar includes the following two buttons:

-  — Click this button to return to the default or Home page for the node displayed in the tab.
-  — Click this button to update the information displayed in the Configure DashBoard Server tab.

Configure DashBoard URM Interface

This tab displays in the DashBoard client Device View when you expand the DashBoard Server node, right-click the DashBoard URM node, and select Open. This web-interface displays a tab within DashBoard and is used to configure how user data and permissions are managed. Use the options in this tab to configure your service as an isolated database or to use an external LDAP Server.

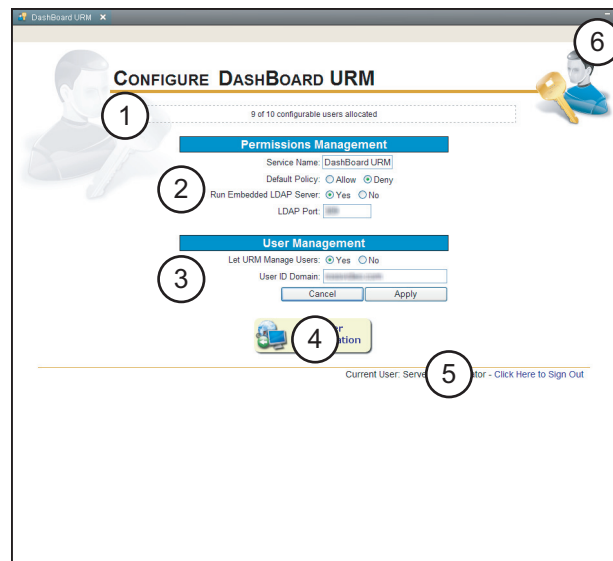


Figure 2.3 Configure DashBoard URM Tab

1. Configurable Users Allocated Field

This field displays the following information:

- the maximum number of users that can be configured and active in your DashBoard URM as stipulated by your license key. Note that if the license allows for an unlimited number of users, this field is blank as the information is not tracked.
- the total number of users that are currently configured and active in your DashBoard URM.

2. Permissions Management Area

This area provides options for configuring how the DashBoard Server manages permissions for the DashBoard URM. There are two types of database management:

- **Embedded LDAP Server** — This configuration enables the DashBoard Server and URM to create and maintain a separate database of permissions granted to users and roles. A user assigned to the Administrator role can manage permissions using the options in the Configure User Rights dialog. The number of users accounts currently configured or available is also displayed. This is the default.
- **External LDAP Server** — This configuration enables the DashBoard Server to import permissions from an external LDAP Server. Permissions for the DashBoard Server mirror those established by the external LDAP Server. Maintenance of this information is done via the external LDAP Server and not through the DashBoard Server and URM interfaces. However, you can still set permissions for devices, such as openGear frames and cards, using the DashBoard URM licensed feature.

3. User Management Area

This area provides options for configuring how the DashBoard Server manages user account and role assignments for the DashBoard URM. There are two types of database management:

- **Embedded LDAP Server** — This configuration enables the DashBoard Server and URM to create and maintain a separate database of user accounts and role assignments. A user assigned to the Administrator role can modify this information using the options in the Configure User Rights dialog. This is the default.
- **External LDAP Server** — This configuration enables the DashBoard Server to import user accounts and roles from your corporate LDAP Server. Settings such as user log in information, and memberships to groups, are assumed from the external LDAP Server. Maintenance of this information is done via the external LDAP Server and not through the DashBoard Server and URM interfaces. When a user account is created, or deleted, from the external LDAP Server, their information is also deleted from the DashBoard Server and URM database the next time you refresh the list in the **Configure User Rights** dialog.

4. Back to Server Configuration Button

Click this button to return to the **DashBoard Server Configuration** page.

5. Current User and Sign Out Link

The **Current User** field displays the user name currently signed in to the DashBoard client. Select **Sign Out** to log out of the interface.

6. Refresh and Home Buttons

This toolbar includes the following buttons:

- 🏠 — Click this button to return to default or Home page of the tab.
- 🔄 — Click this button to update the information displayed in the Configure DashBoard URM tab.

Configure User Rights Dialog Overview

This section provides a general overview of the menus and parameters available in the **Configure User Rights** dialog. This dialog presents options for configuring user permissions. Selecting sub-tabs switches between the views. Each time you launch the **Configure User Rights** dialog, a **Searching for new devices** progress bar displays directly above the **Refresh** button. This progress bar indicates that the DashBoard Server and URM is searching for device information that is not currently stored in the DashBoard Server.

You can access this dialog using one of the following methods:

- expand the **DashBoard Server** node, right-click the **DashBoard URM** node, and select **Permissions**.
- right-click on any device in the DashBoard client Tree View, and select **Permissions**; the device is pre-selected in the dialog.
- double-click the Devices, Users, or Tools node in the DashBoard client Tree View.

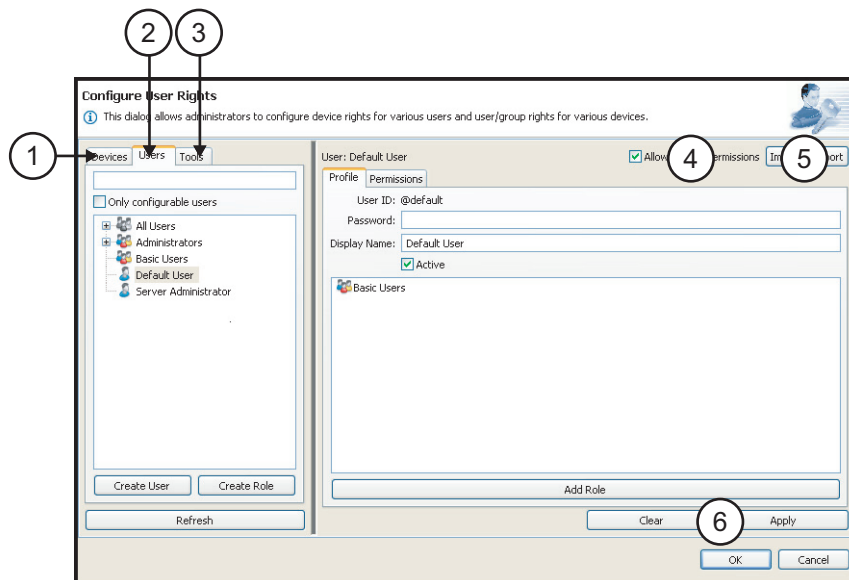


Figure 2.4 Configure User Rights Dialog

1. Devices Tab

The information displayed in the **Devices** tab is a copy of the Basic Tree View with extra nodes for the menus and parameters of devices. Use the options in this tab to specify permissions for devices, and assign users or roles to specific tasks. Permissions can be as specific or as general as required: specify permissions for a single menu on a single card to setting permissions for an entire frame contents, to setting global permissions for all devices detected on your subnet. Refer to the section “**Devices Tab Overview**” on page 2-7 for details on the options available in this tab.

2. User Tab

The **Users** tab displays a tree view that lists the roles and the user accounts assigned to each role. The available roles are shown as the top-level nodes in the tree with users assigned those roles listed beneath. Selecting a role allows the Administrator to see all permission settings for the role, and edit the permissions for that role. Selecting a user allows the Administrator to view/modify all permissions for the user and all groups to which the user belongs. A list of all users is shown under the **All Users** node. Refer to the section “**Users Tab Overview**” on page 2-9 for details on the options available in this tab.

3. Tools Tab

The **Tools** tab displays information from the DashBoard Server that cannot be represented on the **Devices** tab because the device is no longer detected in the current DashBoard client tree view. Elements in the Tools tab are shown in the hierarchy of the settings. Any type of device can be shown in this tree. The devices for which permissions have been defined in this tab need not be present in the current user’s DashBoard client. Refer to the section “**Tools Tab Overview**” on page 2-12 for details on the options available in this tab.

4. Allow custom permissions Checkbox

This check box reminds the Administrator of the number of users/roles that can be configured and when that limit is reached. If the DashBoard Server is not in compliance with its license (there are more users/roles configured than the license allows), all configuration is disabled and the Configure User Rights dialog displays an error message that warns the Administrator must take action to re-enable configuration. This checkbox only displays if your license allows a set number of configurable users/roles.

5. Import and Export Buttons

These buttons can be used to copy parameters and permissions to and from user, roles, and/or objects.

- Click **Import** to copy from one object (of the same type) to the currently selected object.
- Click **Export** to copy permissions from the currently selected object to another object of the same type.

6. Clear and Apply Buttons

Click **Apply** to save changes to all users and roles with unsaved changes. Until the **Apply** button is clicked, all users/groups with unsaved changes are marked with an asterisk (*). Clicking **Clear** clears any unsaved changes, restoring items to the previously saved states.

Devices Tab Overview

This section provides a general overview of the menus and parameters available in the **Devices** tab of the Configure User Rights dialog. This tab enables an Administrator to configure permissions for devices currently detected in the DashBoard client. You can access this dialog by expanding the **DashBoard Server** node, expanding the **DashBoard URM** node, and double-clicking the **Devices** node.

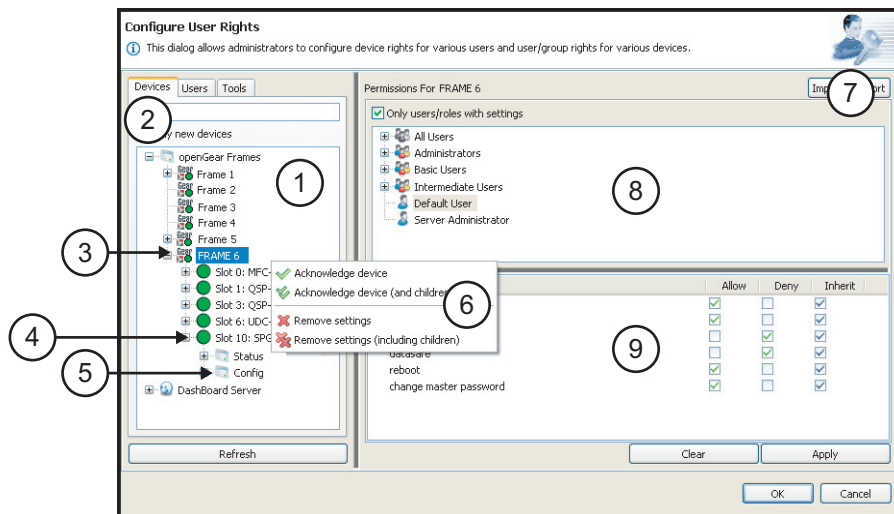



Figure 2.5 Configure User Rights — Devices Tab

1. Device Tree View

The Device View of the tab displays a hierarchical list of the available devices, such as openGear frames and cards, available for configuration by the DashBoard URM. You can expand the nodes to view additional cards, menus, and parameters. For example, in **Figure 2.5** the node for the SPG-8260 card is expanded to display the available tabs and menus.

2. Only New Devices

This tab option enables the tree view to display only those devices communicating with the DashBoard client, that do not have information uploaded and stored to the DashBoard URM LDAP database.

-  — This icon indicates that this node, or a child node, does not have information uploaded and stored to the DashBoard URM LDAP database.
- * — An asterisk beside a device indicates that the specific device, or setting, indicates that the device does not have information stored to the DashBoard URM LDAP database.

3. Parent Device Node

Expanding a parent node displays a list of the associated child devices. You can configure permissions for a single parent device, assign users or roles that are allowed to configure that device, or you can set the device to inherit permissions from the openGear node. You can also simultaneously configure permissions for the parent and any child devices listed below. An example of a parent device is a DFR-8321-N frame.

4. Child Device Node





Expanding a child node displays a list of the menus and parameters available for that device. This list can reflect the menus and parameters available in the DashBoard client. Child devices that have neither had permissions set nor confirmed to be inherit from the hierarchy are shown with a warning icon so they can have permissions set. You can configure permissions for a specific child device, assign users or roles that are allowed to configure that device, or you can set the device to inherit permissions from the openGear node. You can also simultaneously configure permissions for the child device and any objects listed below it in the tree view.

5. Menu Options Node

Extra nodes for the menus and parameters are added beneath the device nodes. The available options are based on the specific device you selected and reflect what is available in the DashBoard client.

6. Acknowledge Device Dialog

This dialog displays when you right-click a device from the Device View. From this dialog you can add new devices to the Tree View by downloading their settings and configurations to your DashBoard Server database. The following options are available:

-  **Acknowledge Device** — Select this option to upload the device name and type to the DashBoard Server. Device information includes all the settings, menus, and permissions for that device. For example, selecting this option for a frame uploads the information only for that frame and not the cards installed in that frame.
-  **Acknowledge Device (and children)** — Select this option to upload information for the selected device and any associated devices listed beneath it in the tree view. Device information includes a list of the available menus and settings for the device. This information is saved in the DashBoard Server database. For example, selecting this option for a frame uploads the information for the frame, and the cards installed in that frame.
-  **Remove Settings** — Select this option to delete the information for this specific device from the DashBoard Server. Any permissions and settings you have specified in the DashBoard URM are no longer in effect. For example, selecting this option for a frame removes the permissions for the frame and not the cards installed in the frame.
-  **Remove Settings (including children)** — Select this option to delete the information for this device and any devices listed under it in the Tree View from the DashBoard Server. Any permissions and settings you have specified in the DashBoard URM are no longer in effect for this device and any child devices.

7. Import and Export Buttons

These buttons can be used to copy permissions to and from devices.

- Click **Import** to copy the currently displayed permissions to another similar device.
- Click **Export** to copy permissions from the currently selected device to another device of the same type.

