DashBoard

The DashBoard
Role-Based Access Control Guide

For DashBoard v9.10.3 & Ross Platform Manager v1.6+

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 RBAC Guide

- Ross Part Number: **8351DR-004A-9.10.3**
- Publication Date: August 29, 2024. Printed in Canada.
- Software Issue: **9.10.3**

The information contained in this Guide is subject to change without notice or obligation. Ross Video Limited assumes no responsibility or liability for errors or inaccuracies that may appear in this manual.

Copyright

© 2024 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

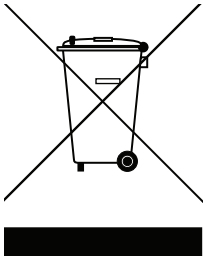
Ross Video products are protected by patent numbers US 7,034,886; US 7,508,455; US 7,602,446; US 7,802,802 B2; US 7,834,886; US 7,914,332; US 8,307,284; US 8,407,374 B2; US 8,499,019 B2; US 8,519,949 B2; US 8,743,292 B2; GB 2,419,119 B; GB 2,447,380 B. Other patents pending.

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

Table of Contents

Introduction

This chapter contains the following sections:

- Product Summary
- Features
- Functional Overview
- Applications
- Installation Overview
- Documentation Terms
- Documentation Conventions
- Contacting Technical Support

Overview

This chapter provides an introduction to the benefits of using the Ross Platform Manager to provide Role-Based Access Control (RBAC) within the DashBoard software application, and includes general information on functions and possible applications.

The Ross Platform Manager and appropriate licenses must be purchased to use Role-Based Access Control and other User Rights Management features described below.

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 User Rights Management (URM) dialog 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**: For more details on RPM capabilities, see the ***Ross Platform Manager User Guide***.

Features

DashBoard offers the following features when combined with the Ross Platform Manager (RPM):

- Role-Based Access Control (RBAC) managed by RPM
- User Rights Management (URM) for DashBoard Connect / openGear device ecosystem
- LDAP Authentication

✶ **Note**: Requires purchase of the RPM Server, software, and licenses for **LDAP Authentication**, and **Role Based Access Control**.

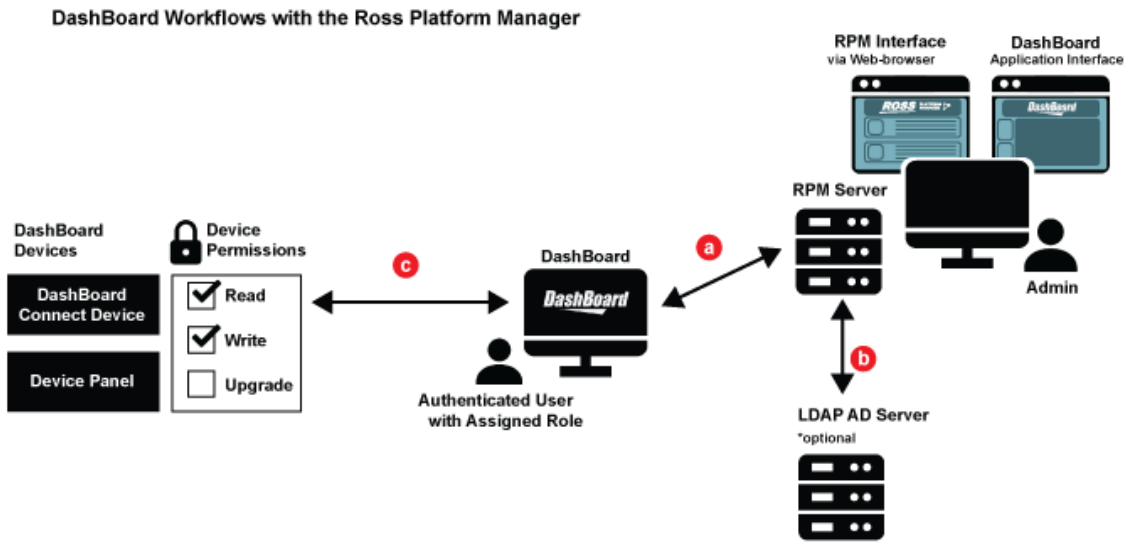
Functional Overview

Once the RPM Server has been added to DashBoard, and Role-Based Access Control permissions are configured, users must log in to the DashBoard client with a username and password before gaining access to the devices on their network. Access to devices is now configured using the options available in the DashBoard User Rights Management dialog.

You have the option of connecting to an external Lightweight Directory Access Protocol (LDAP) Server via the Ross Platform Manager (RPM) interface, or you can use either the RPM interface or DashBoard interface to configure users and roles.

Applications

You can see a diagram below of workflows where the Ross Platform Manager is used to provide authentication for DashBoard, to integrate existing user identity management systems and to provide secure a connection for supported Ross products and DashBoard Connect devices.



a. **DashBoard & RPM** — Adding an RPM node to the DashBoard tree allows administrators to require users to login to access DashBoard Connect devices. RPM is used for authentication.

b. **RPM & Active Directory** — You can integrate your existing user identity management system. RPM can retrieve users and roles from existing LDAP directories or provides the ability to configure Role-Based Access Control (RBAC) from either the RPM web-browser based interface or DashBoard Software Application interface.

c. **DashBoard Connect Devices & Supported Ross Products** — Once devices accessed through DashBoard are configured to require connection to an authenticated DashBoard instance, connection requests from unauthenticated sources are declined. DashBoard device permissions can be set to allow **read**, **write**, and/or **upgrade** permissions based on a user's assigned role.

Installation Overview

The Managing Access Control in DashBoard chapter will provides instructions for adding the RPM Server to DashBoard, and configuring RPM Server's default access control settings in the RPM web-based interface.

