PAXSTORE Role Management User Guide

10-19-2020

V1.0

Preface

This document is provided for informational purposes only. All features and specifications are subject to change without notice. If there are any problems in the documentation, please report them to PAX in writing. This document is not warranted to be error-free. Except as may be expressly permitted in the license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

Security Notice: No part of this publication may be copied, distributed, stored in a retrieval system, translated into any human or computer language, transmitted, in any form or by any means, without the prior written consent of PAX Technology, Inc.

Technical Support

If there is a problem while installing, registering or operating this product, please make sure to review the documentation. If unable to resolve the issue, please contact PAX.

The level of access to this Service is by the support plan arrangements made between PAX and the Organization. Please consult this support plan for further information about entitlements, including the hours when telephone support is available.

Technical Support Contact Information

Phone: (877) 859-0099

Email: support@pax.us

URL: www.pax.us

Revision History

Date	Version	Description
10-19-2020	V1.0	Initial Release

Table of Contents

1. Introduction

The Role Management feature supports access control for users to include; no access, read only access and full privileges for each option.

It also allows the ability to assign levels of access to specific users within the Role Management and Operation Control sections.

1.1 Purpose

The information provided in this document is to describe the features and functionality. It will also describe the steps on how to use the features.

1.2 Intended Audience

- Marketplace Administrators
- Reseller Administrators
- Help Desk
- Account Managers
- Sales Engineers

1.3 Acronyms and Terms

Acronym	Definition
Role Management	Provides specific users selected access levels to feature sections.
Operation Control	Provides specific users access to enable or disable or use the selected features
User List	A list of users assigned to a Role
Role Detail	A detailed list of features with Privileges within a Role.
User	An individual with an approved account in the PAXSTORE.
Privileges	Privileges are grouped features and functions within the store that are designated to a Role. The Privilege will have various levels of access.
Full	Full access which includes, read and write abilities.
Readonly	Limited access which includes read only abilities.

2. Role Management Category

The Role Management category has two features that helps manage user access and feature control throughout the PAXSTORE. These two features are called Role Management and Operation Control. This document will cover these two features.

- **Role Management** - is a security feature that when configured a user can be assigned an access level called a Role. Each Role has it's own specific set of Privileges that a User is assigned.
- **Operation Control** - is a security feature that a User can be assigned access to the assigned store option.

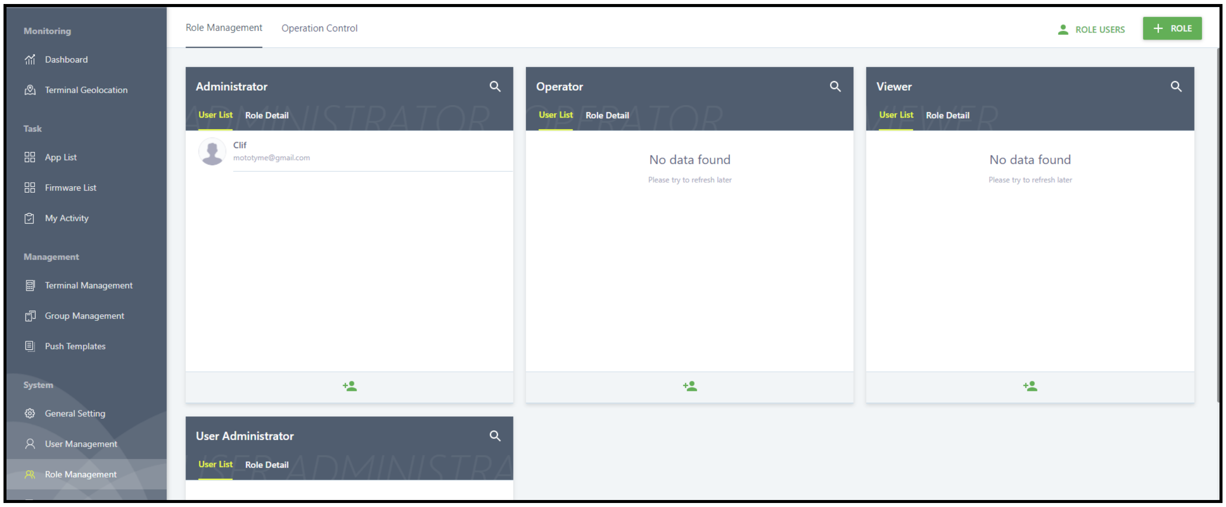
2.1 Role Management

Role Management is a security feature that when configured a user can be assigned an access level called a Role. Each Role has it's own specific set of Privileges that a User is assigned.

Each Role has two features, User List and Role Detail. The User List will list all of the Users included in the Role. The Role Detail will list all of the Privileges and the Access Levels for each Privilege for that Role.

By default there are four roles.