8. Permissions For Area



The Permissions For area displays all users and roles with settings for the selected device or menu item. To view permissions for a specific role or user, select the icon from the Permissions For area and the Property Editor updates to list the permissions.

9. Property Editor

The Property Editor of a device displays a list of the available rights to configure for that specific device. Depending on the device you selected, you can configure permissions for software upgrades, read/write permissions, or for individual menus. Just like configuring users and roles, you can select Allow, Deny, or Inherit for each property listed.

- **Allow** — Select this option to enable the role/user to perform the specific task for this device.
- **Deny** — Select this option to prevent the role/user from performing the specific task.
- **Inherit** — Select this option to assume the permission settings from the hierarchy. For example, selecting Inherit for a specific card will apply the permissions as set in the frame that the card is installed in.

Note that if a property has two check boxes selected:

-  — A blue check mark indicates the property inherits its setting from the hierarchy.
-  — A green check mark indicates the inherited permission setting. For example, in **Figure 2.5**, the Reboot permission is inherited and set to Allow.

Users Tab Overview

This section provides a general overview of the options available in the **User** tab of the **Configure User Rights** dialog. From this tab you can manage users and roles. Use this tab to perform tasks such as create and manage users for an Embedded LDAP database, assign users to roles, and specify permissions. Permissions can be based on the

4. Allow custom permissions Check Box

This check box reminds the Administrator of the number of users/roles that can be configured and when that limit is reached if you do not have a license that enables an unlimited number of users. If the DashBoard Server is not in compliance with its license (there are more users/roles configured than the license allows), all configuration is disabled and the **Configure User Rights** dialog displays an error message that warns the Administrator to take action to re-able configuration.

When running an External LDAP system, right-clicking a user in the **User** tab displays a menu with the following options:

- **Allow custom permissions** — If your DashBoard Server has not reached the maximum number of configurable users as defined by your license, selecting this option enables you to configure the selected user account.
- **Delete setting(s) for user** — Selecting this option enables you to remove permissions for the selected user.

When running an Embedded LDAP system, right-clicking a user in the **User** tab displays a menu with the following options:

- **Delete setting(s) for user** — Selecting this option enables you to remove permissions for the selected user.
- **Delete User Account** — Selecting this option enables you to delete the selected user account. This is helpful when your DashBoard Server is not in compliance with its license.

5. User Editor Area

This area of the dialog displays two tabs: Profile and Permissions. The options in these tabs enable you to configure user data (name, E-mail address), and set permissions.

6. Profile Tab

If you are configuring a user account, this tab displays the account ID, user display name, and enables you to specify a new password or display name. From this tab you can assign users to roles, and activate or de-active the account. If the user is validated against an external LDAP Server, the contact information, password, display name, and permissions are read-only.

If you are configuring a role, this tab displays the role ID and display name as read-only text. If you are using an external LDAP for your user information, all user and role (group) information on this tab is read-only.

7. Permissions Tab

This tab enables you to select and modify permissions specific to the selected user or role. A tree view, based on the information seen in the Basic Tree View of the DashBoard client, enables you to select objects to configure permissions for the specified user or role. Selecting a node in the tree view of this tab displays the settings for that user or role with that object in the Property Editor. For example, selecting a node for a card updates the Property Editor for that user to display the options to configure permissions for.



Select the **Show only devices with settings** option to display only those objects with settings already configured for the selected user or role. The default setting is unselected.

8. Property Editor

The Property Editor for a user shows all of the permissions set for this user. This area updates every time a new user, role, or device is selected for configuration. When configuring permissions, this area displays the available permissions can be set to Allow, Deny, or Inherit. Any object can be selected to have its permissions modified for the user. By default, all the permissions are set to **Inherit** for new accounts and roles.

- **Allow** — Select this option to enable the role or user to perform the specific task. For example, if you select Allow for the Modify Server Settings for the Administrators role, all users assigned to that role can change the settings for the DashBoard Server.
- **Deny** — Select this option to prevent the role or user to perform the specific task. For example, if you select Deny for the Modify Server Settings for the Basic Users role, all users assigned to that role cannot change the settings for the DashBoard Server.
- **Inherit** — Select this option to assume the permission settings from the hierarchy. For example, selecting Inherit for a specific card will apply the permissions as set in the frame that the card is installed in.

Note that if a property has two check boxes selected:

-  — A blue check mark indicates the property inherits its permissions from the hierarchy.
-  — A green check mark indicates the permission inherited. For example, in **Figure 2.6** all the permissions are inherited.

9. Clear and Apply Buttons

Click **Apply** to save changes to all users and roles with unsaved changes. Until the **Apply** button is clicked, all objects with unsaved changes are marked with an asterisk (*). Clicking **Clear** clears any unsaved changes, restoring items to the previously saved states.

Tools Tab Overview

The **Tools** tab enables the Administrator to perform routine maintenance for inactive devices or user accounts. From this tab you can view information for devices no longer displayed in the DashBoard client, and the **Configure User Rights** dialog. Use this tab to perform tasks such as deleting inactive devices no longer used in your facility, updating an offline device before re-installing it to your network, or applying parameters of an inactive device to a newly installed device. For example, you can export permissions from an inactive MUX-8258-A to an active MUX-8258-A in a recently installed DFR-8321-N frame.

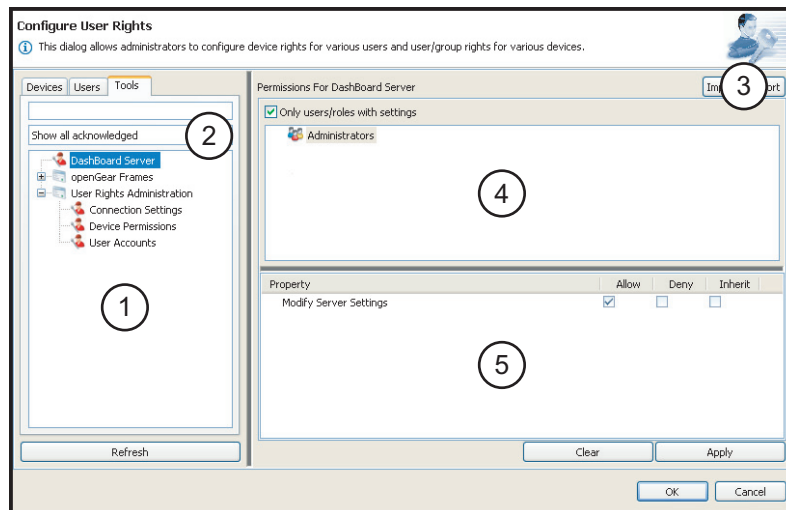




Figure 2.7 Configure User Rights — Tools Tab

1. Tools Tree View

This area displays a list of devices with information saved in the DashBoard Server and URM but are currently inactive. A device is inactive when it is no longer available on the same network that the DashBoard client is using and does not display in the tree views. For example, a card that was physically removed from a frame, or when an entire frame was taken offline. Click **Refresh** to update the list of devices in the tree view.

The view when a node is selected in this tree view is the same as the view when a node in the **Devices** tab is selected. The nodes displayed in this tree view is dependent on what is selected in the **Display** menu. Nodes in the tree view include one of the following icons:

-  — This icon indicates the presence of additional elements listed under the selected node. For example, menus that display in the DashBoard client.
-  — This icon indicates the absence of additional elements.

2. Display Menu

This menu is located at the top of the **Tools** tab and is used to specify the type of information displayed in the tree view.

- **Show all acknowledged** — This option enables the **Tools** tab to display all devices that have information uploaded and permissions configured in the DashBoard Server and URM. This is the default.
- **Show all saved settings** — This option enables the **Tools** tab to display inactive devices that have configured permissions saved in the DashBoard Server and URM.
- **Show missing acknowledged** — This option enables the **Tools** tab to display inactive devices that do have information uploaded to the DashBoard Server and URM but no longer displays in the DashBoard interfaces. For example, an offline MUX-8258-A card that had information uploaded to the DashBoard Server and URM before the card was removed from the frame.
- **Show missing with settings** — This option enables the **Tools** tab to display inactive devices that had permissions configured, but no longer display in the DashBoard interfaces. For example, an offline MUX-8258-A card that was to read-only to the Default User.

3. Import and Export Buttons

These buttons can be used to copy permissions to and from similar objects.

- Click **Import** to copy the currently displayed permissions to another object.
- Click **Export** to copy permissions from the currently selected object to another object of the same type.



4. Permissions For Area

This area displays the roles and users assigned to the device selected in the Tools tree view. You can add additional users and roles to configure permissions for this device.

5. Property Editor

This area displays the properties and permissions configured for the selected device. You can update the settings in this area and click **Apply** to save your changes to the database. The new settings are applied to the device when the device is active. Until the **Apply** button is clicked, all users/groups with unsaved changes are marked with an asterisk (*).

Note that if a property has two check boxes selected:

-  — The blue check mark indicates the property inherits its permissions from the hierarchy.
-  — The green check mark indicates the permission inherited.

Installation

In This Chapter

This chapter provides instructions for installing the DashBoard Server, installing a license key for the DashBoard URM feature, and configuring the DashBoard URM to use an external LDAP Server.

The following topics are discussed:

- Before You Begin
- Installing the DashBoard Server Software
- Verifying the DashBoard Server
- Licensing the DashBoard URM
- Configuring the DashBoard URM

Before You Begin

Before installing any software for your DashBoard Server and URM, ensure that you exit all other programs currently running.



Note — *Contact your I.T. Department if you experience communications issues with DashBoard Server and URM and are running anti-virus software. You may need to verify that there is an exception in your firewall to allow DashBoard to receive UPD data via Port 427.*

System Requirements for the DashBoard Server

Refer to the following section for information on the system requirements for your DashBoard Server.



Note — *You cannot install the DashBoard Server and URM at this time on a computer running Linux® Fedora® or Apple® Mac® OS®.*

Microsoft® Windows® XP/XP64/Vista/Vista64/7 Systems

The following are the minimum requirements when installing the DashBoard Server on a Microsoft Windows system:

- Intel® Pentium 4, 1.6GHz (Intel® Core™ 2 Duo recommended)
- 2GB or more of RAM
- 200MB available in HD space
- Microsoft Windows Server 2008
- Microsoft® Internet Explorer® version 5 (minimum)

Installing the DashBoard Server Software

This section includes instructions for installing the DashBoard Server on your system.

Creating a Backup of the Settings and Licensed Features

It is recommended to create a backup of your DashBoard client settings and license files before installing the DashBoard Server software.

- **Microsoft® Windows®** — DashBoard automatically uninstalls a previously installed version, but not your settings.
 - › To create a back up your settings on a system running Microsoft® XP® or earlier, navigate to the metadata folder located at **c:\Program Files\DashBoard Server** and copy the folder contents to a new location.
 - › If you are running Microsoft® Vista® or higher, the metadata folder is at: **c:\DashBoard Server**. Copy the folder to a new location.

Installing the DashBoard Server Software

Note that if you are running Microsoft Vista or higher, the DashBoard main folder is at: **c:\DashBoard Server** while previous Microsoft operating systems will install DashBoard to **c:\Program Files\DashBoard Server**.

Use the following procedure to install DashBoard Server on a computer running Microsoft Windows®:

1. Verify that you are running DashBoard client software version 4.0 or higher on all workstations to be used in you facility with the DashBoard Server. Refer to the ***DashBoard Control System*** manual for instructions on upgrading your client software.
2. Access the DashBoard Server software using one of the following methods:
 - Contact Ross Technical Support; or
 - Load the DashBoard Server software CD into the DVD/CD ROM tray of your computer.
3. If you are accessing the software from a CD, the **Installation Wizard** automatically runs. If the Wizard does not automatically run, you can also install the DashBoard Server software, navigate to your DVD/CD ROM drive in the **Navigation Pane**, so that the CD contents are displayed in the **Main Window** of Microsoft Windows® Explorer®.
4. Launch **DBServer1.0.0-setup.exe** to begin installing the DashBoard Server onto your computer.
5. Follow the prompts to complete the installation of DashBoard Server onto your computer.

This completes the procedure for installing DashBoard Server on a computer running Microsoft Windows®.

Uninstalling the DashBoard Server Software

Ensure to create a backup for your settings and licensed features as outlined the section “**Creating a Backup of the Settings and Licensed Features**” on page 3-2 if you wish to retain your user data before removing DashBoard Server from your computer.



Important — *If a user is logged into the DashBoard Server when you uninstall the DashBoard Server software, that DashBoard client will run in Unauthenticated mode.*

To uninstall the DashBoard Server software:

1. If you are using a computer running Microsoft® Windows®, use the **Add/Remove Software** program located in the Windows® Control Panel.
2. Do not delete the DashBoard Server directory, instead run the **Add/Remove Software** program. Deleting the directory without running the **Add/Remove Software** program results in a number of dead registry and start

menu items on your system. You can delete the directory to remove your user data after you run the **Add/Remove Software** program.

Verifying the DashBoard Server

Once you have installed the DashBoard Server software, you can launch the DashBoard client to view the read-only information and the error logs for your server. There are several methods for viewing information for your DashBoard Server. For more information on the types of information displayed in the **Configure DashBoard Server** tab, refer to the section “**Configure DashBoard Server Interface**” on page 2-3. Refer to the section “**Configuring for an Embedded LDAP Server**” on page 3-4 for details on re-naming your DashBoard Server.