Documentation Terms

- All references to the **DFR-8300 series frame** also includes all version of the 10-slot and 20-slot frames and any available options.
- "**Card**" refers to openGear terminal devices within openGear frames, including all components and switches.
- "**DashBoard window**" refers to the main DashBoard client interface.
- "**Device**" refers to a product that can be monitored and controlled using DashBoard. Devices include NK routers, openGear cards, and DashBoard Connect devices.
- "**Frame**" refers to any openGear frame within your video system.
- "**System**" refers to the mix of interconnected production and terminal equipment in your environment.
- "**Tree View**" refers to the Basic Tree View and Advanced Tree View unless otherwise noted.
- "**User**" refers to the person who uses the DashBoard client.

Documentation Conventions

Special text formats are used in this guide to identify parts of the user interface, text that a user must enter, or a sequence of menus and sub-menus that must be followed to reach a particular command.

Interface Elements

Bold text is used to identify a user interface element such as a dialog box, menu item, or button. For example:

In the **Media Manager Client**, click **Channel 1** the **Channels** section.

User Entered Text

Courier text is used to identify text that a user must enter. For example:

In the **File Name** box, enter `Channel01.property`.

Referenced Guides

Italic text is used to identify the titles of referenced guides, manuals, or documents. For example:

DashBoard Server and User Rights Management User's Guide

Menu Sequences

Menu arrows are used in procedures to identify a sequence of menu items that you must follow. For example, if a step reads "**Server** > **Save As**," you would click the **Server** menu and then click **Save As**.

Interface Navigation

Navigation procedures assume that you are running Microsoft® Windows®. If you are running Mac® OS or Linux® Fedora®, menu names and options may differ.

Important Instructions

Star icons are used to identify important instructions or features. For example:

✶ Contact your I.T. Department if you experience communication issues with DashBoard and are running anti-virus software.

Getting Help

To access the built-in Help system, click **Help** in the main toolbar.

Alternatively a user can press **F1** to open **Dynamic Help**. The user can then click on areas of the window to display corresponding help information.

The DashBoard User Guide is also supplied as a print-ready PDF file on the Ross Video website.

Contacting Technical Support

At Ross Video, we take pride in the quality of our products, but if problems occur, help is as close as the nearest telephone.

Our 24-hour Hot Line service ensures you have access to technical expertise around the clock. After-sales service and technical support is provided directly by Ross Video personnel. During business hours (Eastern Time), technical support personnel are available by telephone. After hours and on weekends, a direct emergency technical support phone line is available. If the technical support person who is on call does not answer this line immediately, a voice message can be left and the call will be returned shortly. This team of highly trained staff is available to react to any problem and to do whatever is necessary to ensure customer satisfaction.

- **Technical Support:** (+1) 613-652-4886
- **After Hours Emergency:** (+1) 613-349-0006
- **E-mail:** techsupport@rossvideo.com
- **Website:** http://www.rossvideo.com

Managing Access Control in DashBoard

The Ross Platform Manager (RPM) can be used to manage Role-Based Access Control (RBAC) in the Ross facility control system, DashBoard. An RPM server can manage access to other components in the DashBoard device tree, including DashBoard Connect/openGear devices and device pages. RPM supports configuring users and roles natively, or it can sync with an existing Lightweight Directory Access Protocol (LDAP) directory server. This chapter provides steps for managing access control in DashBoard, and assumes that user roles and groups have already been configured using RPM or an LDAP directory server that RPM is connected to.

✶ To use RBAC in DashBoard, an RPM license for RBAC must be purchased and activated. To acquire the appropriate licenses, please contact a representative from Ross Video Technical Support.

This chapter discusses the following topics:

- Before You Begin
- Configure Permissions in RPM
- Adding the RPM Server to DashBoard
- Apply RBAC Permissions in DashBoard
- Login Settings in DashBoard
- Enabling a DashBoard connection to RPM over HTTPS (only for an RPM Server secured via HTTPS)

Before You Begin

This guide assumes that RPM has already been purchased through Ross Video Technical Support and that the required Role Based Access Control license and, if required, LDAP Authentication license have been purchased. You can find the contact information for Ross Video Technical Support in the **Welcome > Contact Us** tab of this manual.

Configure Permissions in RPM

You can configure the default access control permissions and name for the Ross Platform Manager Server in the RPM web interface. RPM can be configured to provide a default permission level for users, to provide access or deny permission. Once it has been configured on the RPM side, an administrator can set up customized role-based access (RBAC) permissions for each DashBoard component.

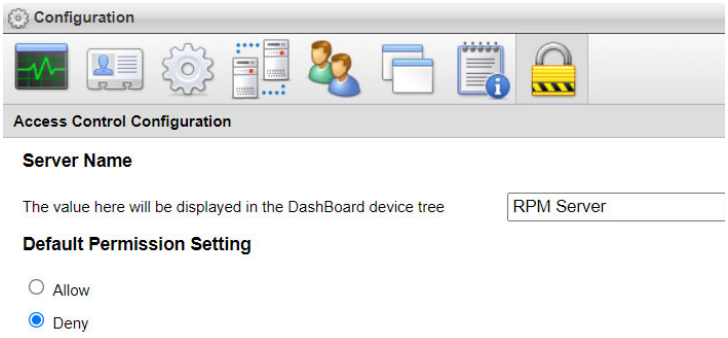
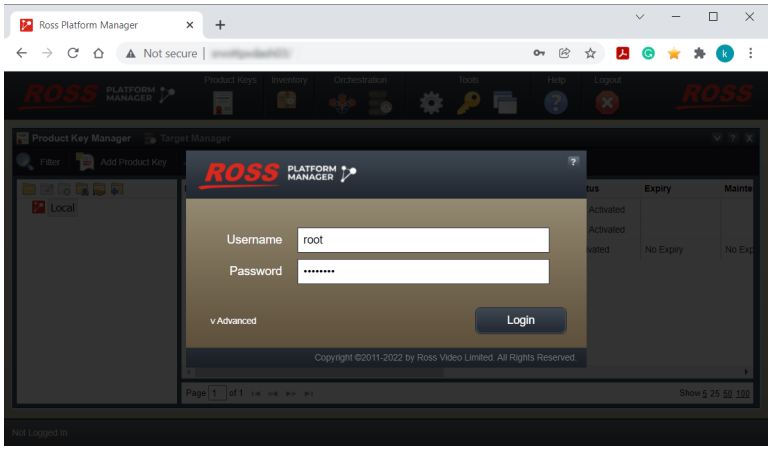


***Figure 2.1** An RPM Server is displayed in the RPM web-based interface with default permissions set to deny*

To configure the default access control permissions in RPM

1. Log in to your Ross Platform Manager interface as a system administrator or root user.



2. On the main toolbar, click the **Configuration** icon. If the **Configuration** icon is not visible, you are not an administrator and cannot configure the server.