- Administrator
- Operator
- Viewer
- User Administrator



Clif
mototyme@gmail.com

No data found
Please try to refresh later

No data found
Please try to refresh later

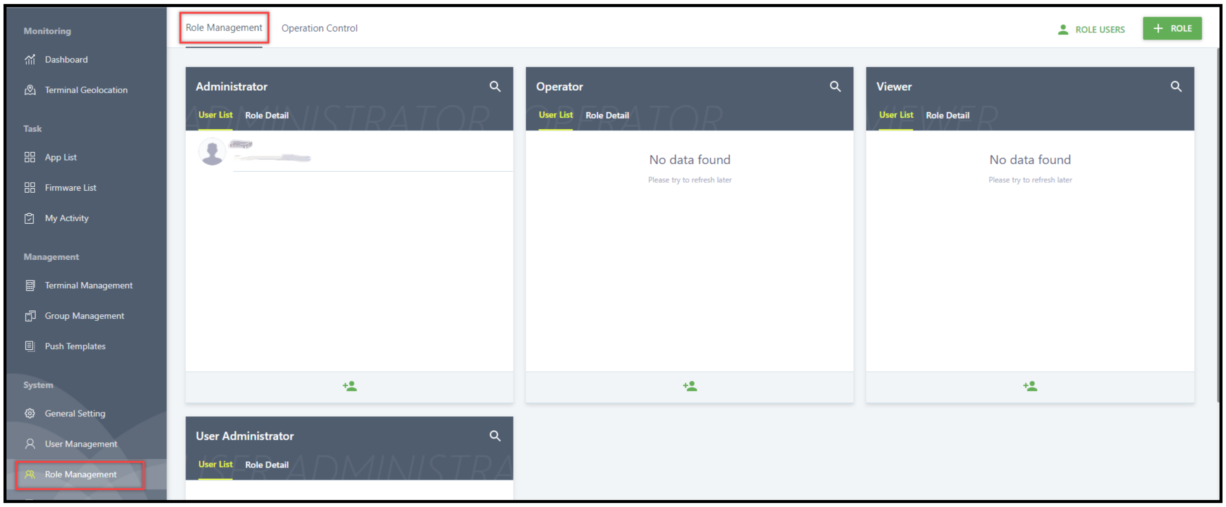
2 .1.1 Access Levels

There are two Access Levels. Only one access level is setup with a User for an assigned feature (Privilege).

- Full - The User has full read and write access with the assigned Privilege.
- Readonly - The User has read only access with the assigned Privilege.

2 .1.2 Accessing Role Management

From the Administrator Center select **[Role Management] > [Role Management].**



No data found

Please try to refresh later

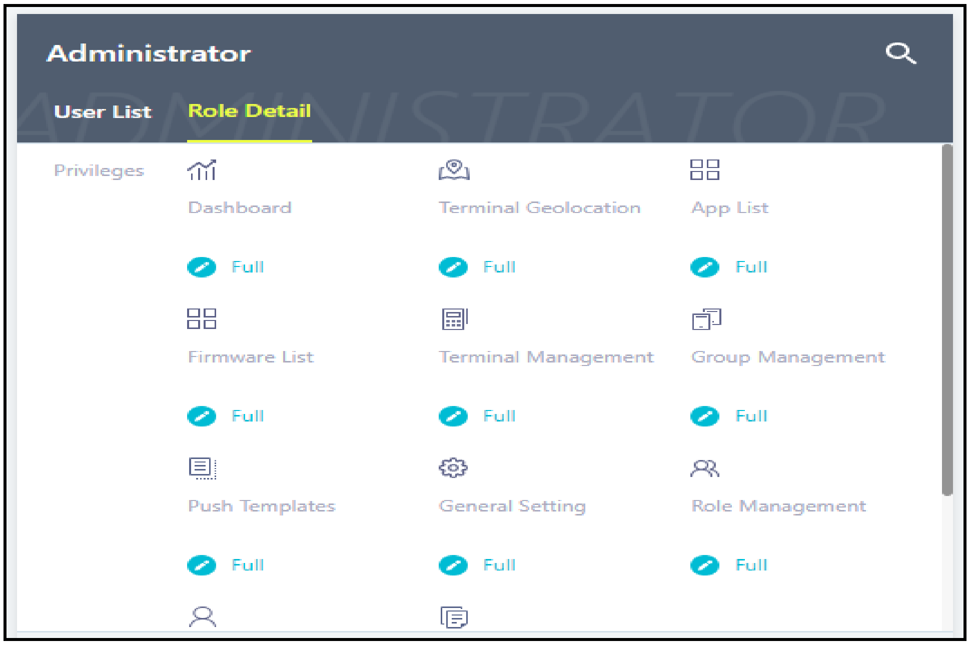
No data found

Please try to refresh later

2 .1.3 Administrator Role

The following **Administrator Role** features and functions have **Full** privileges:

✎ Full	✎ Full	✎ Full
Dashboard	Terminal Geolocation	App List
Firmware List	Terminal Management	Group Management
Push Templates	General Setting	Role Management
User Management	Report Center	



Administrator

User List Role Detail

Privileges

Dashboard ✎ Full

Terminal Geolocation ✎ Full

App List ✎ Full

Firmware List ✎ Full

Terminal Management ✎ Full

Group Management ✎ Full

Push Templates ✎ Full

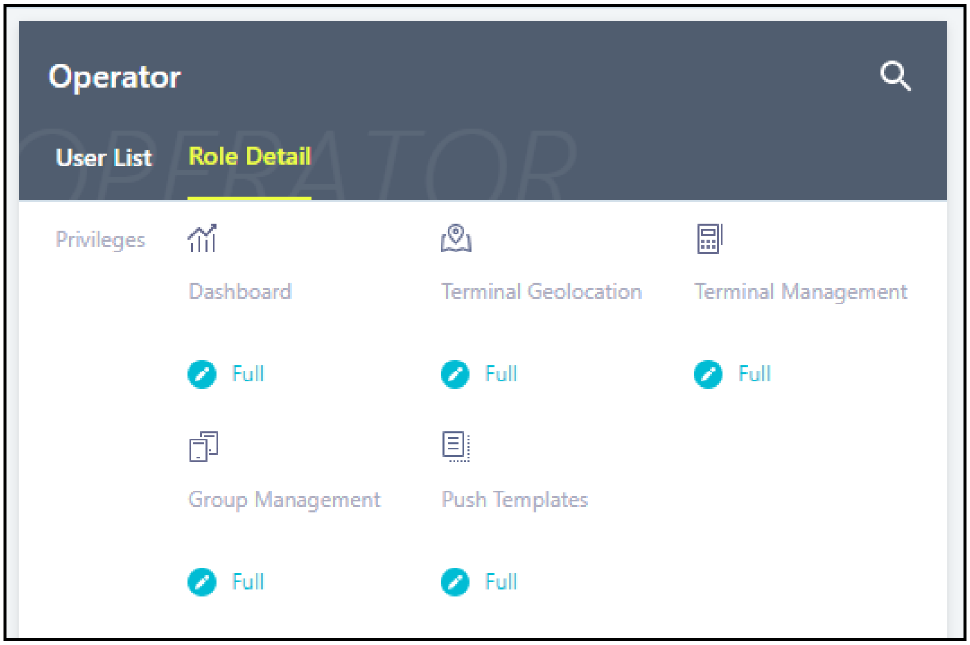
General Setting ✎ Full

Role Management ✎ Full

2 .1.4 Operator Role

The following **Operator Role** features and functions have **Full** privileges:

Dashboard Full	Terminal Geolocation Full	Terminal Management Full
Group Management Full	Push Templates Full	


Operator

User List Role Detail

Privileges

Dashboard: Full

Terminal Geolocation: Full

Terminal Management: Full

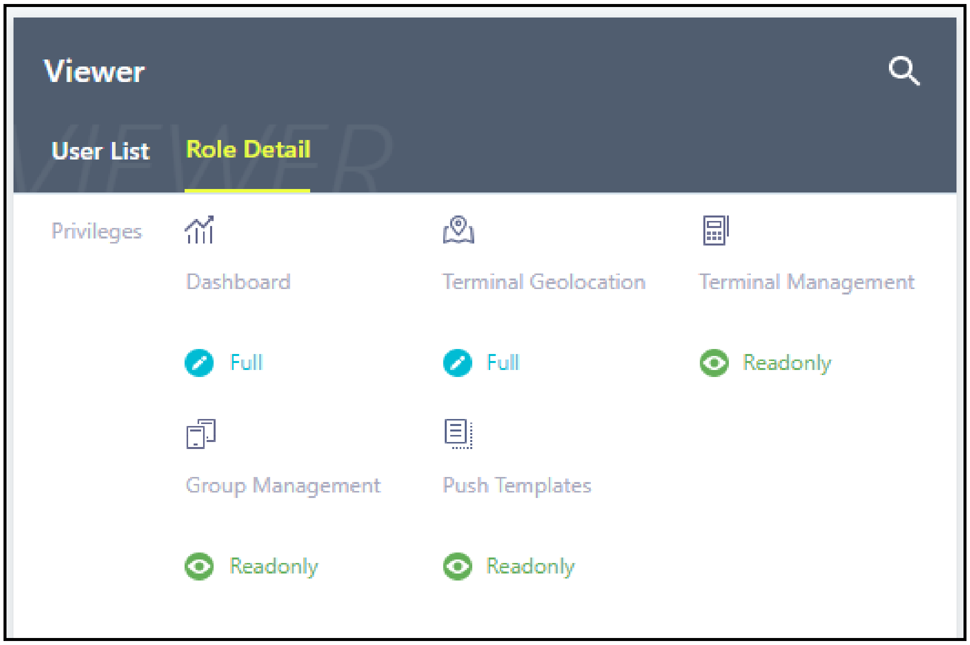
Group Management: Full

Push Templates: Full

2 .1.5 VIEWER ROLE

The following **Viewer Role** features and functions have **Full** and **Readonly** privileges:

Dashboard Full	Terminal Geolocation Full	Terminal Management Readonly
Group Management Readonly	Push Templates Readonly	



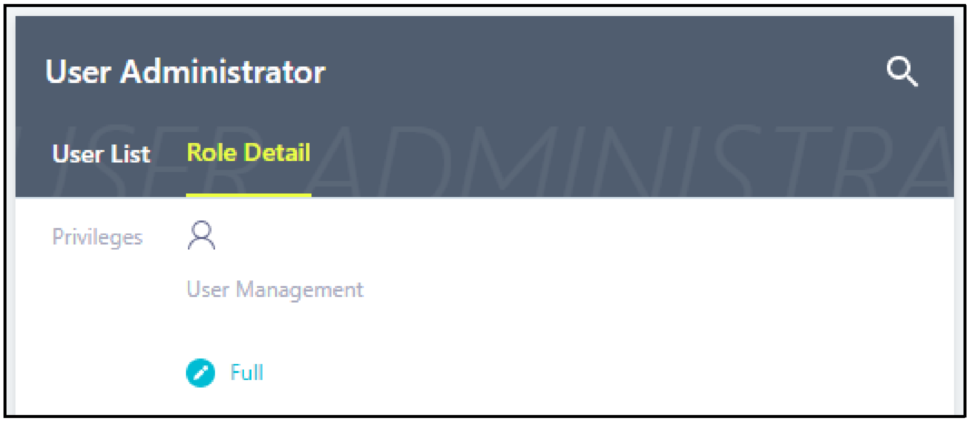
Privileges

Dashboard Full	Terminal Geolocation Full	Terminal Management Readonly
Group Management Readonly	Push Templates Readonly	

2 .1.6 User Administrator Role

The following **Administrator Role** feature has **Full** privileges:

User Management ✎ Full		



User Administrator

Privileges

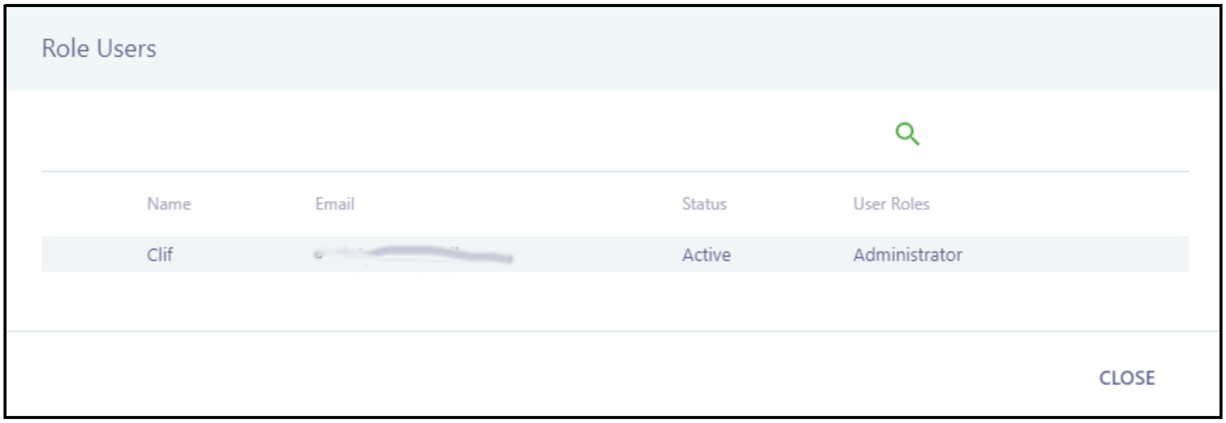
User Management

✎ Full

2 .1.7 Role Users

The Role Users option will display all of the Users and the Users information. It has a search option to search for Role Users.