Operating Tip — *To configure the settings when on a local host without logging into a DashBoard client, navigate to the DashBoard Server and URM web page at <http://localhost:8080/ServerConfig/ViewServices>.*

To view the information via DashBoard:

1. Double-click the DashBoard client icon on your desktop.
2. You are prompted to enter a user name and password. Use the following Default User account information to log in to the DashBoard client for the initial start-up:
 - User name: @default
 - Password: <leave blank>
3. Right-click the DashBoard Server node in the Basic Tree View of the DashBoard client.
4. Select **Open** to display the **Configure DashBoard Server** tab in the Device View.
5. To view the error log for your DashBoard Server, select the **View Error Log** link located in the **Server Information** area.
6. To view the properties for all your licensed features, select the **View License Properties** link located in the **Features** area.
7. To access the **Configure DashBoard URM** tab, select the **View/Configure Service** link located in the **Features** area.

To view the error log for your DashBoard Server:

1. Launch the DashBoard client by double-clicking the DashBoard icon on your desktop.
2. Enter your account ID and password in the **Login to the DashBoard** dialog. The account you are using must be configured as an Administrator.
3. Right-click the DashBoard Server node in the Basic Tree View.
4. Select **Open** to display the **Configure DashBoard Server** tab in the Device View of the DashBoard client.
5. Select **View Error Log**. The tab view updates to display the error log for the DashBoard Server you logged in to.

Licensing the DashBoard URM

This section provides instructions for installing a license key for your DashBoard URM feature.

Before You Begin

When installing a license key:

- Ensure that you are using version 4.0.0 or higher of the DashBoard client. This information is available by selecting **Help > About DashBoard** from the DashBoard client toolbar.
- Ensure that you have installed the DashBoard Server software on your computer.

To install a license key for the DashBoard URM feature:

1. Double-click the DashBoard client icon on your desktop.
2. Right-click the DashBoard Server node in the Basic Tree View of the DashBoard client.
3. Select **Open** to display the **Configure DashBoard Server** tab in the Device View.
4. Locate the **DashBoard URM** header of the **Features** area.
5. Make a note of the text displayed in the **Request Code** field.
6. Contact Ross Video Technical Support using the information found in the section “**Contact Us**” of this manual.
 - When you speak to the Technical Support representative, tell them your name, your facility name, and the **Request Code** from the **DashBoard Server** tab.
 - You will be given a code that must be entered in the **License Key** field of the **DashBoard Server** tab.
 - Make a note of the maximum number of configurable users your license enables for your DashBoard Server.
7. Enter the code in the **License Key** field. It is recommended to record the key code should you need to re-license the DashBoard URM on the same computer.
8. Click **Update**. The header background for the DashBoard URM is green, and the **State** field displays “Running”.

Configuring the DashBoard URM

The **Configure DashBoard URM** tab enables you to select whether the database is an embedded server where user information is managed in DashBoard Server’s LDAP, or to link the database to an external or corporate LDAP directory. The default is an embedded service, where an Administrator manages DashBoard Server user accounts, roles, and permissions using the options in the Configure User Rights dialog. This section outlines how to configure both types.

Configuring for an Embedded LDAP Server

By default, the DashBoard Server and URM is configured to operate as an isolated system where the DashBoard URM service maintains its own database for user information and permissions. Therefore no additional set up is required to use this type of system unless you wish to re-name your server. The server name displays in the Basic Tree View of the DashBoard clients on your network, and the tabs in the **Configure User Rights** dialog.

To re-name your server:

1. Display the **DashBoard Server** tab in the DashBoard client.
2. Type a new name for your server in the **Server Name** field.
3. Click **Apply**.

Configuring for an External LDAP Server

This section outlines how to configure your DashBoard URM service to retrieve user data and permissions from an external LDAP Server. The **Configure URM** menu is a web-interface usable within the DashBoard client.



Important — *It is highly recommended to use an Embedded LDAP Server.*

To configure the permissions database:

1. Navigate to the **Configure DashBoard URM** tab as follows:
 - Right-click the **DashBoard URM** node in the Basic Tree View.
 - Select **Open** to display the tab in the Device View of the DashBoard client.
2. Locate the **Permissions Management** header.
3. If required, type a new display name for your DashBoard URM in the **Service Name** field.
4. Select **No** from the **Run Embedded LDAP Server**. The DashBoard URM will apply the same permissions for users as defined by the external LDAP Server.
5. Type the required contact information for the external LDAP Server in the following fields:
 - **LDAP Host/IP** — Enter the host name, or IP address, for the external LDAP Server host that will be used to determine user permissions.
 - **Bind DN** — Enter the LDAP Distinguished Name of LDAP User that can be used to read/modify the information on the LDAP Server.
 - **Bind Password** — Enter the corresponding password for the username entered in the **Bind DN** field.
 - **LDAP Port** — Enter the port on which the external LDAP Server is listening. The default is 389.
6. Click **Apply** to save your changes.

To configure the user accounts and roles database:

1. Navigate to the **Configure DashBoard URM** tab as follows:
 - Right-click the **DashBoard URM** node in the Basic Tree View.
 - Select **Open** to display the tab in the Device View of the DashBoard client.
2. Locate the **User Management** header.
3. Select **No** from the **Let URM Manage Users**.
4. Specify an external LDAP Server to retrieve user data from an external LDAP Server by updating the following fields:
 - **User ID Domain** — All user IDs are required to be in the form of an E-mail address using the domain name (without the @ symbol). The User ID Domain field enables you to create a default suffix for the E-mail address that is automatically added to the User ID field of the Login dialog.
 - **LDAP Host/IP** — Enter the host name, or IP address, for the external LDAP Server host.
 - **Bind DN** — Enter the LDAP Distinguished Name of LDAP User that can be used to read the information on the LDAP Server.
 - **Bind Password** — Enter the corresponding password for the username entered in the **Bind DN** field.
 - **LDAP Port** — Enter the port on which the external LDAP Server is listening. The default is 389.

5. Configure the DashBoard URM service to retrieve user data from an external LDAP Server.
 - **Base User DN** — Enter the root node for the list of users in the external LDAP.
 - **Object Class** — Enter the attribute that defines the object class for user data.
 - **User ID Attribute** — Enter the attribute that the external LDAP filter uses as a user ID.
 - **Full Name Attribute** — Enter the attribute that the external LDAP filter uses to specify a user's full name.
 - **Email Address Attribute** — Enter the attribute that the external LDAP filter uses to specify a user's E-mail address.
6. Configure the DashBoard URM service to define roles as set by an external LDAP Server:
 - **Base Group DN** — Enter the root node for all of the roles (groups) in the LDAP server.
 - **Object Class** — Enter the attribute that defines the object class for groups.
 - **Group ID Attribute** — Enter the attribute that the external LDAP filter uses as a group ID.
 - **Group Name Attribute** — Enter the attribute that the external LDAP filter uses to specify a group's full name.
 - **Group Membership Attribute** — Enter
7. Click **Apply** to save your changes.

Configuring Roles and Accounts

In This Chapter

This chapter outlines how to create user accounts and roles, manage user permissions, and assign users to specific roles. The procedures assume the following: the DashBoard URM is operating as an embedded (isolated) database where an Administrator sets the user data and permissions and not an external LDAP Server, the DashBoard Server and URM display names are set to the default values.



Note — *Contact Ross Video Technical Support if the Administrator is unable to log in to DashBoard client.*

The following topics are discussed:

- User Permissions Overview
- Using an External LDAP Server
- Configuring the Administrators Role
- Configuring the Basic Users Role
- Creating a New Role
- Configuring the Default User Account
- Creating a New User Account
- Assigning Users to Roles
- Managing Permissions

User Permissions Overview

The first step to configuring your DashBoard Server and URM is to define the roles for your service, such as Basic and Administrator. These roles are set up by default in the software, but you may want to modify their permissions to suit your facility needs. Then you will create user accounts, with each account using a unique ID and password. Once you have the roles configured and created all your user accounts, you can further define your accounts by assigning them to those roles. The specific permissions you wish to grant each user or role can be as complex or as simplistic as you require.



Note — *If you are using an external LDAP Server for the user database, you cannot edit the user or role details from the **Configure User Rights** dialog in DashBoard. You can configure permissions for those users and roles. For more information on the features of the Configure User Rights dialog, refer to the section “**Configure User Rights Dialog Overview**” on page 2-6.*

Configuring Roles

A role is a group of users that share the same permissions because they belong to that specific role. By default, when using the internal LDAP Server, the DashBoard URM includes two roles: Administrator and Basic User. You

can configure additional roles, based on any number of parameters, as required. If you are using an external LDAP Server, only the roles defined by the LDAP are used.

You need at least one Administrator who can modify server and URM settings. The DashBoard Server and URM automatically includes an Administrator role and a Basic Users role.

- **Administrator** role — You can use this role to set permissions for configuring server and URM settings, network settings, and/or to perform software upgrades.
- **Basic Users** role — You can use this role to assign permissions that might apply to a wide range of users who do not need full access.

Configuring User Accounts


Users can be assigned individual accounts, with a unique user ID and password, or log into the DashBoard client using the Default User account. When using an embedded LDAP Server, you can create and manage user accounts and the information is confined to the DashBoard Server and URM. For each user account, you configure the following:

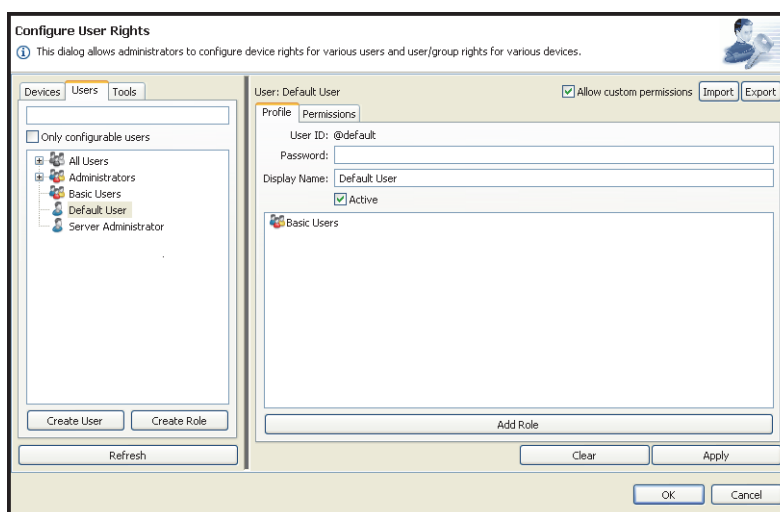
- **User ID** — This is the e-mail address the user enters in the **User name** field of the DashBoard client log in dialog.
- **Password** — This is the text the user enters in the **Password** field of the DashBoard client login dialog.
- **Display Name** — This is the text that displays in the **Current User** field of the DashBoard client.
- **Active** check box — Selecting this check box for the user account validates the account. Clearing the check box disables the account and the information can no longer be used to log into the DashBoard client.



Note — *If you are using an external LDAP Server for the user database, you can only manage the user permissions from the **Configure User Rights** dialog in DashBoard.*

To display the **Configure User Rights** dialog:

1. Double-click the DashBoard client icon on your desktop.
2. You are prompted to enter a user name and password. Use the following Default User account information to log in to the DashBoard client for the initial start-up:
 - User name: @default
 - Password: <leave blank>
3. Navigate to the **Users** tab in the **Configure User Rights** dialog as follows:
 - In the DashBoard client, expand the **DashBoard Server** node in the Basic Tree View.
 - Expand the **DashBoard URM** node.
 - Select  **Users** to display the **Configure User Rights** dialog. The **Users** tab is automatically selected in the dialog.



Configure User Rights Dialog - Users Tab

Using an External LDAP Server

Linking to an external LDAP Server prevents the need for extra user data management at the DashBoard Server level. If you have elected to use an external LDAP Server as a basis for your DashBoard Server and URM database, ensure that you have set up DashBoard to communicate with your external LDAP Server as outlined in the section “**Configuring for an External LDAP Server**” on page 3-5.

User Accounts and Roles

Because user account and role (group) information is derived from the external LDAP Server, permissions are managed by your external LDAP database. However, you can update the list of user accounts and roles by clicking **Refresh** in the **Users** tab. Clicking **Refresh** clears the cache in the configuration client and updates the DashBoard Server and URM. This action also detects changes in the groups.

- If users are deleted from the external LDAP Server, their permissions are removed from the DashBoard URM directory only when you delete their account via the **Configure User Rights** dialog. The DashBoard Server will completely remove all user data for users that have been removed from the external LDAP Server directory.
- The **Missing Users** node in the **Users** tab displays only when there are configurable user accounts which have been removed/disabled and you do not have a license that allows an unlimited number of configured accounts.
- If roles are deleted from the external LDAP Server, their permissions are no longer valid in the DashBoard URM directory.
- If users are removed from the groups in the external LDAP Server, the change is reflected in the DashBoard URM directory.

Permissions for Devices

Even if you have elected to use an external LDAP Server for your user account and role management, you can still assign permissions for devices. Refer to the section “**Device Management Overview**” on page 5-1 for details on configuring user permissions for devices.

Configuring the Administrators Role

This section outlines how to configure the default Administrators role for the DashBoard Server and URM. The permissions you configure for this role will depend on your facility requirements and the types of tasks you wish to

assign to this role. The following are some of the available objects in the tree views you can configure permissions for:

- **openGear Frames** — Select this node to configure permissions for openGear devices displayed in the DashBoard client tree view. Refer to the section “**Device Management Overview**” on page 5-1 for more information.
- **DashBoard Server** — Select this node to configure permissions for the DashBoard Server only. You can expand this node to display further objects to configure, or you can configure the entire system.
- **DashBoard URM** — Select this node, located under the DashBoard Server node, to configure permissions for elements of the DashBoard URM.