3. On the **Configuration** window toolbar, click the **Access Control** icon.

   The **Access Control** panel opens.

4. For the RPM **Server Name**, enter a meaningful name. For example **`RPM Server - Deny`** or **`RPM Server - FullAccess`**.

5. For the **Default Permissions** settings, select one of the following:

   › **Allow** — Select this as the default setting to allow users full access to components in the DashBoard tree.

   › **Deny** — Select this as the default setting to deny users access to components in the DashBoard tree.

   Note: A user with admin rights can then configure custom role-based access control at a later point from within the DashBoard application, to allow or deny access to specific components in DashBoard.

To change the RPM server name displayed in DashBoard

To help keep track of the default access control settings for the RPM server, you may wish to add a meaningful name for the server.

1. Log in to your Ross Platform Manager interface as a system administrator.
2. On the main toolbar, click the **Configuration** icon. If the **Configuration** icon is not visible, you are not an administrator and cannot configure the server.

   The **Configuration** window opens.

3. On the **Configuration** window toolbar, click the **Access Control** icon.

   The **Access Control** panel opens.

4. For the RPM **Server Name**, enter a meaningful name. This is the name that will be displayed for the RPM Server when you add the RPM server to DashBoard.
5. Click **Apply Changes > OK**.

Adding the RPM Server to DashBoard

You can use the RPM Server to enforce RBAC for Ross Video's open source facility control system, DashBoard.

To add the RPM Server to DashBoard

The RPM Server must be added to the DashBoard device tree to apply RBAC.

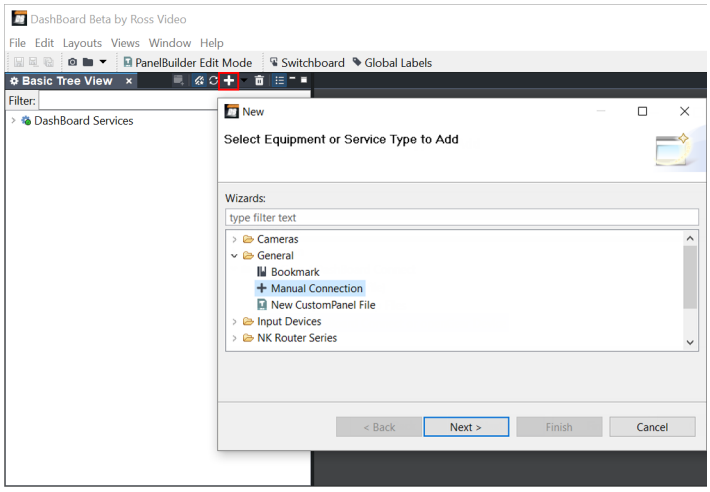
✶ You must download a version of DashBoard that supports RBAC features. Currently DashBoard v9.4 and later support RBAC using RPM v1.6 or later.

You can download the latest version of DashBoard from the Ross Video website:

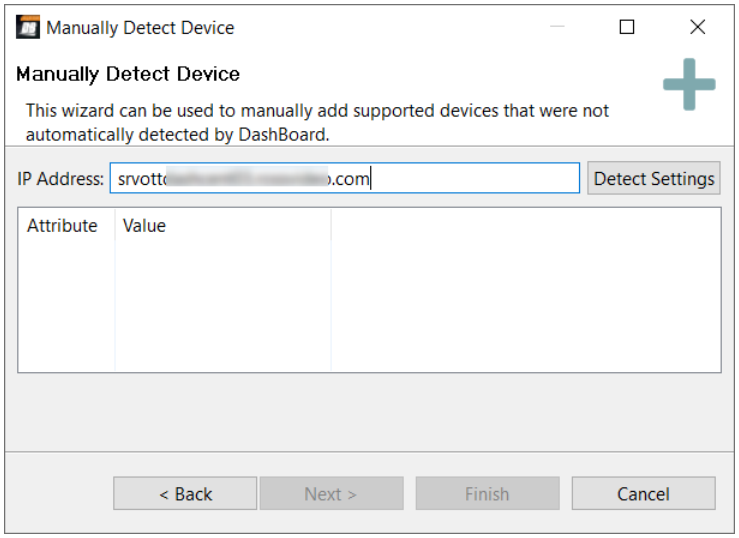
› https://www.rossvideo.com/support/software-downloads/dashboard/

1. To add the RPM Server in DashBoard, open the DashBoard software application, and from the **Basic Tree View** toolbar, click the plus icon.

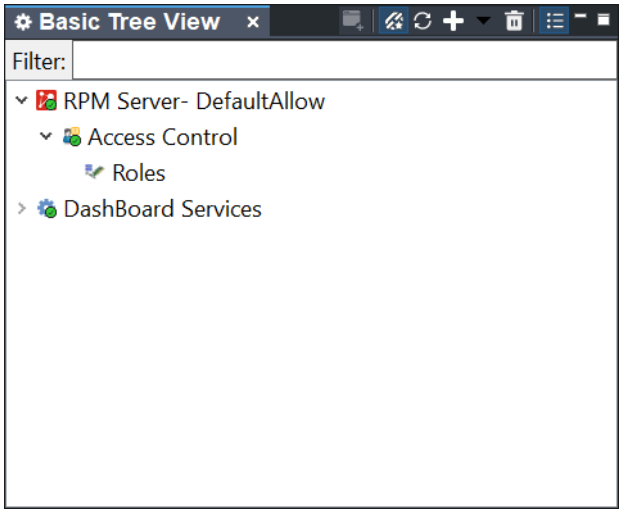
✶ **Important**: If the RPM Server has been configured to deny access by default, then once you have completed the wizard steps below, then DashBoard will require you to login as a user with an admin role to access DashBoard resources. The default admin role will have access to all resources, but if you sign in as a user without the correct permissions then you may be locked out of resources.