- **Name** - The name of the User.
- **Email** - The email of the User.
- **Status** - The status of the User either Active, Inactive, Registered or Suspended.
- **User Roles** - Will display the User Role and the User can have more than one Role. All Roles of the User will be displayed.

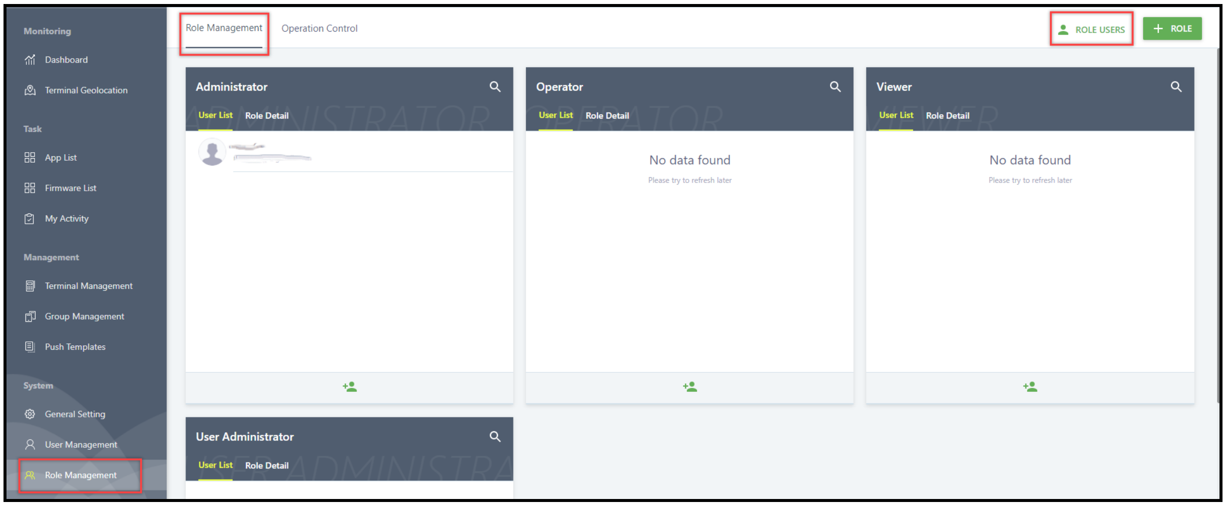


Role Users

Name	Email	Status	User Roles
Clif	[redacted]	Active	Administrator

2 .1.8 Accessing Role Users

From the Administrator Center select **[Role Management] > [Role Management] > [ROLE USERS].**



No data found

Please try to refresh later

No data found

Please try to refresh later

2 .1.9 Feature Definitions

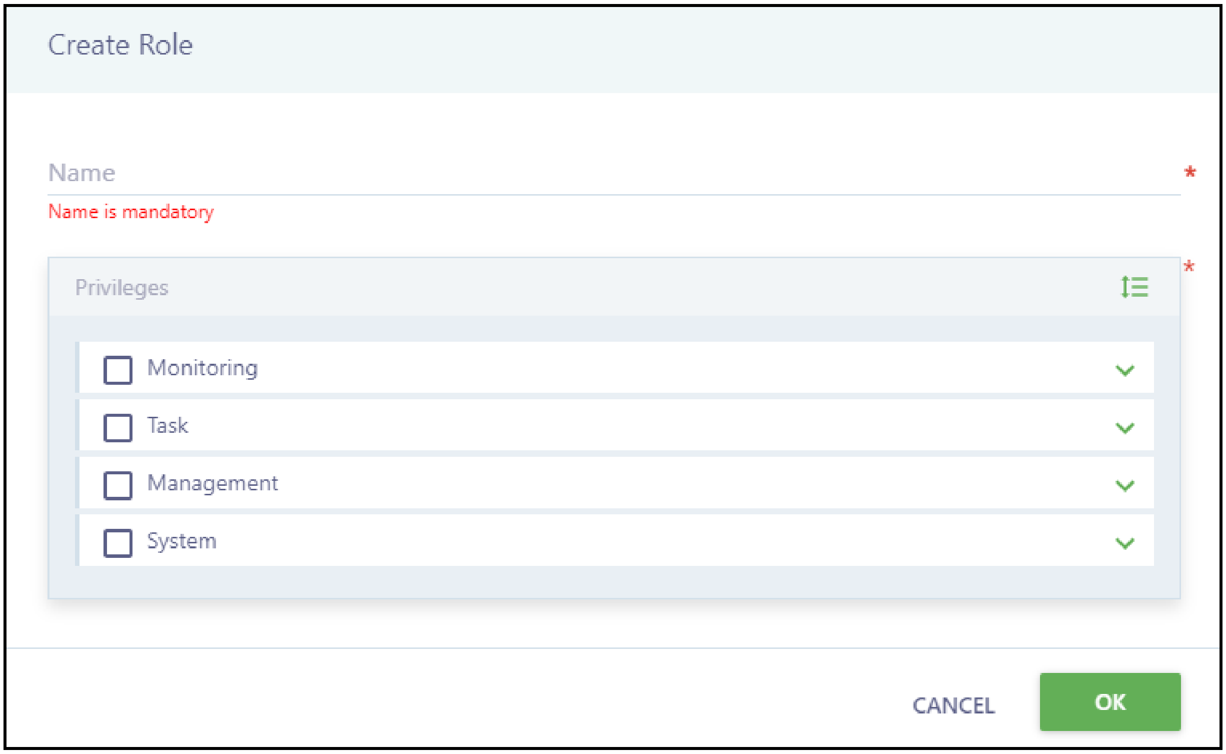
Feature	Definition
Dashboard	Widgets that display various performance reports and the Terminal Map. Reports can be added or removed.
Terminal Geolocation	GPS Terminal Location, terminal details, terminal apps, terminal status
App List	List of Terminal Applications, app details, app settings, installed terminals
Firmware List	List of Firmware, notice of firmware updates, firmware details, by terminal
Terminal Management	Section to add, move or delete terminals, add, modify or delete applications for terminals. See terminal status and terminal information.
Group Management	Section for managing Groups by General Group and Dynamic Group, Group Details, Terminal List, Group Detail, Parameter Variables
Push Templates	Ability to create, delete, manage, and push templates.
General Setting	This is an Admin level management section for UI, API and RKI settings.
User Management	This is used to manage Users status and password resets.
Role Management	This section controls User access to various features within the store. Full or Readonly access.
Report Center	Ability to view, print, and export various reports.