To display the Editor Area for the Administrators role:

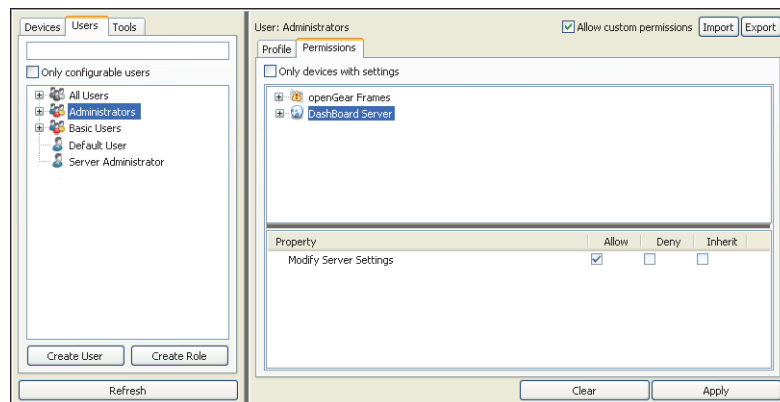
1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Select the **Administrators** node.
3. Select the **Profile** tab to view a list of users assigned to the role. By default, the Administrators role is set to Active (the **Active** check box is selected).
4. Select the **Permissions** tab to configure permissions for the role.

To configure permissions for the DashBoard Server:

1. Display the **Permissions** tab in the **Configure User Rights** dialog for the role.
2. Select the **DashBoard Server** node. The **Property Editor** displays the available options for the Administrators role.



Note — If you select **Inherit** for any of the properties, the permissions for that property are inherited from the hierarchy (higher levels of the tree). If there are settings not set higher in the tree, the properties then assume the value of the Default Policy as defined in the **Configure DashBoard URM** tab.

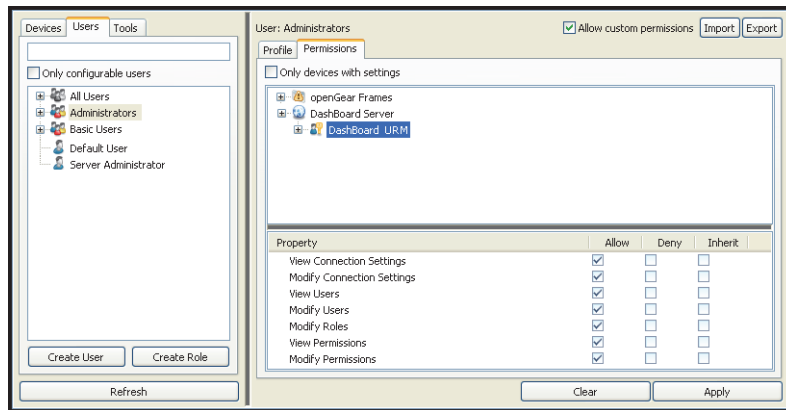


Administrators Role — DashBoard Server Settings

3. Configure the following permissions:
 - **Modify Server Settings** — Specifies whether any user assigned to this role can modify/view connection settings, modify/view user accounts, modify roles, and modify/view device permissions. This is a global setting and specifies permissions for the entire DashBoard Server and URM.
4. Click **Apply** to save your changes.

To configure permissions for the DashBoard URM:

1. Display the **Permissions** tab in the **Configure User Rights** dialog for the role.
2. Expand the **DashBoard Server** node.
3. Select **DashBoard URM**. The **Property Editor** displays the available options for the Administrators role.



Administrators Role — DashBoard URM Settings

4. Configure the following permissions for the DashBoard URM:
 - **View Connection Settings** — Specifies if the Administrators role can view the DashBoard Server and URM settings.
 - **Modify Connection Settings** — Specifies if the Administrators role can update and change the communication settings for the DashBoard URM.
 - **View Users** — Specifies if the Administrators role can only view the user account settings. This role cannot modify the settings.
 - **Modify Users** — Specifies if the Administrators role can modify information about the users such as the display name. Only applies when using an embedded LDAP.
 - **Modify Roles** — Specifies if the Administrators role can modify information about the role, and able to add/remove users from the roles. Only applies when using an embedded LDAP.
 - **View Permissions** — Specifies if the Administrators role can view the permissions for user accounts and devices.
 - **Modify Permissions** — Specifies if the Administrators role can change the permission settings for user accounts, and devices.
5. Click **Apply** to save your changes.

To configure permissions for an element in the DashBoard URM:

1. Display the **Permissions** tab in the **Configure User Rights** dialog for the role.
2. Expand the **DashBoard Server** node.
3. Expand the **DashBoard URM** node.
4. Select the element of the DashBoard URM you wish to configure permissions for. The **Property Editor** displays the available options for that element.



Note — If you select **Inherit** for any of the properties, the permissions for that property are inherited from the DashBoard URM and/or the DashBoard Server configuration.

5. If you selected **Connection Settings**, you can configure the following permissions: **Modify Connection Settings** and **View Connection Settings**.

6. If you selected **User Accounts**, you can configure the following permissions: **Modify Roles**, **Modify Users**, and **View Users**.
7. If you selected **Device Permissions**, you can configure the following permissions: **Modify Permissions**, and **View Permissions**.
8. Click **Apply** to save your changes.

To configure permissions for all openGear devices:

Refer to the section “**Configuring Permissions for openGear Devices**” on page 5-3 for details.

To configure permissions for a specific openGear device:

Refer to the section “**Configuring Permissions for a Device**” on page 5-4 or the section “**To configure permissions for a specific menu of a device:**” on page 5-5 for details.

Configuring the Basic Users Role

The DashBoard Server and URM come standard with two pre-configured roles: Basic Users and Administrators role.

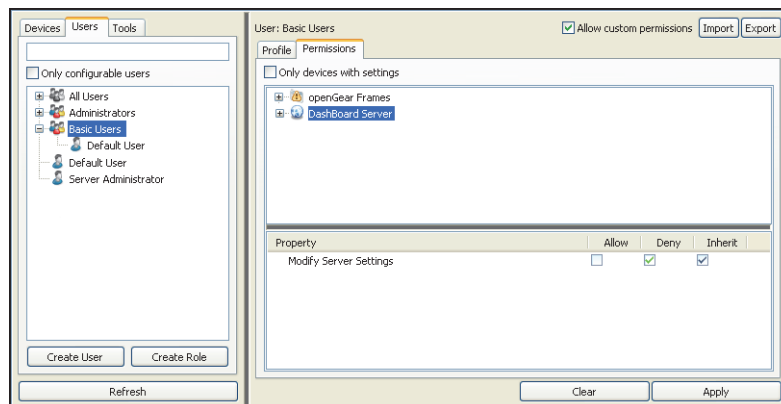
This section outlines how to configure the Basic User role and assumes that you want to limit the permissions granted to this role as compared to the Administrators role. For example, you may only want Administrators to change server settings while denying Basic Users all access to server settings.



Note — *The Default User is automatically assigned to the Basic Users role.*

To display the Editor area for the Basic Users role:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Select the **Allow custom permissions** check box.
3. Select the **Basic Users** node.
4. Select the **Profile** tab to activate the role, and assign users to the role. By default, the Basic Users role is set to Active (the **Active** check box is selected).
5. Select the **Permissions** tab to configure permissions for the role.



Basic Users Role — Permissions Tab

To configure all permissions for the DashBoard Server:

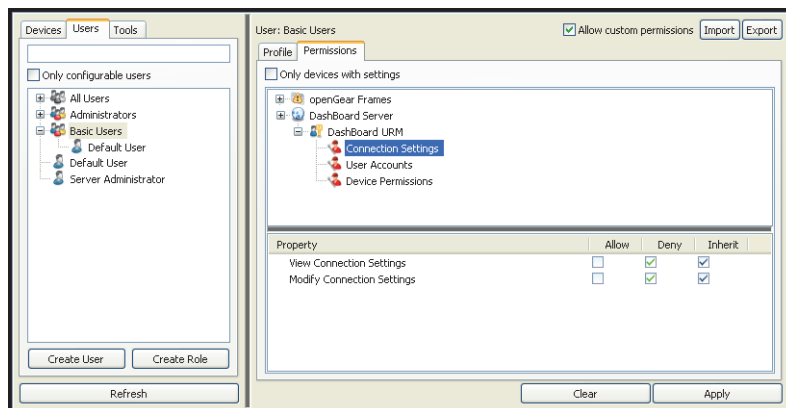
1. Select the **Permissions** tab.
2. Select **DashBoard Server**. The **Property Editor** updates with a list of options available for the DashBoard Server. Note that you are now configuring all the server options including all the DashBoard URM options for the Basic Users role.
3. Select Allow, Deny, or Inherit for each property listed in the **Property Editor**. Refer to step 3. in the section “**To configure permissions for the DashBoard Server:**” on page 4-4 for property descriptions.
4. Click **Apply** to save your changes.

To configure permissions for the DashBoard URM:

1. Select the **Permissions** tab in the **Configure User Rights** dialog.
2. Expand the **DashBoard Server** node.
3. Select the **DashBoard URM** node. The **Property Editor** updates with a list of options available for the DashBoard URM. Note that you are configuring all the DashBoard URM options for the Basic Users role.
4. Select Allow, Deny, or Inherit for each property listed in the **Property Editor**. Refer to step 4. in the section “**To configure permissions for the DashBoard URM:**” on page 4-5.
5. Click **Apply** to save your changes.

To configure permissions for an element of the DashBoard URM:

1. Select the **Permissions** tab in the **Configure User Rights** dialog.
2. Expand the **DashBoard Server** node.
3. Expand the **DashBoard URM** node.
4. Select the element you wish to configure permissions for. The **Property Editor** updates with a list of options available for the selected element.



Basic Users Role — DashBoard URM Element

5. Select Allow, Deny, or Inherit for each property listed in the **Property Editor**. Refer to step 5. to step 7. in the section “**To configure permissions for the DashBoard URM:**” on page 4-5.
6. Click **Apply** to save your changes.

For more information on configuring permissions for devices, refer to the section “**Device Management Overview**” on page 5-1.

Creating a New Role

A role is a group of users that share the same permissions to perform tasks in the DashBoard Server and URM. The permissions and tasks that define a role can be as general or as specific as required. User accounts can belong to any number of roles, with each role defining specific tasks and permissions that may overlap.

You can define permissions for a role based on any combination of the following:

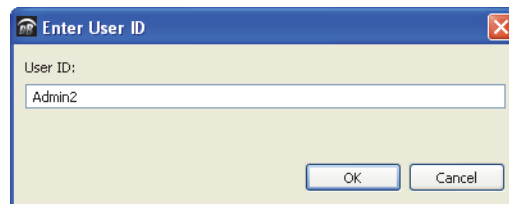
- a single device type, menu, and/or parameter or a combination of these
- multiple device types, menus, and/or parameters
- all openGear devices as a whole
- one or more, or all, the elements of the DashBoard URM
- one or more, or all, the elements of the DashBoard Server

This section provides a general overview of how to create and configure a new role in the DashBoard Server and URM.

For information on configuring permissions for devices, refer to the section “**Device Management Overview**” on page 5-1.

To create a new role:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. If you have a license that limits the number of users for your DashBoard Server, ensure the **Allow custom permissions** check box is selected.
3. Click **Create Role** to display the **Enter ID** dialog.



Enter ID Dialog

4. Type a valid, and unique, name in the **Role ID** field. The name must be between 5-25 characters in length.
5. Click **OK**. The **Editor** area displays the configuration options for the new role. The **Profile** tab is automatically selected.
6. You must add at least one user to the role as follows:
 - Click **Add User** to display the **Add Users** dialog.
 - From the provided list, select a user.
 - Click **Add**.
7. Click **Apply** to save the new role. If you change menus, accounts, or roles, you will be prompted to save the new role.

To configure permissions for the DashBoard Server:

1. Select the **Permissions** tab in the **Configure User Rights** dialog.
2. Expand the **DashBoard Server** node.
3. Select the **DashBoard Server** node. The **Property Editor** updates with a list of options available for the DashBoard Server. Note that you are configuring all the server options including all the DashBoard URM options for the new role.

4. Select Allow, Deny, or Inherit for each property listed in the **Property Editor**. Refer to step 2. in the section “**To configure permissions for the DashBoard Server:**” on page 4-4.
5. Click **Apply** to save your changes.

To configure permissions for the DashBoard URM:

1. Select the **Permissions** tab in the **Configure User Rights** dialog.
2. Expand the **DashBoard Server** node.
3. Select the **DashBoard URM** node. The **Property Editor** updates with a list of options available for the DashBoard URM. Note that you are configuring all the DashBoard URM options.
4. Select Allow, Deny, or Inherit for each property listed in the **Property Editor**. Refer to step 4. in the section “**To configure permissions for the DashBoard URM:**” on page 4-5.
5. Click **Apply** to save your changes.

To configure permissions for an element of the DashBoard URM:

1. Select the **Permissions** tab in the **Configure User Rights** dialog.
2. Expand the **DashBoard Server** node.
3. Expand the **DashBoard URM** node.
4. Select the DashBoard URM element you wish to configure permissions for. The **Property Editor** updates with a list of options available for the selected element.
5. Select Allow, Deny, or Inherit for each property listed in the **Property Editor**. Refer to step 5. to step 7. in the section “**To configure permissions for the DashBoard URM:**” on page 4-5.
6. Click **Apply** to save your changes.