2. Select **General > Manual Connection** as the type and click **Next**.
3. Add the fully qualified server name, click **Detect Frame Information** and once the information populates click **Finish**.

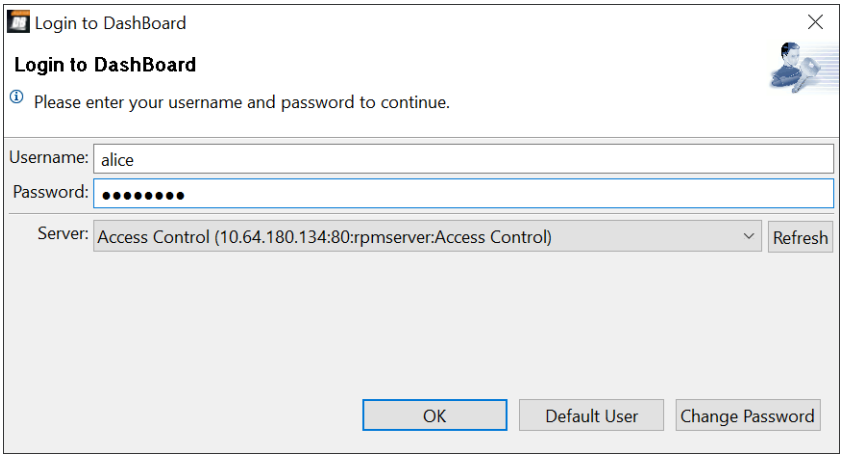


The RPM Server appears on the left, in the DashBoard tree view.

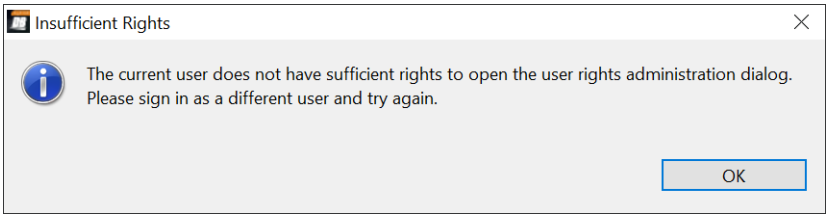


A prompt will appear that requires you to log in to DashBoard.

4. Login with the admin credentials that you created in RPM.



Tip: If you do not have the correct permissions, you will see a prompt appear:



Tip: If the user is not set to “active” in the RPM user settings, you will see a prompt appear:

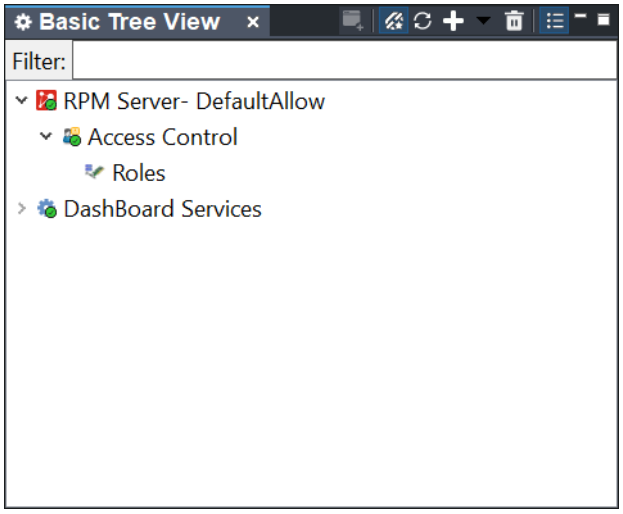
Once you have successfully logged in, you can go to the next steps to learn how to apply RBAC permissions in DashBoard, or you can apply permissions in RPM.

Apply RBAC Permissions in DashBoard

You can configure user permissions and assign roles in either the DashBoard or RPM interface, however you can only apply RBAC permissions to access DashBoard equipment, and devices from the DashBoard interface.

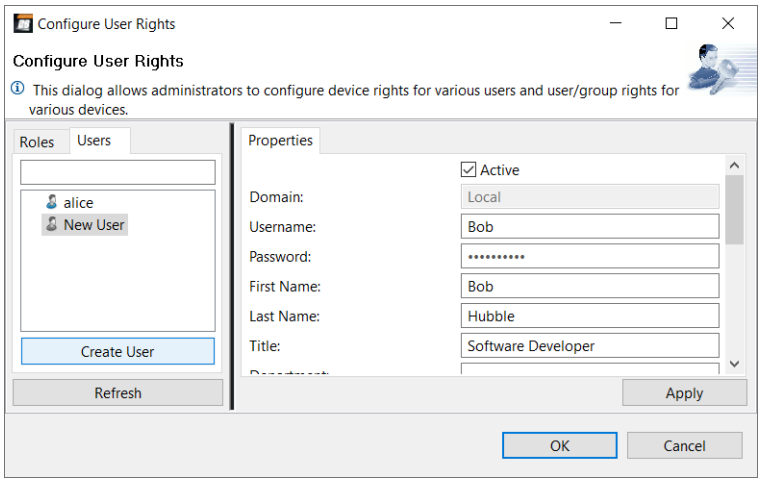
To create or edit a user in DashBoard

1. From the DashBoard tree view, expand the RPM Server node to view the Access Control and Roles sub-nodes. Double-click on the **Roles** node to open the **Configure User Rights** dialog.