2.2 + Role

The + Role feature allows creating a new custom Role. The new custom role can have it's own unique name and configuration based from selecting the available Privilege options. Role Users can be assigned to the new custom Role.

There are many Privileges and Access options available for configuration:

- Monitoring
  - Dashboard
  - Terminal Geolocation
- Task
  - App List
    - Readonly Privileges
    - Full Privileges
  - Firmware List
    - Readonly Privileges
    - Full Privileges
- Management
  - Terminal Management
    - Readonly Privileges
    - Full Privileges
  - Group Management
    - Readonly Privileges
    - Full Privileges
  - Push Template
    - Readonly Privileges
    - Full Privileges
- System
  - General Setting
    - Readonly Privileges
    - Full Privileges
  - User Management
    - Readonly Privileges
    - Full Privileges



Create Role

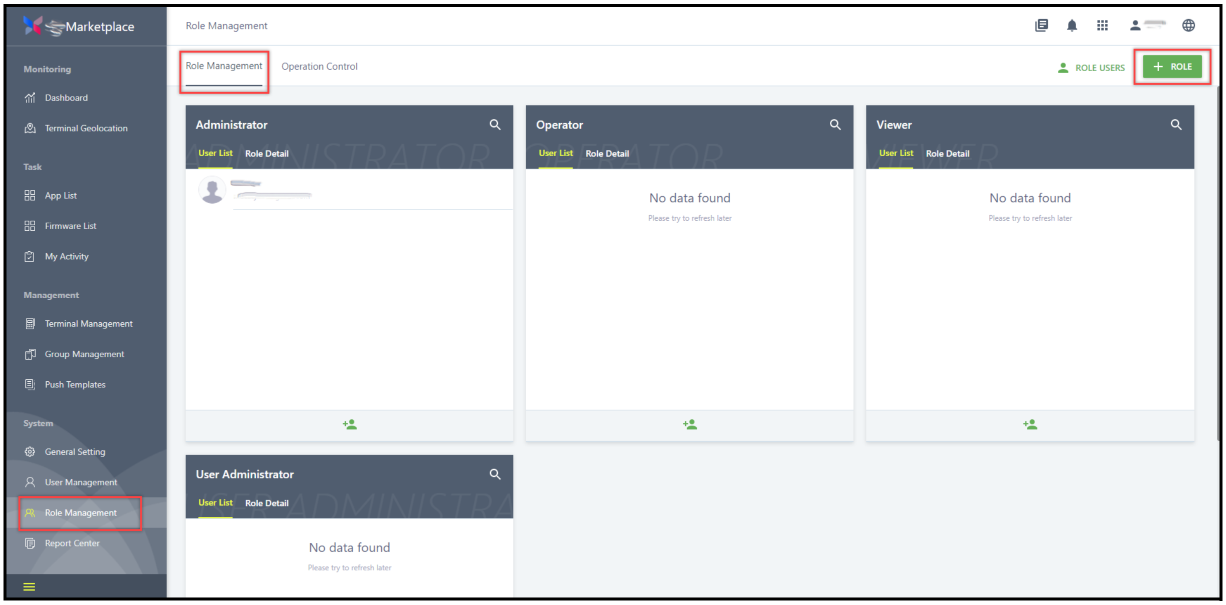
Name *

Name is mandatory

Privileges *

2 .2.1 Accessing + Role

From the Administrator Center select **[Role Management] > [Role Management] > [+ ROLE].**