To configure permissions for all openGear devices:

Refer to the section “**Configuring Permissions for openGear Devices**” on page 5-3 for details.

To configure permissions for a specific openGear device:

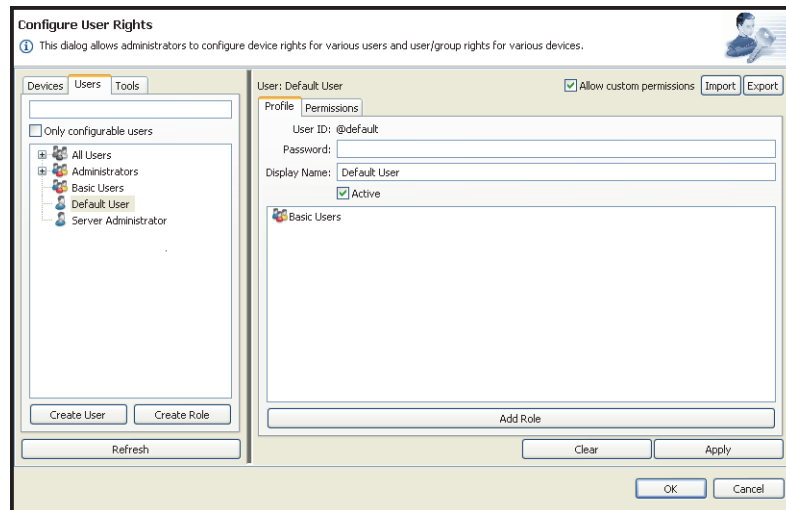
Refer to the section “**Configuring Permissions for a Device**” on page 5-4 or the section “**To configure permissions for a specific menu of a device:**” on page 5-5 for details.

Configuring the Default User Account

The Default User account can be modified to include as many, or as little, permissions as you require. This account is available regardless if you are using an embedded LDAP or an external LDAP Server. Notice that the Default User account is automatically assigned to the Basic Users role and updating the role will also change the permissions for the Default User account until the account is no longer assigned to that role. For example, if you are configuring an open application, the Default User permissions include modifying settings for the Server, URM, and/or devices.

To display the Editor for the Default User account:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Select the **Allow custom permissions** check box.
3. Expand the **All Users** node.
4. Select **Default User** to display the profile and permission options for this user account.



Configure User Rights Dialog — Default User Account Details

To configure the Default User account profile:

1. Select the **Profile** tab.
2. To modify the password, type a new password in the **Password** field.
3. To modify the name displayed in the **Current User** field of the DashBoard client, type the new name in the **Display Name** field. This is the name that displays in the Current User field and Basic Tree View of the DashBoard client, and in the menus of the Configure User Rights dialogs.
4. Click **Apply** to save your changes.

To configure specific permissions for the user account:

1. Select the **Permissions** tab.
2. To modify permissions for the DashBoard Server, refer to the section “**To configure permissions for the DashBoard Server:**” on page 4-4.
3. To modify permissions for the DashBoard URM, refer to the section “**To configure permissions for the DashBoard URM:**” on page 4-5.
4. To modify permissions for an element in the DashBoard URM, refer to the section “**To configure permissions for an element of the DashBoard URM:**” on page 4-7.
5. To modify permissions for a device, refer to the following sections:
 - “**Configuring Permissions for openGear Devices**” on page 5-3
 - “**Configuring Permissions for a Device**” on page 5-4
 - “**To configure permissions for a specific menu of a device:**” on page 5-5

Creating a New User Account

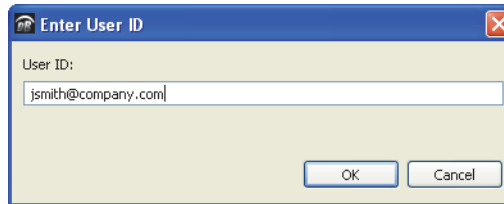
The DashBoard Server and URM enables you to create accounts that can be used by specific users. Each account User ID will requires the e-mail address of that user.



Operating Tip — You may wish to verify the number of configurable users your license allows before creating new accounts. This information is displayed in the *Configure DashBoard URM* or *Configure DashBoard Server* tabs.

To create a new user account:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Click **Create User** to display the **Enter User ID** dialog.



Enter User ID Dialog

3. Type a valid, and unique, e-mail address in the **User ID** field.
4. Click **OK**.
5. Type a password in the **Password** field. This is the password the user will be prompted for when logging into the DashBoard client.
6. Click **OK**.
7. Select the **Allow custom permissions** check box in the **Configure User Rights** dialog.
8. Select the **Profile** tab.
9. To modify the name displayed in the **Current User** field of the DashBoard client:
 - Type the new name in the **Display Name** field.
 - Click **OK**.
10. To activate the new account, select the **Active** check box. Clearing the check box disables the user account.
11. To assign the user account to a role:
 - Click **Add Role**. The **Add User** dialog displays.
 - Select the role(s) you wish to assign to the new user account.
 - Click **Add**.
12. Click **Apply** to save your changes. The new user account displays under the **All Users** node and under any role nodes that the user was assigned to.

To configure specific permissions for the user account:

1. Select the **Permissions** tab.



Operating Tip — *The Configure User Rights dialog displays an error message when you select a user account that is non-configurable (the user icon is grayed out).*

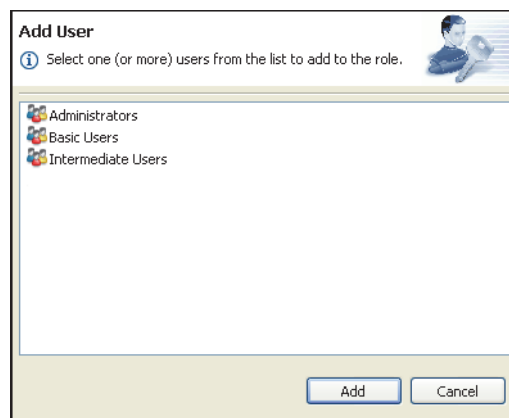
2. To modify permissions for the DashBoard Server, refer to the section “**To configure permissions for the DashBoard Server:**” on page 4-4.
3. To modify permissions for the DashBoard URM, refer to the section “**To configure permissions for the DashBoard URM:**” on page 4-5.
4. To modify permissions for an element in the DashBoard URM, refer to the section “**To configure permissions for an element of the DashBoard URM:**” on page 4-7.
5. To modify permissions for a device, refer to the following sections:
 - “**Configuring Permissions for openGear Devices**” on page 5-3
 - “**Configuring Permissions for a Device**” on page 5-4
 - “**To configure permissions for a specific menu of a device:**” on page 5-5

Assigning Users to Roles

Once you have created your user accounts, and configure the roles in the DashBoard Server and URM, you can assign users to any number of roles. If any role that a user is a member gives that user the permissions to perform a task. Conversely, if the role disallows performing a task, that user can no longer perform that same task even if their user account permissions are set otherwise.

To assign a single user to a role:

1. Display the **Editor** for the user account you wish to assign to a role as follows:
 - Select the **Users** tab in the **Configure User Rights** dialog.
 - Expand the **All Users** node.
 - Select the user account you wish to configure. The **Profile** tab updates to display the information for the selected user account.
2. Click **Add Role** to display the **Add User** dialog.



Add User Dialog

3. Select the role(s) you want to assign to the selected user.
4. Click **Add**.
5. Click **Apply** to apply your changes to the user account.

To assign multiple users to a role:

1. Display the **Editor** for the role you wish to assign:
 - Select the **Users** tab in the **Configure User Rights** dialog.
 - Select the role node you wish to assign. The **Profile** tab updates to display the information for the selected role. Notice that the users already assigned to this role are listed.
2. Click **Add User** to display the **Add User** dialog.
3. Select the user accounts you want to assign to the selected role.
4. Click **Add**.
5. Click **Apply** to apply your changes to the role.

Managing Permissions

This section provides additional information for managing user accounts and role permissions.

Login Settings

You can specify login settings for each DashBoard client in your facility such as timeout times, default data source that users log in to, and what log in data the client retains.

To configure the login settings for a DashBoard client:

1. Launch the DashBoard client.
2. From the DashBoard client main toolbar, select **Window > Preferences**.
3. Select **Login Settings**.
4. To specify what login data the DashBoard client retains automatically:
 - **Remember nothing** — Select this option to have the DashBoard client not retain any log in data from the last account that signed into the client.
 - **Remember last user ID** — Select this option to have the DashBoard client recall the last user account ID only. The **User ID** field of the **Login to DashBoard** dialog is automatically populated with the last user account ID logged into the client. However, the user will still need to enter their password. This is the default.
 - **Sign me in automatically** — Select this option to have the DashBoard client automatically sign in the account currently logged in to the client. This option is only available when running Microsoft® Windows® or Apple Mac® OS X.
5. If you have more than one DashBoard Server and URM running in your facility, specify a server for the DashBoard client to access by selecting it from the **Data Source** field.
6. To set the amount of time that must lapse before a user account is automatically logged out of the DashBoard client:
 - Click the **Timeout** menu to expand the list.
 - Select a time frame from the list. Selecting **Unlimited** enables a user account to remain logged into the DashBoard client for an indefinite period of time. The default is 20 minutes.



Operating Tip — The **Current User** field in the DashBoard client displays a green background. This background represents the amount of time left before the user is automatically logged out. If the timeout value is set to **Unlimited**, the **Current User** field does not display a green background.

7. Click **Apply** to save your changes. Clicking **Restore Defaults** returns all values in Login Settings menu to reset to the factory default values.
8. Click **OK** to exit the dialog.

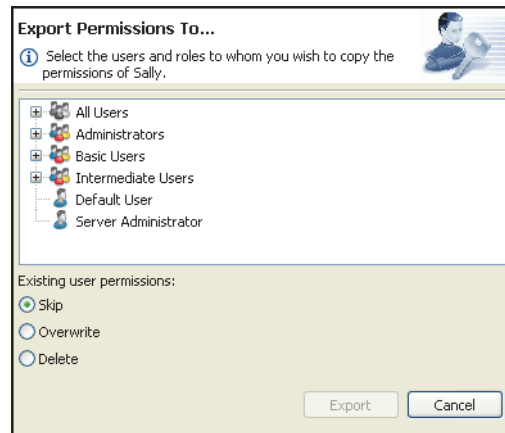
Copying Permissions

Permissions can be copied from a user account or role to another account or role. For example, you can copy permissions from one user account to another user account or to a role. Keep in mind that if any role that a user is a member of has the permissions to perform a task, that user also has the permissions to perform that task.

- **Export** button — Clicking this button displays a dialog that enables you to select the users and roles to copy the permissions *from* the selected role or user. For example, you wish to update Role A to have the same rights as Role B. You would then select Role A, click **Export**, and select the Role B from the provided list.
- **Import** button — Clicking this button displays a dialog that enables you to select the users and roles to copy the permissions *to* the selected role or user. For example, you wish to grant User 1 with the same rights as User 2. You would then select User 2, click **Import**, and select User 1 from the provided list.

To export permissions from an account:

1. Display the **User** tab in the **Configure User Rights** dialog.
2. Select the user account that you want to export permissions from.
3. Click **Export** to display the **Export Permissions** dialog.

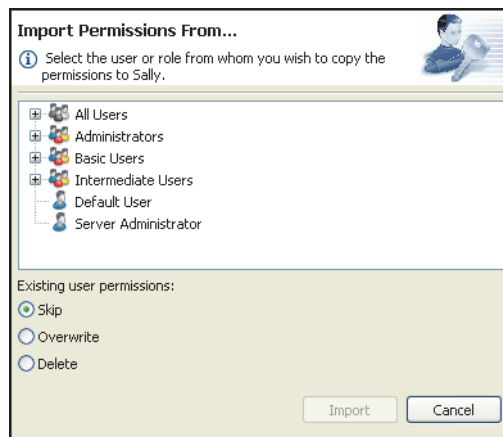


Export Permission Dialog

4. Select the user account you want to update. The settings from this account will change to match the settings from the account you selected in step 2.
5. If there are existing permissions for that account, select one of the following options from the **Existing user permissions list**:
 - **Skip** — Select this option to have the DashBoard URM to ignore any existing settings. These settings will not be modified. This is the default.
 - **Overwrite** — Select this option to have the DashBoard URM update the existing settings with the new settings.
 - **Delete** — Select this option to delete all existing settings for the user account and copy the new permissions.
6. Click **Copy**. The **Permissions Copied** dialog displays once the parameters are copied.
7. Click **OK** to exit the dialog.
8. Click **Apply** to save your settings.

To import permissions to an account:

1. Display the **User** tab in the **Configure User Rights** dialog.
2. Select the user account that you want to import permissions to.
3. Click **Import** to display the **Import Permissions** dialog.



Import Permissions Dialog

4. Select the destination account you want to update. The settings from this account are applied to the account you selected in step 2.
5. If there are existing permissions for that user, select one of the following options from the **Existing user permissions list**:
 - **Skip** — Select this option to have the DashBoard URM to ignore any existing settings. These settings will not be modified. This is the default.
 - **Overwrite** — Select this option to have the DashBoard URM update the existing settings with the new settings.
 - **Delete** — Select this option to delete all existing settings for the user account and copy the new permissions.
6. Click **Copy**. The **Permissions Copied** dialog displays once the parameters are copied.
7. Click **OK** to exit the dialog.
8. Click **Apply** to save your settings.