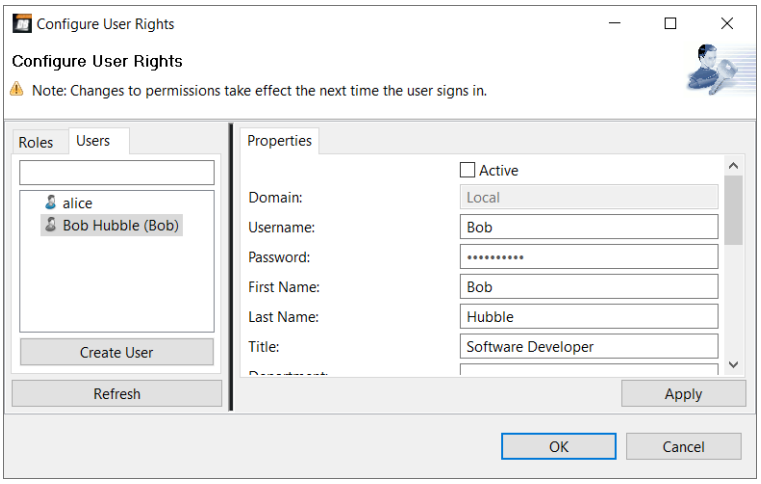
The **Configure User Rights** dialog opens.

2. You can proceed to configure User Rights and Permissions



3. Click the **Users** tab, and click the **Create User** button. Upon first use, the **Properties** tab on the right will display a blank “New User’ profile that is ready to be filled in, but typically a prompt will appear to request the

User Name.

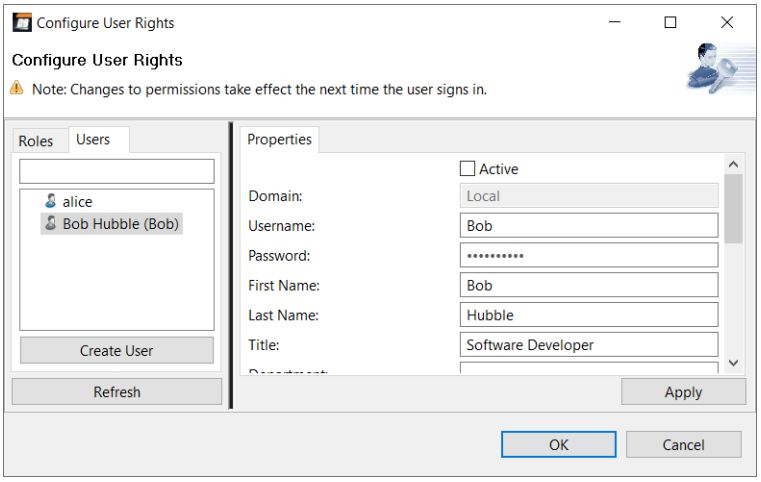


4. Add the appropriate user information (required fields are identified with an asterisk *):

   - Domain
   - Username*
   - Password*
   - First Name
   - Last Name
   - Title
   - Department
   - Email
   - Phone
   - Mobile

   Click the **Apply** button.

   The new user should now appear in the list under the Users tab, as shown:

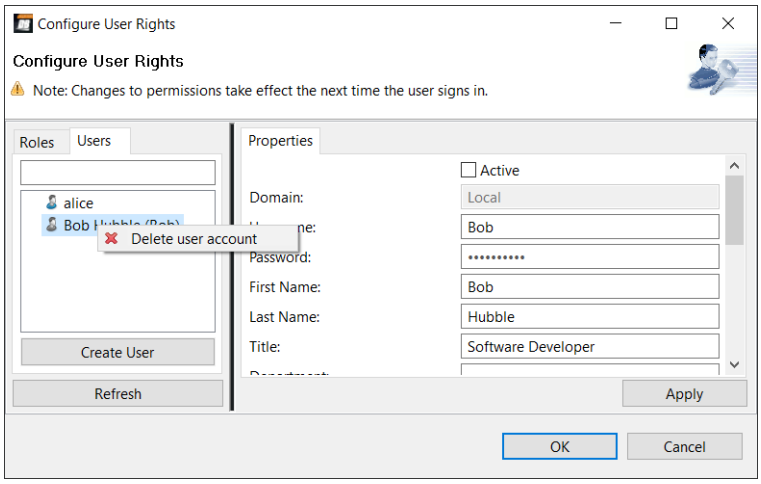


5. Click **OK.**

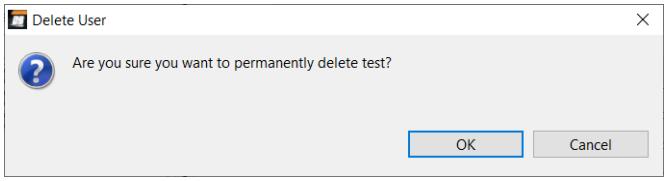
To delete a user in DashBoard

✶ **Important**: Before you try to delete a user, ensure that you have removed any assigned roles first.

1. From the **Configure User Rights** dialog, click the **Users** tab, and type the name of the user you wish to remove in the search filter.
2. Right-click on the user you wish to delete and select **Delete User Account**.



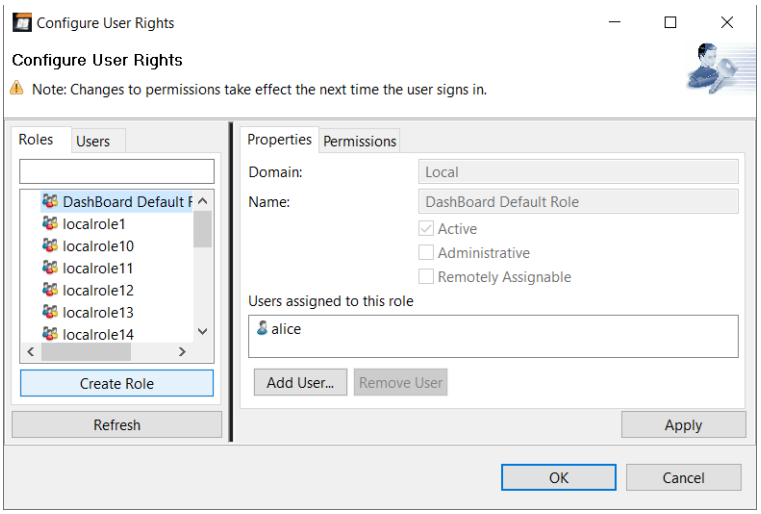
3. Click **OK** to confirm that you wish to permanently delete the user**.**



The user account will no longer work when the user next attempts to sign in.