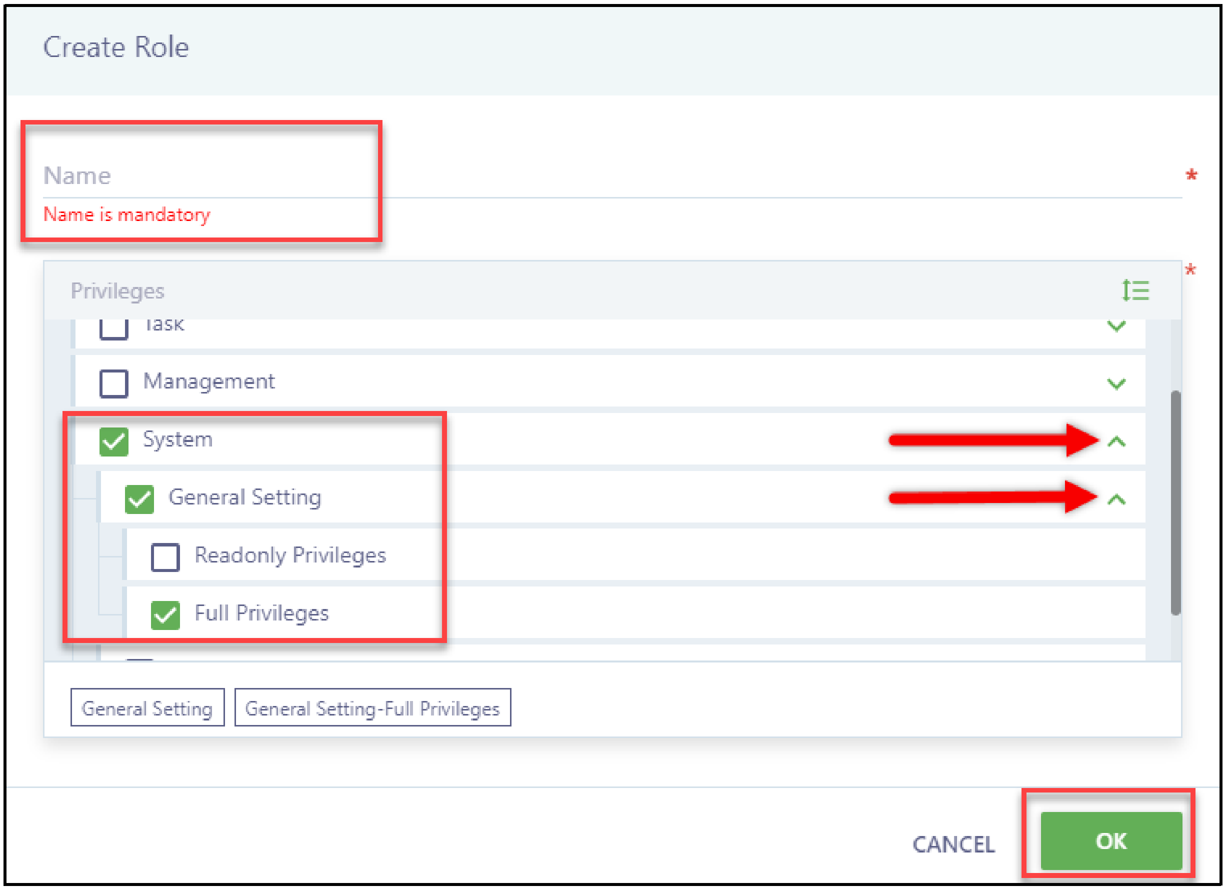
No data found

Please try to refresh later

2 .2.2 How to Create a Role

The Role Management feature has an option to create a custom Role. This section covers how to create a custom Role. It is possible to create multiple custom Roles.

From the Administrator Center select **[Role Management] > [Role Management] > [+ ROLE] >** enter the **[< name >]** of the new Role **>** select the desired **[Privilege]** and then select the up/down arrow to display additional supporting **Privileges** and **Access Types.** Select the desired supporting **[Privilege]** and **[Access Type]** > and then select **[OK]** to save the selections**.**