Deleting User Roles and Accounts

You can delete a user account or role from the DashBoard Server and URM. Note that deleting a role that a user is assigned to removes the associate permissions for that role; permissions revert back to the user account settings. Note that deleting a role does not delete the users assigned to that role.

To delete a role:

1. Display the **User** tab in the **Configure User Rights** dialog.
2. Right-click the role you wish to delete permissions for.
3. Select **Delete role** to delete the role from the DashBoard Server and URM. Any users assigned to that role no longer have the permissions that were defined by that role.

To delete a user account:

1. Display the **User** tab in the **Configure User Rights** dialog.
2. Right-click the user account you wish to delete permissions for.
3. Select **Delete user account** to delete the user account from the DashBoard Server and URM. Any roles or devices that the user was assigned to no longer recognize this account. The account can no longer log in to the DashBoard client.

Disabling User Roles and Accounts

Disabling roles and accounts is used when your DashBoard Server is non-compliant with the number of accounts as determined by your license key. A user or role that is disabled still displays in the tree view of the **Configure User Rights** dialog, but with a grayed out icon.



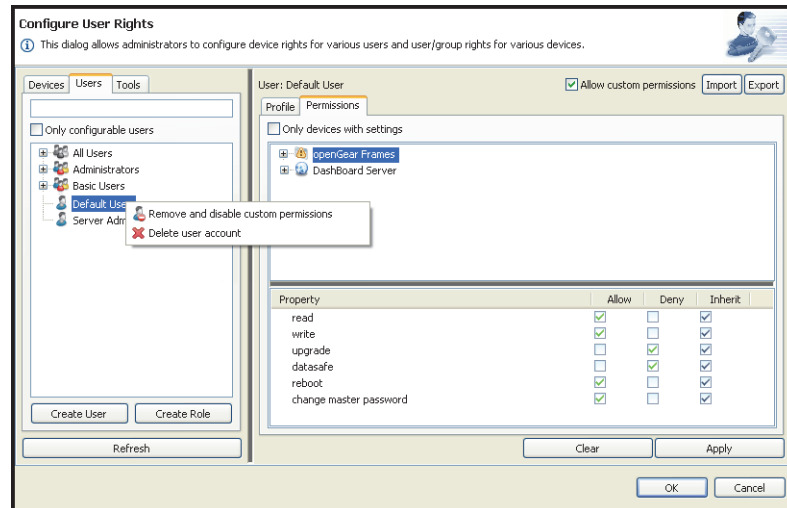
Operating Tip — To enable an account or role, right-click the applicable icon in the **Users** tab and select **Allow custom permissions**.

To disable a role:

1. Display the **User** tab in the **Configure User Rights** dialog.
2. Right-click the role you wish to disable permissions for.
3. Select **Remove and disable custom permissions** to remove the user account from the DashBoard Server and URM.

To disable a user account:

1. Display the **User** tab in the **Configure User Rights** dialog.
2. Right-click the user account you wish to disable permissions for.



Disable Custom Permissions — User Account

3. Select **Remove and disable custom permissions** to remove all permissions for the user and set the account to non-configurable.

To re-enable a user account:

1. Display the **User** tab in the **Configure User Rights** dialog.
2. Right-click the user account you wish to enable permissions for.
3. Select **Enable custom permissions** to re-establish permissions for the user and set the account to configurable.

Changing Passwords for Accounts

If the Modify Users property is set to Allow for a role, users assigned to that role can change the password for any user account in the DashBoard Server and URM. For information on changing the password for your MFC-8300 series Network Controller card, refer to the **MFC-8300 Series User Guide** for details.



Operating Tip — Users can change their passwords using the options in the **Login** dialog of the DashBoard client.

To change the password for a user account:

1. Log into the DashBoard Server and URM using an account that is able to modify user accounts.
2. Display the **Users** tab in the **Configure User Rights** dialog.
3. Expand the **All Users** node.
4. Select the user account you wish to change the password for. The **Editor** area and the **Property Editor** display the account information.
5. Select the **Profile** tab.
6. Type a new password into the **Password:** field.
7. Click **Apply** to save your changes.
8. Notify the user whose account you updated. The DashBoard Server and URM does not automatically notify users when their information has changed.

Managing Devices

In This Chapter

This chapter provides an overview of the options available for managing device permissions in the DashBoard Server and URM. Permissions management for your devices can be as specific, or as general, as required by your facility. This chapter assumes you are configuring openGear devices, such as frames and cards. However, the general principles are the same for other types of devices. For specific information on configuring other device types not presented here, refer to the documentation that came with your device.

The following procedures assume that the DashBoard Server and URM display names are set to the default values.

The following topics are discussed:

- Device Management Overview
- Updating the List of Devices
- Configuring Permissions for openGear Devices
- Configuring Permissions for a Device
- To configure permissions for a specific menu of a device:
- Managing Device Permissions

Device Management Overview

You can further define permissions for users by defining permissions for devices that display in the DashBoard client. Permissions for devices can be as specific as required. For example, a user has denied write permission access to the network settings for an openGear card, but has write access to all other menus and parameters for that card.

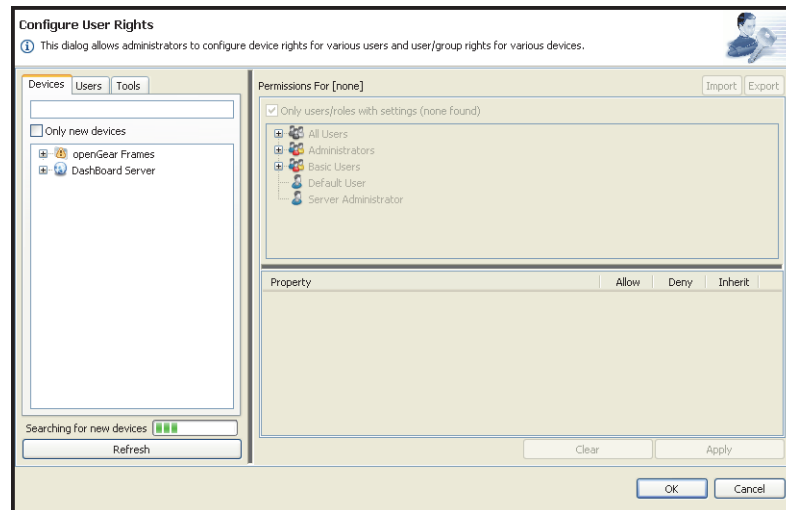
- Selecting **Deny** for a property denies access to that parameter or device. For example, a user may have read and write permissions for all devices except for the MDK-111A-M card in a specific frame.
- Selecting **Allow** for a property enables access to that parameter or device.
- Selecting **Inherit** for a property sets the permissions for the device as specified by the device it is sub-ordinate to.

You can configure permissions using the **Devices** tab options in the **Configure User Rights** dialog.

To display the **Devices** tab in the **Configure User Rights** dialog:

1. Launch the DashBoard client by double-clicking the DashBoard icon on your desktop.
2. Enter your account ID and password in the **Login to the DashBoard** dialog. The account you are using must be configured as an Administrator.
3. In the DashBoard client, expand the **DashBoard Server** node in the Basic Tree View.
4. Expand the **DashBoard URM** node.

5. Select the **Devices** node. The **Configure User Rights** dialog displays with the **Devices** tab automatically selected.
 - Each time you launch the **Configure User Rights** dialog, a **Searching for new devices** progress bar displays directly above the **Refresh** button. This progress bar indicates that the DashBoard Server and URM is searching for device information that is not currently stored in the DashBoard Server.



Configure User Rights — Searching for new devices Progress Bar

- Devices and menus that have neither had permissions set nor confirmed to be “wide open” are displayed in the **Devices** tab tree view with an asterisk.

Updating the List of Devices

The **Devices** tab lists the devices available to the DashBoard Server and is similar to the list in the Basic Tree View of the DashBoard client. You can also specify that the tab only lists new devices (devices that have not had their information uploaded to your DashBoard Server yet). This is especially useful for maintenance once you have configured devices and only add devices infrequently, allowing you to list only those new devices that do not have permissions set.

Updating the Device List

Before configuring device permissions, you should ensure that the information displayed in the **Devices** tab is current and complete. You can achieve this by refreshing the device list and then uploading information for any new devices. This section outlines how to update the list of devices in the **Devices** tab.

To list only new devices in the **Devices** tab:

1. Display the **Devices** tab in the **Configure User Rights** dialog.
2. Select the **Only new devices** check box in the **Devices** tab.

To refresh the list of devices:



1. Display the **Devices** tab in the **Configure User Rights** dialog.
2. Click **Refresh**.

Updating Device Information

You can update information for a specific device, such as a specific openGear card, or for a series of devices, such as an openGear frame and all the cards installed in it. An easy way to determine if information for a device is

uploaded is the presence of the warning icon beside the item in the tree view. An asterisk (*) signifies that information has not been uploaded for that device.

To upload device information:

1. Display the **Devices** tab in the **Configure User Rights** dialog.
2. If you select the **Only new devices** check box, the tree view in the **Devices** tab displays only those devices which information has not be uploaded for yet.
3. Expand the nodes in the tree view to navigate to the device you wish to upload information for. For example, to upload information for an MDK-111A-M card, expand the openGear Frames node, expand the node for the frame the card is installed in, then select the node for the actual card.
4. Right-click the device you want to upload information for.
5. Select one of the following:
 -  **Acknowledge Device** — Select this option to upload information for the selected device only. For example, if you have selected an openGear card, it will upload information for the card only. Information on the menus and their settings will be not uploaded to the DashBoard Server. You will notice that an asterisk (*) is displayed beside each item not uploaded.
 -  **Acknowledge Device (and children)** — Select this option to upload information for the selected devices and any devices, menus, or parameters listed beneath it. For example, if you selected this option for an openGear frame, information for the frame, all the installed cards, and their associated menus is uploaded to the DashBoard Server.
6. A progress dialog displays while the information is uploaded to your DashBoard Server. The dialog closes when the upload process is complete.

Configuring Permissions for openGear Devices

This section outlines how to configure permissions for devices listed under the openGear node in the Devices tab of the Configure User Rights dialog. The procedure for configuring permissions for a role or user is the same as outlined below.

To configure permissions for all openGear devices:

1. Display the **Devices** tab in the **Configure User Rights** dialog.
2. Double-click the **openGear Frames** node in the **Devices** tab.
3. If the **Only users/roles with settings** check box is selected, the **Permissions For** area displays a tree view of users and roles with permissions already set. Clearing the check box lists all users and roles configured in the DashBoard URM.
4. From the tree view in the **Permissions For** area, select the user(s) and/or role(s) you wish to configure permissions for all openGear devices. The Property Editor window now displays the available permissions to configure.

5. From the **Property Editor**, select Allow, Deny, or Inherit for each property listed:
 - **read** — Specifies if the role/user can view the openGear devices communicating with the DashBoard Server.
 - **write** — Specifies if the role/user can modify parameters of the openGear devices communicating with the DashBoard Server.
 - **upgrade** — Specifies if the role/user can perform software upgrades for the openGear devices communicating with the DashBoard Server.
 - **datasafe** — Specifies if the role/user can access the following DataSafe™ features of all the openGear devices communicating with the DashBoard Server: **Restore configuration from file**, and **Restore configuration from another card**.
 - **reboot** — Specifies if the role/user can re-start all the openGear devices communicating with the DashBoard Server.
 - **change master password** — Specifies if the role/user can change the master password for the frames communicating with the DashBoard Server and listed under the **openGear Frames** node.
6. Click **Apply** to save your settings.


Configuring Permissions for a Device

A device is defined as an object whose parameters are accessed by expanding at least one node in the **Devices** tab of the **Configure User Rights** dialog. An example of a device is an openGear frame, such as the DFR-8321-N, or an openGear card such as the MDK-111A-M. Depending on how you wish to configure your devices, you can set permissions for a user in one of the following manners:

- inherit permissions from the hierarchy of device(s)
- inherit permissions from the role(s) the user is a member of
- permissions set on a per device type basis (e.g. all openGear MDK-111A-M cards)


This section outlines how to configure permissions for devices listed under the openGear node in the Devices tab of the Configure User Rights dialog, including permissions for specific menu items. Your specific devices, the menus and permissions, may differ from what is presented here. For information on configuring the password for your MFC-8300 series Network Controller card, refer to the ***MFC-8300 Series User Manual***. For information on the specific menus available for your device, refer to the ***User Guide*** that came with your device.

To configure permissions for a device:

1. Display the **Devices** tab in the **Configure User Rights** dialog.
2. Expand the openGear Frames node in the **Devices** tab.
3. If the device includes an asterisk (*) beside its icon, you may want update the information for that device as follows:
 - Right-click the parent device node.
 - Select  **Acknowledge Device (and children)** to update the device information for the parent device and any associated child devices and menus.
 - The icon for the device changes to no longer include an asterisk (*).
4. Select the node for the parent device you wish to configure. The **Property Editor** is updated to include a list of available users and roles. The **Property Editor** is now disabled, but displays the available permissions to configure.
5. From the **Permissions For** window, select the user(s) and/or role(s) you wish to configure permissions for. The **Property Editor** is now enabled.

6. From the **Property Editor**, select Allow, Deny, or Inherit for each property listed. Note that selecting Inherit specifies that permissions for this device will be inherited from the openGear settings, and/or the role/account settings.
 - **read** — Specifies if the role/user can only view the parent device communicating with the DashBoard Server.
 - **write** — Specifies if the role/user can modify parameters of the parent device communicating with the DashBoard Server.
 - **upgrade** — Specifies if the role/user can perform software upgrades for the parent device communicating with the DashBoard Server.
 - **datasafe** — Specifies if the role/user can access the DataSafe™ feature of the parent device communicating with the DashBoard Server.
 - **reboot** — Specifies if the role/user can reboot the parent device communicating with the DashBoard Server.
7. Click **Apply** to save your settings.