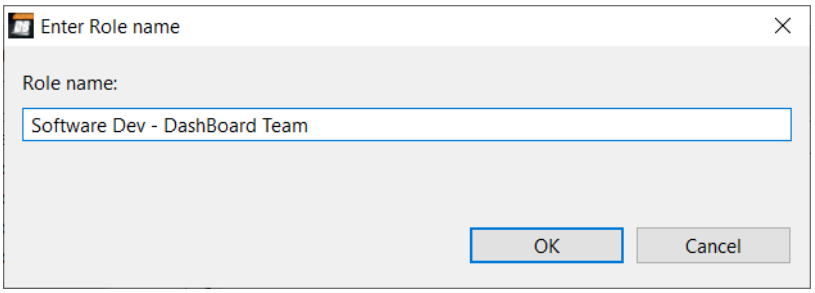
To create and assign a role in DashBoard

1. From the **Configure User Rights** dialog, click the **Roles** tab, select **Create Role**.



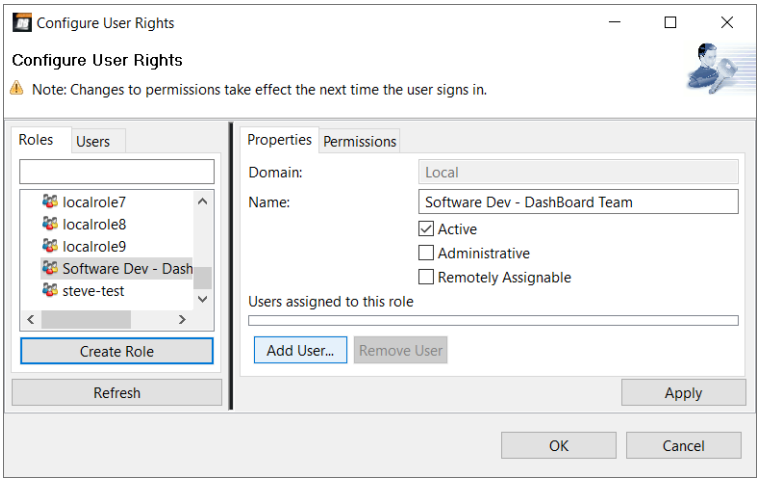
An Enter Role name prompt will appear.

2. Enter a meaningful Role name**.**



3. Configure the **Role Properties** and **Permissions** under each respective tab, as shown below:

   - **Properties** tab:



   › **Domain** — This field is not editable, and displays whether the role was created locally or via LDAP Active Directory.

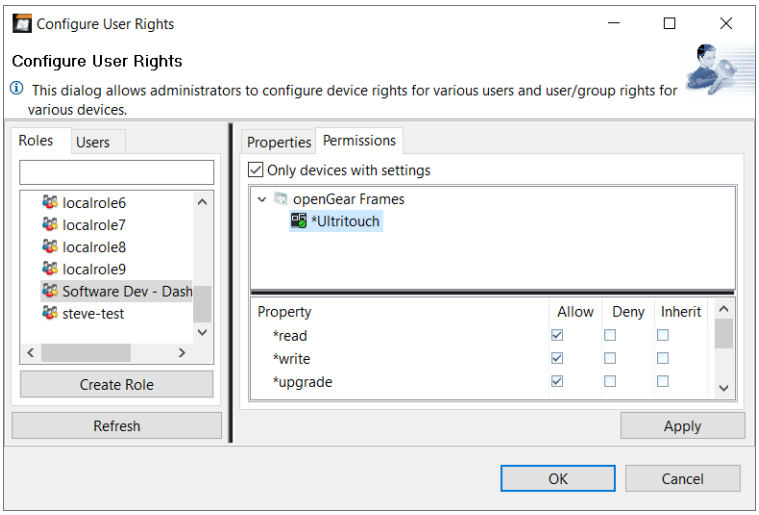
   › **Active** — Required for active users. Check this box to deactivate a user account.

   › **Administrative** — Check this box to provide administrative permissions.

   › **Remotely Assignable** — Check this box to allow the role to be edited in the RPM web-based interface.

› **Add User** — Add any users you wish to assign this role to.

- **Role Permissions** tab:



› **Only devices with settings** — Check this box to constrain permissions to the devices listed here. The devices you see here have already been added to DashBoard and appear in the **Tree View.** You must then select Allow, Deny or Inherit to set permissions for each device or sub node for different access user permission levels (read, write or upgrade).

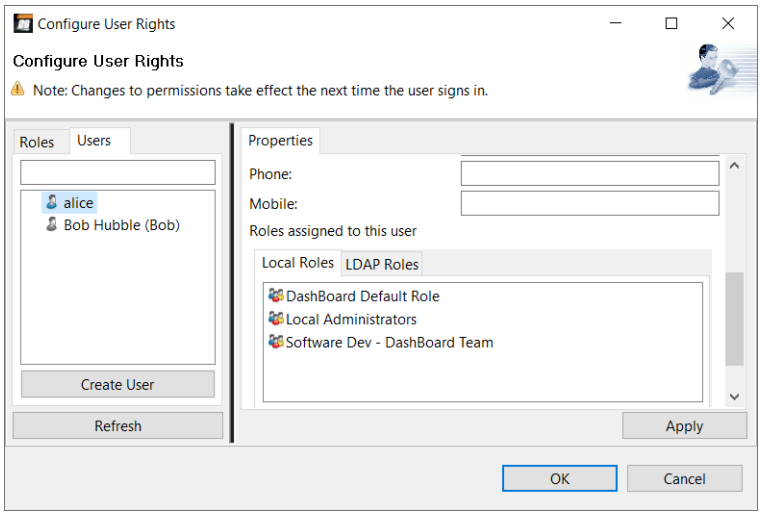
Allow — Check this box to allow access to the selected device.