Create Role

Name *

Name is mandatory

Privileges *

□ Task

□ Management

☑ System

☑ General Setting

□ Readonly Privileges

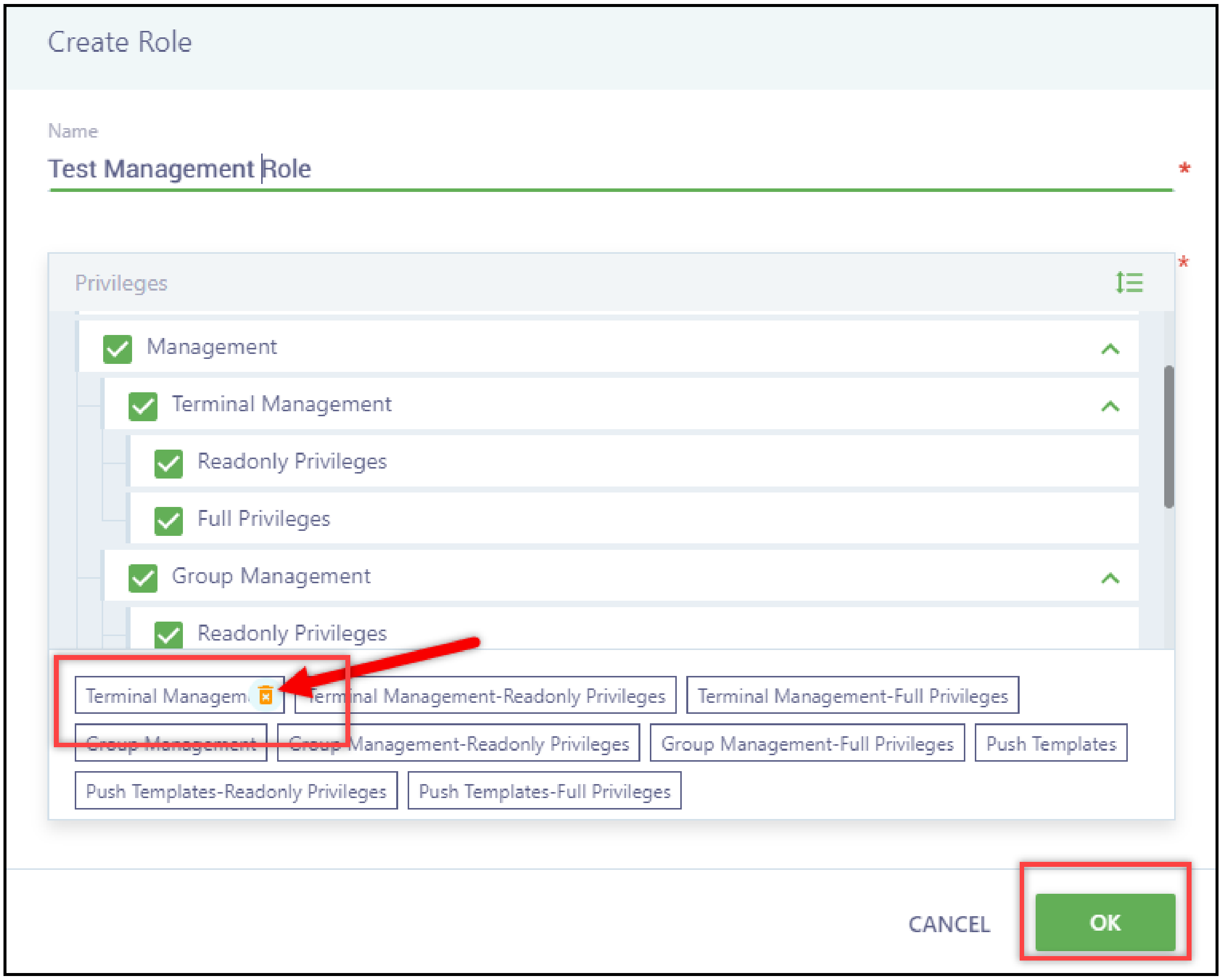
☑ Full Privileges

General Setting

General Setting-Full Privileges

2 .2.3 Deleting a Feature

It is also possible to delete features from the list by selecting the feature from the list at the bottom of the page and select **[OK]** to save settings.



Create Role

Name

Test Management Role *

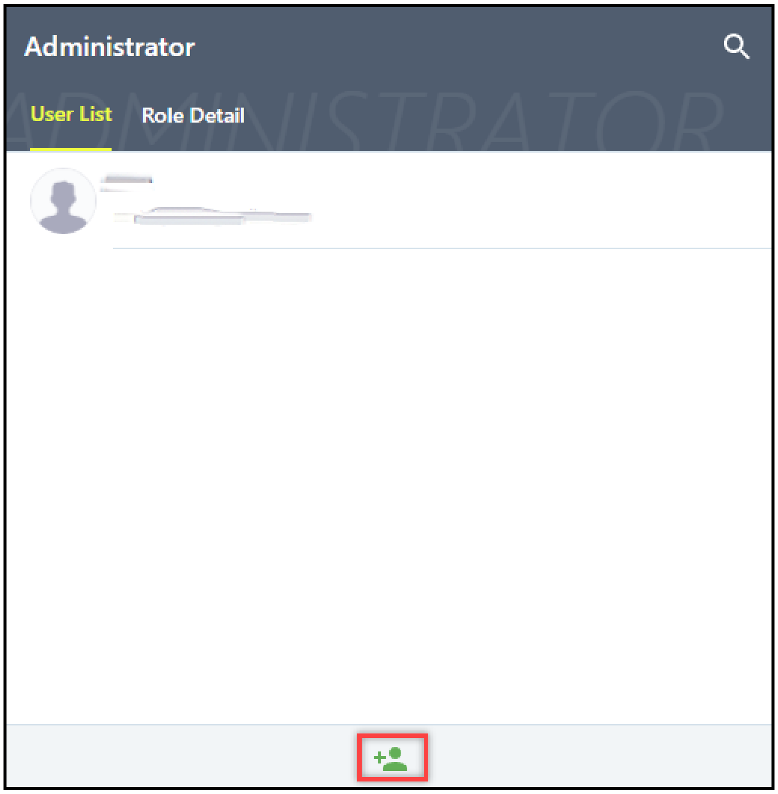
Privileges *

☑ Management
☑ Terminal Management
☑ Readonly Privileges
☑ Full Privileges
☑ Group Management
☑ Readonly Privileges

Terminal Managem ☒ | Terminal Management-Readonly Privileges | Terminal Management-Full Privileges | Group Management | Group Management-Readonly Privileges | Group Management-Full Privileges | Push Templates | Push Templates-Readonly Privileges | Push Templates-Full Privileges

2 .2.4 Role Management Add User

From the Administrator Center select **[Role Management] > [Role Management] >** select the desired **[<Role Management>] > [User List] >** select the green add + User icon at the bottom > enter the **[<User email address>]** > **[OK]** to save.

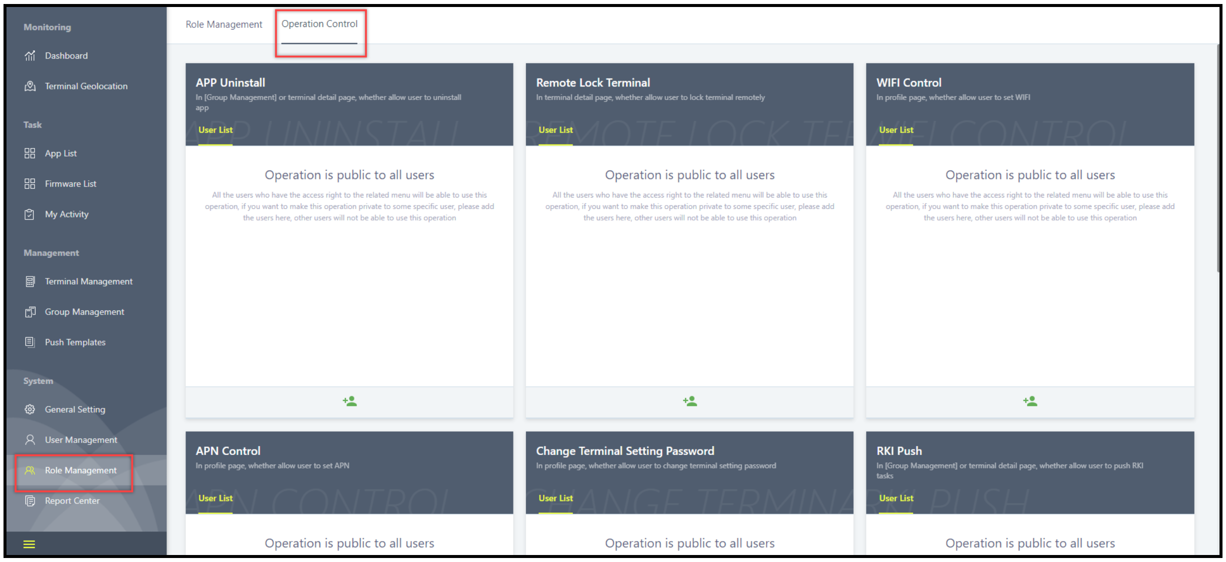


2.3 Operation Control

Operation Control is a security feature that a User can be assigned access to the store option.