To configure permissions for a specific menu of a device:

1. Display the **Devices** tab in the **Configure User Rights** dialog.
2. Expand the openGear Frames node in the **Devices** tab.
3. Navigate to the device you wish to set permissions for.
4. If the child device includes an asterisk (*) beside its icon, you may want to update the information for that device as follows:
 - Right-click the parent device node.
 - Select  **Acknowledge Device (and children)** to update the device information for the parent device and any associated child devices and menus.
 - The icon for the device changes to no longer include an asterisk (*).
5. Expand the device node you wish to configure a menu for. A list of menus is displayed beneath the selected node. Each entry represents a menu that displays in the DashBoard client. This list varies depending on the device you selected. Expanding the node for a menu lists the available options in that menu.
6. Select the node for the menu or menu item you wish to configure. The **Property Editor** is updated to include a list of available users and roles. The **Property Editor** is now disabled, but displays the available permissions to configure.
7. From the **Permissions For** area, select the user(s) and/or role(s) you wish to configure permissions for. The **Property Editor** is now enabled.
8. From the **Property Editor**, select Allow, Deny, or Inherit for each property listed. Note that selecting Inherit specifies that permissions for this device will be inherited from the parent device settings.
 - **read** — This property specifies whether the user/role can view the information in the menu.
 - **write** — This property specifies whether the user/role can modify the menu parameters.
9. Click **Apply** to save your settings.

Managing Device Permissions

This section provides additional information on copying and deleting permissions for your devices.

Copying Permissions

Permissions can be copied from a device to another compatible device. For example, you can copy permissions from one MDK-111A-M card to another MDK-111A-M card but not to a FSR-6601 card. The individual card

settings are not copied, just the permissions. To copy the card settings, you must use the DataSafe™ feature of your MFC-8300 series Network Controller card.

To export permissions from a device:

Refer to the section “**To export permissions from an account:**” on page 4-14 for details.



To import permissions to a device:

Refer to the section “**To import permissions to an account:**” on page 4-14 for details.



Deleting Permissions

You can delete permissions for a menu, a child device, a parent device, or a combination. You can also delete permissions for all openGear devices available in the DashBoard Server. This section outlines how to delete permissions for all openGear devices, for individual devices, or a series of related devices.

To delete permissions for all openGear devices:

1. Display the **Devices** tab in the **Configure User Rights** dialog.
2. Right-click the openGear node in the **Devices** tab.
3. Select one of the following:
 -  **Remove Settings** — Select this option to delete permissions for the openGear node only. Permissions for individual devices listed under the openGear node are not affected.
 -  **Remove Settings (including children)** — Select this option to delete permissions for all devices listed under the openGear node.

To delete permissions for a specific device:

1. Display the **Devices** tab in the **Configure User Rights** dialog.
2. Expand the openGear node in the **Devices** tab.
3. Navigate to the device you wish to delete permissions for.
4. Select one of the following:
 -  **Remove Settings** — Select this option to delete permissions for the selected parent device only. Permissions for child devices listed under the parent device node are not affected.
 -  **Remove Settings (including children)** — Select this option to delete permissions for all devices listed under the selected parent device.

Maintenance

In This Chapter

This chapter provides a general overview of the **Tools** tab in the **Configure User Rights** dialog. From this tab you can monitor the inactive devices, and update their settings.

The following topics are discussed:

- Managing Inactive Devices
- Reviewing User Permissions

Managing Inactive Devices

Inactive devices are objects with information previously stored in the DashBoard Server and URM but are not displayed in the Tree View of the current user's DashBoard client. The Tools tab in the Configure User Rights dialog displays a view of permissions that have already been established on the DashBoard Server for inactive devices. Information from the DashBoard Server and URM for devices not currently detected in the DashBoard client is also displayed.

To display the Tools Tab:

1. Launch the DashBoard client by double-clicking the DashBoard icon on your desktop.
2. Enter your account ID and password in the **Login to the DashBoard** dialog. The account you are using must be configured as an Administrator.
3. In the DashBoard client, expand the **DashBoard Server** node in the Basic Tree View.
4. Expand the **DashBoard URM** node.
5. Double-click the **Tools** node. The **Configure User Rights** dialog displays with the **Tools** tab automatically selected.



Deleting Inactive Devices

You can delete inactive devices from the DashBoard Server and URM. This action deletes all device information, including any configured permissions, for the selected device from the database. You will not be able to retrieve, or undo, the deleted data. Note that this action does not delete objects from the tree view in the DashBoard client. This action just deletes information from the DashBoard Server database.



To delete all information for openGear devices:

1. Display the **Tools** tab in the **Configure User Rights** dialog.
2. Right-click the openGear node in the **Tools** tab.



3. Select one of the following:

-  **Remove settings** — Select this option to delete all the saved permissions and device information for the openGear node only. The devices listed under the openGear node are not affected.
-  **Remove settings (including children)** — Select this option to delete all the permissions and device information for all inactive devices listed under the openGear node. Settings and permissions for all the devices are removed from the database.

To delete permissions for a parent device:

1. Display the **Tools** tab in the **Configure User Rights** dialog.
2. Expand the openGear node in the **Tools** tab.
3. Right-click the inactive parent device you wish to delete permissions for.
4. Select one of the following:
 -  **Remove settings** — Select this option to delete permissions and device information for the selected parent device only. Devices listed under the parent device node are not affected.
 -  **Remove settings (including children)** — Select this option to delete permissions and device information for all devices listed under the selected parent device.

To delete permissions for a child device:

1. Display the **Tools** tab in the **Configure User Rights** dialog.
2. Expand the openGear node in the **Tools** tab.
3. Expand the parent device node the child device is located under.
4. Right-click the child device node you wish to delete permissions for.
5. Select one of the following:
 -  **Remove Settings** — Select this option to delete permissions for the selected child device only. Permissions for menus and options listed under the child device node are not affected.
 -  **Remove Settings (including children)** — Select this option to delete permissions for the selected child device and all menus and options listed under that child device.

Copying Permissions for Inactive Devices

Permissions can be copied from an inactive device to any other compatible device or vice versa. The compatible device can be active or not, but must be the same type. For example, you can copy permissions from an inactive MDK-111A-M to an active MDK-111A-M, but not to an FSR-6601.

To export permissions from a device:

1. Display the **Tools** tab in the **Configure User Rights** dialog.
2. Expand the openGear node in the **Tools** tab.
3. Select the node for the device you want to export permissions from. The **Permissions For** and **Property Editor** are updated.
4. Click **Export** to display the **Export Permissions** dialog.
5. Select the source device you want to update. The settings from this device will change to match the settings from the device you selected in step 3.
6. If you do not wish to copy permissions for any child devices, such as card settings, clear the **Also copy/replace permissions for all child objects** checkbox. This box is selected by default.

7. Click **Copy**. The **Permissions Copied** dialog displays once the parameters are copied.
8. Click **OK** to exit the dialog.
9. Click **Apply** to save your settings.

To import permissions to a device:

1. Display the **Tools** tab in the **Configure User Rights** dialog.
2. Expand the openGear node in the **Tools** tab.
3. Select the node for the device you want to import to. The **Permissions For** and **Property Editor** are updated.
4. Click **Import** to display the **Import Permissions** dialog.
5. Select the destination device you want to update. The settings from this device are applied to the device you selected in step 3.
6. If you do not wish to copy permissions for any child devices, such as card settings, clear the **Also copy/replace permissions for all child objects** checkbox. This box is selected by default.
7. Click **Copy**. The **Permissions Copied** dialog displays once the parameters are copied.
8. Click **OK** to exit the dialog.
9. Click **Apply** to save your settings.

Adding Users and Roles to an Inactive Device

You can still add users and roles to inactive devices much like active devices as outlined in the chapter “**Managing Devices**” on page 5-1. The settings do not take affect until the inactive device is online and displays in the DashBoard client.

For details on adding users and roles to all openGear devices, refer to the section “**Configuring Permissions for openGear Devices**” on page 5-3. To learn more on adding users and roles to individual devices, refer to the section “**Configuring Permissions for a Device**” on page 5-4 and the section “**To configure permissions for a specific menu of a device:**” on page 5-5.

Reviewing User Permissions

You can also review the roles and accounts currently active in the DashBoard Server from the **Tools** tab. This tab provides you with an overview of which roles and users have permissions set for the DashBoard Server, and the specific settings of any roles that have permissions set for the DashBoard URM.

This section provides a general summary on reviewing the roles and accounts of your DashBoard Server and URM.

To review permissions for the DashBoard Server:

1. Display the **Tools** tab in the **Configure User Rights** dialog.
2. Select DashBoard Server. The **Permissions For** area updates to list all the roles currently assigned permissions for the DashBoard Server.
3. Select a role from the **Permissions For** area. The **Property Editor** updates to list the permissions and configured settings for this role that affect the DashBoard Server.
4. Configure permissions as required. Refer to the section “**To configure permissions for the DashBoard Server:**” on page 4-4 for details on the available options.
5. Repeat step 3. and step 4. for each role you wish to monitor.
6. Click **Apply** to save your changes.

To review permissions for the DashBoard URM:

1. Display the **Tools** tab in the **Configure User Rights** dialog.
2. Select **User permissions Administration**. The **Permissions For** area updates to list all the roles currently assigned permissions for the DashBoard URM.
3. Select a role from the **Permissions For** area. The **Property Editor** updates to list the permissions and configured settings for this role that affect the DashBoard URM.
4. Configure permissions as required. Refer to the section “**To configure permissions for the DashBoard URM:**” on page 4-5 for details on the available options.
5. Repeat step 3. and step 4. for each role you wish to monitor.
6. Click **Apply** to save your changes.

Appendix A. Applications

In This Chapter

This appendix provides examples of how to configure permissions for an open application, a closed application, and a custom application. Each section provides an example of an application and includes the necessary steps to configuring that application. The information provided in this appendix are examples only and your facility requirements may differ from what is presented here.

The procedures in this appendix assume that the facility is installing one DFR-8321-N frame that includes two MDK-111A-K cards, one MUX-8258-A card, one DMX-8259-A card, two HDC-8222 cards, and one QSP-8229 card. It is also assumed that the Administrator setting up each application is familiar with the DashBoard Server and URM interfaces.

The following topics are discussed:

- Configuring an Open Application
- Configuring a Closed Application
- Configuring a Custom Application

Configuring an Open Application

This section outlines how to configure an open application with the following users:

- One user (User A) is an Administrator with full access to all devices. This user can also modify the settings for the DashBoard Server and the DashBoard URM.
- Three users (User B, C, and D) have individual accounts. Each user has full access to all devices but not to the DashBoard Server and URM settings.
- The Default User also has full access to all devices, but cannot access the DashBoard Server and URM settings.

To configure the DashBoard URM default permissions:

This procedure sets all the permissions to Allow by default.

1. Navigate to the **Configure DashBoard URM** tab as follows:
 - Right-click the **DashBoard URM** node in the Basic Tree View.
 - Select **Open** to display the tab in the Device View of the DashBoard client.
2. Locate the **Permissions Management** header.
3. Select the **Allow** option for the **Default Policy**.

To configure the Administrator role:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Select the **Administrators** node.
3. Select the **Permissions** tab.

4. Update the list of available devices and parameters.
5. To configure permissions for all openGear devices listed in the DashBoard client:
 - Select the openGear node. The **Property Editor** updates to list the available options.
 - Select **Allow** for each property listed in the **Property Editor**.
 - Click **Apply** to save your changes.
6. To configure permissions for the DashBoard Server:
 - Select the DashBoard Server node. The **Property Editor** updates to list the available options.
 - Select **Allow** for each property listed in the **Property Editor**.
 - Click **Apply**.
7. To configure permissions for the DashBoard URM:
 - Expand the DashBoard Server node.
 - Select the DashBoard URM node. The **Property Editor** updates to list the available options.
 - Select **Allow** for each property listed in the **Property Editor**.
 - Click **Apply**.

To configure the user account for User A:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Click **Create User** to display the **Enter User ID** dialog.
3. Follow the on-screen instructions and enter the E-mail address, password, and a display name for User A. Click **OK** to add the user to the database.
4. Select **User A** from the tree view in the **Users** tab.
5. Select the **Profile** tab.
6. Click **Add Role** to display the **Add User** dialog.
7. Select **Administrators**.
8. Click **OK**. The **Profile** tab updates.
9. Click **Apply** to save your changes.

To configure the Basic Users role:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Select the **Basic Users** node from the tree view in the **Users** tab.
3. Select the **Permissions** tab.
4. Update the list of available devices and parameters.
5. To configure permissions for all openGear devices listed in the DashBoard client:
 - Select the openGear node. The **Property Editor** updates to list the available options.
 - Select **Allow** for each property listed in the **Property Editor**.
 - Click **Apply** to save your changes.
6. To configure permissions for the DashBoard Server:
 - Select the DashBoard Server node. The **Property Editor** updates to list the available options.
 - Select **Deny** for each property listed in the **Property Editor**.
 - Click **Apply**.

7. To configure permissions for the DashBoard URM:
 - Expand the DashBoard Server node.
 - Select the DashBoard URM node. The **Property Editor** updates to list the available options.
 - Select **Deny** for each property listed in the **Property Editor**.
 - Click **Apply**.