Deny — Check this box to deny access to the selected device.

Inherit — Check this box to inherit the settings from the "parent" device.

› **Apply**— Click this button when complete.

4. After your changes have been applied, go back to the **Users** tab to confirm that the appropriate users now have the role assigned under **Properties > Local Roles**.



For more information on configuring users and roles, see the ***Ross Platform Manager User Guide*** chapters:

› Configuring User Permissions

› Configuring LDAP Authentication

Login Settings in DashBoard

The default **Login Settings** can be configured in DashBoard.

To Change the Default Login Settings in DashBoard

Users can change the default login settings in their DashBoard **Preferences** from the DashBoard top menu, under **Window > Preferences > Login Settings**.

1. To open the DashBoard **Preferences** pane, go to the top menu and select **Window > Preferences > Login Settings**.
2. Ensure the appropriate **Data Source** is selected for the RPM Server, and then choose from the following Login Settings:
   - Remember nothing
   - Remember last user ID
   - Sign me in automatically
3. You can also adjust the default Timeout of 20 minutes to your preferred value.
4. **Apply** your new settings or click **Restore Default** to return to the original DashBoard default settings.

Enabling a DashBoard connection to RPM over HTTPS

You can secure the Ross Platform Manager (RPM) server with HTTP Secure (HTTPS) to allow the client and server to first establish a secure encrypted channel over Secure Socket Layers (SSL). This is recommended for enhanced security and to ensure that the RPM web-based interface always displays the appropriate security certificate to indicate that it is from a trusted organization.

A Ross commissioner sets up the RPM server with secure HTTPS certificate. This chapter assumes that the RPM web-based interface uses a trusted certificate, and provides details on how to import the server certificate into DashBoard's list of trusted security certificates.

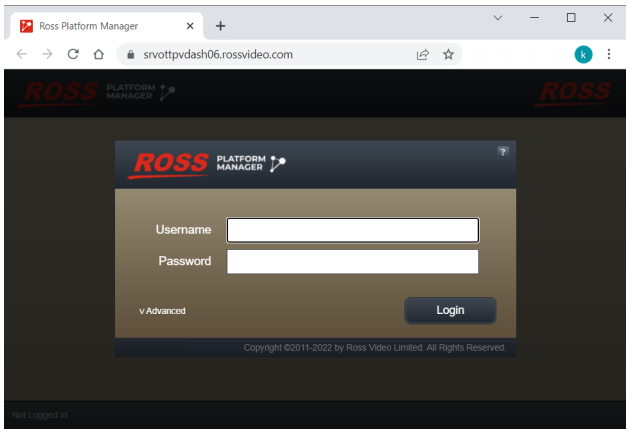
These procedures are tested and shown using the latest Chrome Browser (version 98.0.4758.81).

✶ **Important**: If you wish DashBoard to communicate with an RPM server that has been secured via HTTPS, it is required that you complete the steps below to enable a secured connection to RPM before adding the RPM server to DashBoard.

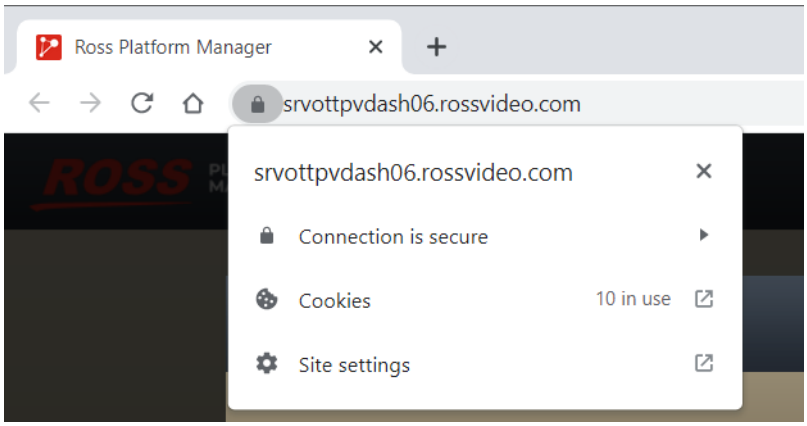
To enable a DashBoard connection to RPM over HTTPS

You will download the exported RPM server certificate, .CER file from the Chrome browser and import the RPM server's trusted CA certificate to store it in DashBoard's list of trusted security certificates.

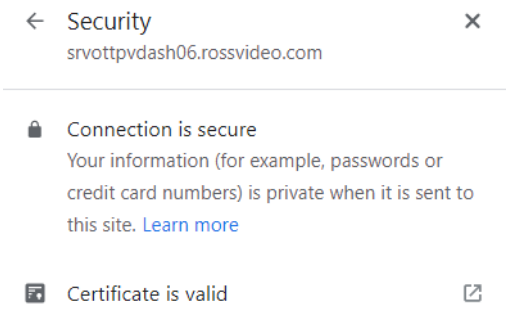
1. Open the web browser, in this case Google Chrome, and navigate to the HTTPS version of the Ross Platform Manager address. For example, `https://srvottdash01.rossvideo.com`.



