



Configuring RBAC Using Admin UI

This chapter describes the Security feature of Prime Cable Provisioning. Use this feature to configure and manage various levels of security. For conceptual information about the RBAC feature, see [RBAC Management, page 3-14](#).

For better user management and security, Prime Cable Provisioning introduces Role Based Access Control (RBAC) that provides an approach to restrict access to system functions and resources to authorized users. Roles are composed of fine grain privileges. A privilege is a base unit of enforcement. A role groups a set of privileges into a logical job function to enable the customization of authorization policies beyond the default provided out of the box.

Prime Cable Provisioning comes with some default out of the box (OOTB) roles, privileges, users, user groups and domains that you can leverage from. Apart from these default configurations, you can also define your own setup to meet your organization requirements. The default OOTB configurations cannot be edited or deleted.

There are four levels of checks.

- URL access check - Enforcement by web facing components such as Admin UI or web services.
- Operation/Method level check - Enforcement done by the components protecting access to operations. This type of access check is primarily performed in the RDU and DPE CLI. It is meant to ensure that the user has the correct privileges to invoke operations.
- Instance level check - Enforcement to ensure that the user has access to a specific object. This enforcement is performed in the RDU and leverage database capabilities.
- Property level check - Enforcement to ensure that the user has write access to a specific property. This enforcement is performed in the RDU.

Configuring Security

Use the Security menu to configure and manage various levels of security. You can:

- Add, modify, or delete domains, see [Domain Management, page 13-2](#).
- Add, modify, clone or delete roles using the default privileges, see [Role Management, page 13-3](#).
- Add, modify, clone or delete user groups, assign roles to the user groups, see [User Group Management, page 13-4](#).
- Map the existing external user groups to the Prime Cable Provisioning user groups, see [User Group Mapping, page 13-5](#).
- Add, modify, or delete users, assign roles and domains to these users, see [User Management, page 13-5](#).

Domain Management

Domains are a set of instances with various objects such as Device, COS, File, DPE, NR, Provisioning Group, and DHCP Criteria. Domain represents a collection of these objects grouped for instance level access control. Only authenticated users with the appropriate access privileges will be able to view the instances that exist in their domains.

Domains are represented hierarchically with all the custom domains added as sub domains of the default domain RootDomain. A user who has access to a parent domain can access all of the sub domains of that parent domain.

Adding a Domain

**Note**

By default, Domain management related pages or widgets are not available in the Admin UI. Even the instance level authz field is not displayed.

To enable them, the property `/adminui/enableDomainAdministration` must be set to true. This property can be set in the `adminui.properties` file located at `BPR_HOME/rdu/conf`. Restart the tomcat server after making the changes to the property file.

To add a domain:

-
- Step 1** Choose **Security > Domain Management**.
 - Step 2** Select a parent domain and click **Add Domain** to display the Add Domain page.
 - Step 3** Enter the new domain's name. Domains must have unique names across the system.
 - Step 4** Enter a short description of the new domain.

**Tip**

Use the description field to identify the domain or any detail that uniquely identifies the new domain.

-
- Step 5** Click **Save**.
-

Role Management

A role is a job function that defines a set of capabilities a user or user group can perform. These capabilities are governed by the privileges assigned to the role. Privileges allow the user to perform operations like create, read, update, and delete objects and its properties in Prime Cable Provisioning. Privileges are in-built in Prime Cable Provisioning and cannot be modified, see [Table 13-2](#) for the list of default privileges.

A set of default out-of-the-box roles are available for use. You also can create custom roles with any set of in-built privileges assigned to a custom role. These roles are loaded into the RDU database after installing Prime Cable Provisioning.

Adding a New Role

To add a role:

Step 1 Choose **Security > Role Management**.

Step 2 Click **Add Role** to display the Add Role page.

Step 3 Enter the new role's name.

Step 4 Enter a short description of the new role.



Tip Use the description field to identify the role or any detail that uniquely identifies the new role.

Step 5 To add privileges to the new role:

- a. Click the Privileges tab and then click Add Privileges.
- b. Check the appropriate check box to determine the new role's privilege.
- c. Click **Apply**.

Step 6 To add the properties that can be modified for this role:

- a. Click the Modifiable Device Properties tab and then click Add Modifiable Device Properties.
- b. Check the appropriate check box to add the permission to modify the selected device properties to the new role.
- c. Click **Apply**.

Step 7 To add custom property:

- a. Click the Custom Properties tab and then click Add Custom Properties.
- b. Check the appropriate check box to add the custom property to the new role.
- c. Click **Apply**.



Note If you are adding a custom property through the Admin UI, it can be of type String only. However, if you are adding it using the Configuration.addRole API, it need not be restricted to the type String alone.

Step 8 Click **Save**.

Modifying a Role

The default roles listed in [Table 13-3](#) cannot be modified. To modify a custom role, select the role and click **Edit**. Make the necessary edits and click **Save**.

**Note**

If you are modifying a custom property through the Admin UI, it can be of type String only. However, if you are using the Configuration.changeRoleProperties API, it need not be restricted to the type String alone.

User Group Management

A user group is a collection of users. Similar to a user, a user group can also be assigned roles. Users who belong a user group will inherit all the roles assigned to that the user group. Those roles are constrained to only be valid on the resources that are also members of the group. A user can be a member of more than one group. The set of privileges the user gains is the aggregate of all those from the role.