To create additional user accounts:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Create a new user account for User B as follows:
 - Click **Create User** to display the **Enter User ID** dialog.
 - Follow the on-screen instructions and enter the E-mail address, password, and display name for User B.
 - Click **OK** to add the user to the database.
3. Repeat step 2. for User C and User D, entering unique information for each user.
4. Assign Users B, C, and D to the Basic Users role:
 - Select the **Basic Users** node from the **Users** tab.
 - Select the **Profile** tab.
 - Click **Add User** to display the **Add User** dialog.
 - Select **User B**, **User C**, and **User D** from the list.
 - Click **Add**.
5. Click **Apply** to save your changes.

To configure the Default User account:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Select the **Default User** node from the tree view in the **Users** tab.
3. Configure permissions for the Default User as follows:
 - Select the **Profile** tab.
 - Click **Add Role** to display the **Add User** dialog.
 - Select **Basic Users**.
 - Click **OK**. The **Profile** tab updates.
4. Click **Apply** to save your changes.

Configuring a Closed Application

This section outlines how to configure a closed application with the following users:

- One user (User A) is an Administrator with full access to all devices. This user can also modify the settings for the DashBoard Server and the DashBoard URM.
- Two users (User B and User C) have only read-only access to the openGear devices, but cannot access the DashBoard Server and URM settings.
- The Default User has read-only access to all openGear devices, but cannot access the DashBoard Server and URM settings.

To configure the DashBoard URM Default permissions:

This procedure sets all the permissions to Deny by default.

1. Navigate to the **Configure DashBoard URM** tab as follows:
 - Right-click the **DashBoard URM** node in the Basic Tree View.
 - Select **Open** to display the tab in the Device View of the DashBoard client.
2. Locate the **Permissions Management** header.
3. Select the **Deny** option for the **Default Policy**.

To configure the Administrator role:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Select the **Administrators** node.
3. Select the **Permissions** tab.
4. Update the list of available devices and parameters.
5. To configure permissions for all openGear devices listed in the DashBoard client:
 - Select the openGear node. The **Property Editor** updates to list the available options.
 - Select **Allow** for each property listed in the **Property Editor**.
 - Click **Apply** to save your changes.
6. To configure permissions for the DashBoard Server:
 - Select the DashBoard Server node. The **Property Editor** updates to list the available options.
 - Select **Allow** for each property listed in the **Property Editor**.
 - Click **Apply**.
7. To configure permissions for the DashBoard URM:
 - Expand the DashBoard Server node.
 - Select the DashBoard URM node. The **Property Editor** updates to list the available options.
 - Select **Allow** for each property listed in the **Property Editor**.
 - Click **Apply**.

To configure the user account for User A:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Click **Create User** to display the **Enter User ID** dialog.
3. Follow the on-screen instructions and enter the E-mail address, a password, and a display name for User A. Click **OK** to add the user to the database.
4. Select **User A** from the tree view in the **Users** tab.
5. Select the **Profile** tab.
6. Click **Add Role** to display the **Add User** dialog.
7. Select **Administrators**.
8. Click **OK**. The **Profile** tab updates.
9. Click **Apply** to save your changes.

To configure the Basic Users role:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Select the **Basic Users** node from the tree view in the **Users** tab.
3. Select the **Permissions** tab.

4. Update the list of available devices and parameters.
5. To configure permissions for all openGear devices listed in the DashBoard client:
 - Select the openGear node. The **Property Editor** updates to list the available options.
 - Select **Allow** for the **read** property.
 - Select **Deny** for the **datasafe**, **reboot**, **upgrade**, and **write** properties.
 - Click **Apply** to save your changes.
6. To configure permissions for the DashBoard Server:
 - Select the DashBoard Server node. The **Property Editor** updates to list the available options.
 - Select **Deny** for each property listed in the **Property Editor**.
 - Click **Apply**.
7. To configure permissions for the DashBoard URM:
 - Expand the DashBoard Server node.
 - Select the DashBoard URM node. The **Property Editor** updates to list the available options.
 - Select **Deny** for each property listed in the **Property Editor**.
 - Click **Apply**.

To create additional user accounts:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Create a new user account for User B as follows:
 - Click **Create User** to display the **Enter User ID** dialog.
 - Follow the on-screen instructions and enter the E-mail address, password, and display name for User B.
 - Click **OK** to add the user to the database.
3. Repeat step 2. for User C and User D, entering unique information for each.
4. Assign Users B, C, and D to the Basic Users role as follows:
 - Select the **Basic Users** node from the **Users** tab.
 - Select the **Profile** tab.
 - Click **Add User** to display the **Add User** dialog.
 - Select **User B**, **User C**, and **User D** from the list.
 - Click **Add**.
5. Click **Apply** to save your changes.

To configure the Default User account:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Select the **Default User** node from the tree view in the **Users** tab.
3. Configure permissions for the Default User as follows:
 - Select the **Profile** tab.
 - Click **Add Role** to display the **Add User** dialog.
 - Select **Basic Users**.
 - Click **OK**. The **Profile** tab updates.
4. Click **Apply** to save your changes.

Configuring a Custom Application

This section outlines how to configure a custom application with the following users:

- One user (User A) can modify the settings for the DashBoard Server and the DashBoard URM. This user also has full access to all the cards and the frame.
- Two users (User B and User C) are assigned to the Device Admin role which grants full access to all the cards and the frame.
- Two users (User D and User E) are assigned to the Audio Admin role which grants only read and write access to the MUX-8258-A and DMX-8259-A cards.
- Two users (User F and User G) are assigned to the Keyer Admin role which grants read and write access to the MDK-111A-K cards, the HDC-8222 cards, and the QSP-8229 card.
- The Default User is restricted to read-only access to openGear devices.
- All users, except User A, do not have access to the DashBoard Server and URM.

To configure the Administrator role:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Select the **Administrators** node.
3. Select the **Permissions** tab.
4. Update the list of available devices and parameters.
5. To configure permissions for all openGear devices listed in the DashBoard client:
 - Select the openGear node. The **Property Editor** updates to list the available options.
 - Select **Allow** for each property listed in the **Property Editor**.
 - Click **Apply** to save your changes.
6. To configure permissions for the DashBoard Server:
 - Select the DashBoard Server node. The **Property Editor** updates to list the available options.
 - Select **Allow** for each property listed in the **Property Editor**.
 - Click **Apply**.
7. To configure permissions for the DashBoard URM:
 - Expand the DashBoard Server node.
 - Select the DashBoard URM node. The **Property Editor** updates to list the available options.
 - Select **Allow** for each property listed in the **Property Editor**.
 - Click **Apply**.

To configure the user account for User A:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Click **Create User** to display the **Enter User ID** dialog.
3. Follow the on-screen instructions and enter the E-mail address, a password, and a display name for User A. Click **OK** to add the user to the database.
4. Select **User A** from the tree view in the **Users** tab.
5. Select the **Profile** tab.
6. Click **Add Role** to display the **Add User** dialog.
7. Select **Administrators**.
8. Click **OK**. The **Profile** tab updates.

9. Click **Apply** to save your changes.

To create additional user accounts:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Create a new user account for User B as follows:
 - Click **Create User** to display the **Enter User ID** dialog.
 - Follow the on-screen instructions and enter the E-mail address, password, and display name for User B.
 - Click **OK** to add the user to the database.
3. Configure permissions for User B as follows:
 - Select **User B** from the tree view in the **Users** tab.
 - Select the **Profile** tab.
 - Click **Add Role** to display the **Add User** dialog.
 - Select **Basic Users**.
 - Click **OK**. The **Profile** tab updates.
4. Click **Apply** to save your changes.
5. Repeat step 2. to step 5. for each additional user, entering unique information for each.

To configure the Device Admin role:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Click **Create Role**.
3. Enter the required information in the **Enter Role** dialogs.
4. Add users to the Device Admin role as follows:
 - Click **Add Users**.
 - Select **User B** and **User C** from the list.
 - Click **Add**.
5. Select the **Permissions** tab.
6. Select the **Show only devices with settings** radio button to update the list of available devices and parameters.
7. To configure permissions for all openGear devices listed in the DashBoard client:
 - Select the openGear node. The **Property Editor** updates to list the available options.
 - Select **Allow** for each property listed in the **Property Editor**.
 - Click **Apply** to save your changes.
8. To configure permissions for the DashBoard Server:
 - Select the DashBoard Server node. The **Property Editor** updates to list the available options.
 - Select **Allow** for each property listed in the **Property Editor**.
 - Click **Apply**.
9. To configure permissions for the DashBoard URM:
 - Expand the DashBoard Server node.
 - Select the DashBoard URM node. The **Property Editor** updates to list the available options.
 - Select **Allow** for each property listed in the **Property Editor**.
 - Click **Apply**.
10. Click **Apply** to save your changes.

To configure the Audio Admin role:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Click **Create Role**.
3. Enter the required information in the **Enter Role** dialogs.
4. Add users to the Audio Admin role as follows:
 - Click **Add Users**.
 - Select **User D** and **User E** from the list.
 - Click **Add**.
5. Select **Audio Admin** from the tree view in the **Users** tab.
6. Select the **Permissions** tab.
7. Select the **Show only devices with settings** radio button to update the list of available devices and parameters.
8. To configure permissions for the MUX-8258-A card as follows:
 - Expand the openGear node.
 - Expand the DFR-8321-N node.
 - Select the MUX-8258-A card. The **Property Editor** updates to list the available options.
 - Select **Allow** for the **read** and **write** properties.
 - Select **Deny** for the **datasafe**, **reboot**, and **upgrade** properties.
 - Click **Apply** to save your changes.
9. Repeat step 8. for the DMX-8259-A card.
10. To configure permissions for an MDK-111A-M card:
 - Select the first MDK-111A-M card. The **Property Editor** updates to list the available options.
 - Select **Deny** for all the properties.
 - Click **Apply** to save your changes.
11. Repeat step 10. for the remaining MDK-111A-M card, the two HDC-8222 cards, and the QSP-8229 card.
12. To configure permissions for the DashBoard Server:
 - Collapse the openGear node.
 - Select the DashBoard Server node. The **Property Editor** updates to list the available options.
 - Select **Deny** for each property listed in the **Property Editor**.
 - Click **Apply**.
13. To configure permissions for the DashBoard URM:
 - Expand the DashBoard Server node.
 - Select the DashBoard URM node. The **Property Editor** updates to list the available options.
 - Select **Deny** for each property listed in the **Property Editor**.
 - Click **Apply**.

To configure the Keyer admin Role:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Click **Create Role**.
3. Enter the required information in the **Enter Role** dialogs.

4. Add users to the Keyers Admin role as follows:
 - Click **Add Users**.
 - Select **User F** and **User G** from the list.
 - Click **Add**.
5. Select **Keyer Admin** from the tree view in the **Users** tab.
6. Select the **Permissions** tab.
7. Update the list of available devices and parameters.
8. To configure permissions for the first MDK-111A-M card as follows:
 - Expand the openGear node.
 - Expand the DFR-8321-N node.
 - Select the first MDK-111A-M card. The **Property Editor** updates to list the available options.
 - Select **Allow** for the **read** and **write** properties.
 - Select **Deny** for the **datasafe**, **reboot**, and **upgrade** properties.
 - Click **Apply** to save your changes.
9. Repeat step 8. for the second MDK-111A-M card, the two HDC-8222 cards, and the QSP-8229 card.
10. To configure permissions for an MUX-8258-A card:
 - Select the MUX-8258-A card. The **Property Editor** updates to list the available options.
 - Select **Deny** for all the properties.
 - Click **Apply** to save your changes.
11. Repeat step 10. for the DMX-8259-A card.
12. To configure permissions for the DashBoard Server:
 - Collapse the openGear node.
 - Select the DashBoard Server node. The **Property Editor** updates to list the available options.
 - Select **Deny** for each property listed in the **Property Editor**.
 - Click **Apply**.
13. To configure permissions for the DashBoard URM:
 - Expand the DashBoard Server node.
 - Select the DashBoard URM node. The **Property Editor** updates to list the available options.
 - Select **Deny** for each property listed in the **Property Editor**.
 - Click **Apply**.

To configure the Basic Users role:

1. Display the **Users** tab in the **Configure User Rights** dialog.
2. Select the **Basic Users** node from the tree view in the **Users** tab.
3. Select the **Permissions** tab.
4. Update the list of available devices and parameters.
5. To configure permissions for all openGear devices listed in the DashBoard client:
 - Select the openGear node. The **Property Editor** updates to list the available options.
 - Select **Allow** for the **read** property.
 - Select **Deny** for the **datasafe**, **reboot**, **upgrade**, and **write** properties.
 - Click **Apply** to save your changes.

6. To configure permissions for the DashBoard Server:
 - Collapse the openGear node.
 - Select the DashBoard Server node. The **Property Editor** updates to list the available options.
 - Select **Deny** for each property listed in the **Property Editor**.
 - Click **Apply**.
7. To configure permissions for the DashBoard URM:
 - Expand the DashBoard Server node.
 - Select the DashBoard URM node. The **Property Editor** updates to list the available options.
 - Select **Deny** for each property listed in the **Property Editor**.
8. Click **Apply**.
9. Add users to the Basic Users role as follows:
 - Select **Basic Users** from the tree view in the **Users** tab.
 - Select the **Profile** tab.
 - Click **Add Users**.
 - Select **Default User** from the list.
 - Click **Add**.
10. Click **Apply**.