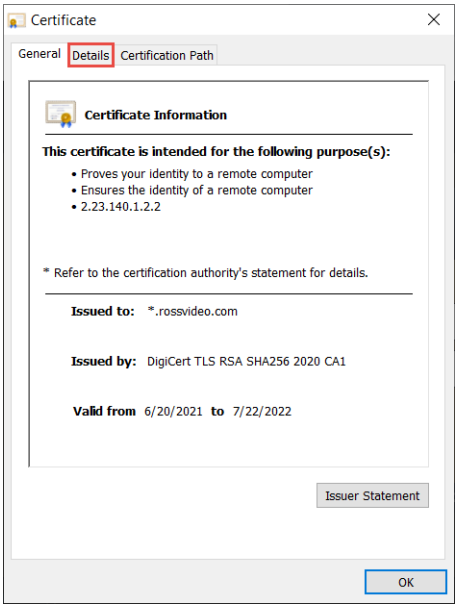
2. Click on the "Secured" lock icon that appears in front of the RPM interface's URL in the Chrome browser.



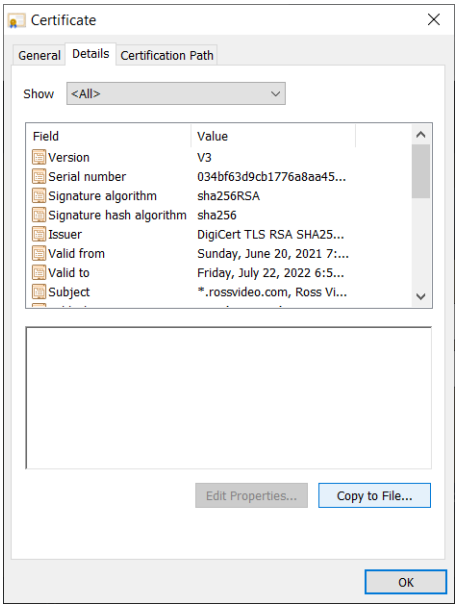
3. Click **Connection is secure** > **Certificate is valid**. The Certificate dialog opens.



4. Confirm that the certificate statements are correct and valid, and click the **Details** tab.

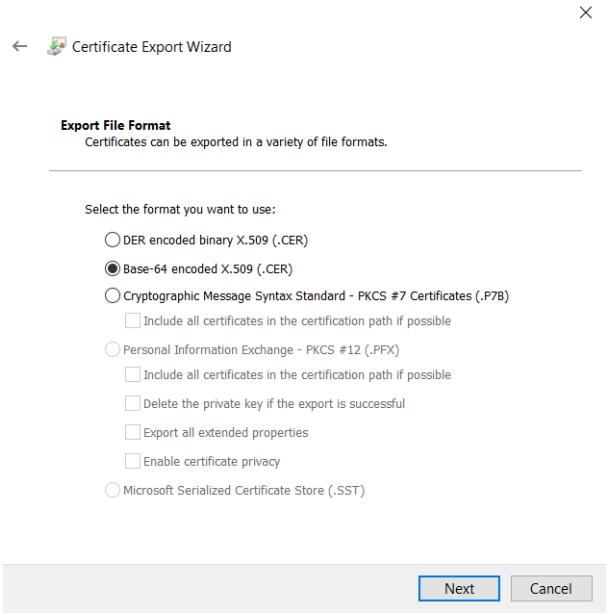


5. Select **Copy to File**, and the Certificate Export Wizard appears. Set the following:



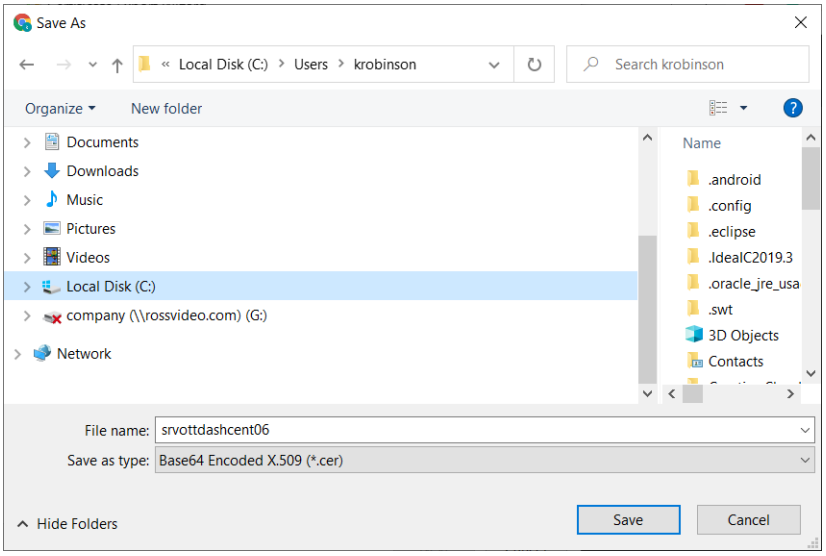
   a. In the Certificate Export Wizard, to start the process click **Next**.

b. For the Export File Format, select the **Base-64 encoded X.509 (.CER)** and click **Next**.



c. For the File to Export, click **Browse...**, choose the file directory, and then enter the name for the exported .CER file.
Take note of the directory that you choose to save the .CER file to (in this case `C:\Users\krobinson\srvottdashcent06.cer`)

Click **Save**.



d. To complete the Certificate Export Wizard, click **Finish**. A popup will indicate that the certificate was successfully imported.

e. Click **OK**.

6. Now that you have the location of the .CER file noted down, locate the directory path that you installed DashBoard in. Typically DashBoard is installed in the C Drive: `C:\DashBoard\`.

In this example the following values are used:

- **Exported server certificate** — `C:\Users\krobinson\srvottdashcent06.cer`
- **DashBoard installation folder** — `C:\DashBoard\`

7. Open the Command Line Interface (CLI) and run the following command:

✶ Make sure to modify the example paths to match your own settings.

Example

```
keytool -keystore "C:\DashBoard\jre\lib\security\cacerts" -import
-alias rpm -file "C:\Users\krobinson\srvottdashcent06.cer"
-trustcacerts -storepass changeit
```

8. Click **Yes** when prompted.

You can now proceed to add your HTTPS enabled RPM Server to DashBoard to use RBAC functionality.

For More Information on...

- Adding the RPM Server to DashBoard