The User List will list all of the Users included in the Operational Control feature.

From the Administrator Center select **[Role Management] > [Operation Control].**



APP Uninstall
In [Group Management] or terminal detail page, whether allow user to uninstall app

Operation is public to all users
All the users who have the access right to the related menu will be able to use this operation, if you want to make this operation private to some specific user, please add the users here, other users will not be able to use this operation

Remote Lock Terminal
In terminal detail page, whether allow user to lock terminal remotely

Operation is public to all users
All the users who have the access right to the related menu will be able to use this operation, if you want to make this operation private to some specific user, please add the users here, other users will not be able to use this operation

WIFI Control
In profile page, whether allow user to set WIFI

Operation is public to all users
All the users who have the access right to the related menu will be able to use this operation, if you want to make this operation private to some specific user, please add the users here, other users will not be able to use this operation

APN Control
In profile page, whether allow user to set APN

Operation is public to all users

Change Terminal Setting Password
In profile page, whether allow user to change terminal setting password

Operation is public to all users

RKI Push
In [Group Management] or terminal detail page, whether allow user to push RKI tasks

Operation is public to all users

IMPORTANT: By default all Operation Controls has all Users with full access to the options. As soon as a User is assigned an Operation Control feature that selected Operational Control drops all Users accept the assigned Users. Only the assigned Users are supported for that Operation Control feature.

2 .3.1 *OPERATIONAL CONTROL FEATURES*

The Operational Control Features are features within the store that Users can enable or disable or operate a store feature.

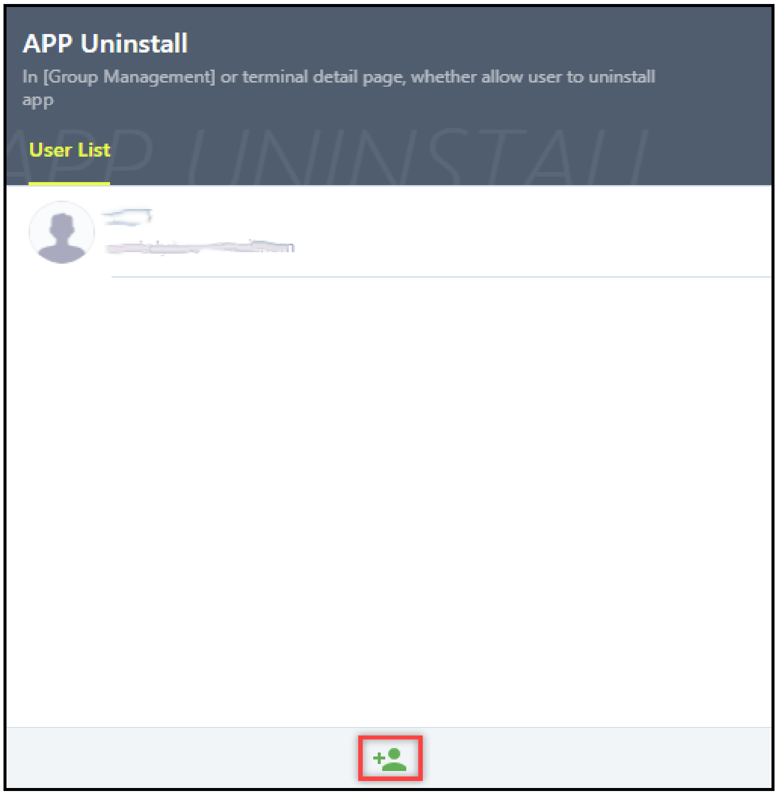
Feature	Definition
APP Uninstall	In the Group Management or Terminal Detail section the ability to use the Push Uninstall Applications feature.
Remote Lock Terminal	In the Terminal Detail section the ability to remotely lock or unlock a terminal.
WIFI Control	In the Reseller/Merchant Profile section the ability to configure the Wi-Fi settings.
APN Control	In the Reseller/Merchant Profile section the ability to configure the terminal APN settings.
Change Terminal Setting Password	In the Reseller/Merchant Profile section the ability to edit the terminal password.

Feature	Definition
RKI Push	In the General Settings ability to setup RKI
RKI Setting	In the General Settings ability to create RKI keys
Air Viewer	In the Terminal Detail section allows remote access to a terminal.

2 .3.2 How to add Users to Operation Control

From the Administrator Center select **[Role Management] > [Operation Control] >** select the desired **[<Operation Control>] > [User List] >** select the green add + User icon at the bottom > enter the **[<User email address>]** > **[OK]** to save settings.

IMPORTANT: By default all Operation Controls has all Users with full access to the options. As soon as a User is assigned an Operation Control feature that selected Operational Control drops all Users accept the assigned Users. Only the assigned Users are supported for that Operation Control feature.



APP Uninstall

In [Group Management] or terminal detail page, whether allow user to uninstall app

[redacted]

Customer Support

For questions or help with the PAXSTORE please contact your service provider or PAX customer support.

9am - 1am EDT Monday - Friday
9am - 5pm EDT Saturday
Hours Subject to Change

Contact Information
support@pax.us
(877) 859-0099
www.pax.us

PAX Technology Inc.
8880 Freedom Crossing Trail
Building 400
3rd Floor, Suite 300
Jacksonville, FL 32256

This document is provided for informational purposes only. All features and specifications are subject to change without notice. The PAX name and PAX logo are registered trademarks of PAX Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

PAX Technology, Inc. is not responsible for the content, quality, accuracy or completeness of any information or materials contained in on these pages. PAX Technology, Inc. does not endorse any content, viewpoints, products, or services contained on these pages and shall not be held liable for any losses caused by reliance on the accuracy, reliability or timeliness of such information. Any person or entity that relies on any information obtained from these pages does so at his/her own risk.