From the User Group Management option you can add, modify, delete and clone user groups.

Adding a New User Group

To add a user group:

-
- Step 1** Choose **Security > User Group Management**.
 - Step 2** Click **Add User Group** to display the Add User Group page.
 - Step 3** Enter the new user group's name.
 - Step 4** Enter a short description of the new user group.

**Tip**

Use the description field to identify the user group's role or any detail that uniquely identifies the new user group.

-
- Step 5** Click Add Roles.
 - Step 6** Check the appropriate check box to determine the new user group's role.
 - Step 7** Click **Apply**.
 - Step 8** Click **Save**.
-

**Note**

Only the administrator can delete any other user groups that appears in the User Group Management page. You cannot delete the default user group, called Administrators.

User Group Mapping

Prime Cable Provisioning provides user-group mapping, which enables mapping of an external user-group name to a Prime Cable Provisioning user-group name. An external group can be mapped to any existing Prime Cable Provisioning user-group. In the example table below Operator is mapped to ProvGroupAdmin and Admin is mapped to administrators.

Table 13-1 lists examples for User Group mapping.

Table 13-1 Example User Group Mapping

External user-group	RDU user-group name
Operator	ProvGroupAdmin
Admin	Administrators

In the user-group mapping table, set of external group names must be unique and not duplicates. However, more than one external group can map to an internal user-group.

**Note**

Before deleting an internal user-group, all the mappings to that user-group should be deleted.

Adding a User Group Mapping

To create a new user group mapping:

- Step 1** Choose **Security > User Group Mapping**.
- Step 2** Click **Add User Group Mapping**. A new blank row appears.
- Step 3** Enter the existing external user group name in the Remote Group Name field.

**Note**

Remote Group Name field is case sensitive.

- Step 4** Select the user group to be mapped from the User Group Name drop-down list.
- Step 5** Click **Save**.

User Management

Managing users involves adding, modifying, and deleting users who administer Prime Cable Provisioning. Depending on your privileges you can use this menu to add, modify, and delete users. This menu displays all users configured to use Prime Cable Provisioning and identifies their user groups.

Prime Cable Provisioning provides role based access to a user with specific privileges to ensure access control and the integrity of provisioning data. A user can be assigned roles that determine the scope of actions they can perform in Prime Cable Provisioning. A user can also be added to user groups with pre-assigned roles.

The assigned username appears near the top-right corner of every screen on the administrator user interface.

**Note**

During migration from an acceptable previous release to Prime Cable Provisioning, all migrated read-only users are assigned to the out of the box read only role and RootDomain. Similarly, all the read-write users are assigned to the out of the box read only role and RootDomain.

You can administer users only if you have user related privileges.

Adding a New User

Adding a new user is a simple process of entering the user's name and creating a password. However, while creating a new user you must specify number of sessions, assign a role, or add the user to a user group or domain to be able to gain privileges to perform specific actions.

**Note**

Prime Cable Provisioning comes with one Admin user already created; you cannot create this user again.

To add a new user:

- Step 1** Choose **Security > User Management**.
- Step 2** Click **Add** to display the Add User page.
- Step 3** Enter the new user's name.
- Step 4** You can restrict the number of concurrent sessions a user can have by modifying the value in the **Number of sessions allowed** field. If you do not specify any value in this field, the number of sessions allowed for the user would be decided on the value of the field at the RDU Defaults page.
- Step 5** Enter a short description of the new user.

**Tip**

Use the description field to identify the user's job, position, or any detail that uniquely identifies the new user.

- Step 6** Enter a password and confirm it. Ensure that the password that you enter has at least 8 characters.
- Step 7** To add roles to the new user:
 - a. Click the Roles tab and then click Add Roles.
 - b. Check the appropriate check box to determine the new user's role.
 - c. Click **Apply**.
- Step 8** To add the new user to a user group:
 - a. Click the Usergroup tab and then click Add Usergroups.
 - b. Check the appropriate check box to add the new user to the user groups.
 - c. Click **Apply**.
- Step 9** To add the new user to a domain:
 - a. Click the Domain tab and then click Add Domains.
 - b. Check the appropriate check box to add the new user to the domain.

c. Click **Apply**.

Step 10 Click **Save**.



Note Remember to record and store the new user's password in a safe place to help prevent loss or theft and possible unauthorized entry.

Default Configurations

This section describes the default configurations of Prime Cable Provisioning.

Default Privileges

Table 13-2 lists the default privileges in Prime Cable Provisioning.

Table 13-2 **Default Privileges**

Privileges	Description
All	
*	The user is granted access to all the objects. It is equivalent to granting all the privileges to the user.
Class of Service	
PRIV_COS_CREATE	Enables adding a new COS object in the system.
PRIV_COS_READ	Enables viewing a COS object and all of its properties. Enables the selection of COS objects.
PRIV_COS_UPDATE	Enables modifying any property of a COS object.
PRIV_COS_DELETE	Enables deleting a COS object from the system.
DHCP Criteria	
PRIV_DHCP_CRITERIA_CREATE	Enables adding a new DHCP Criteria object in the system.
PRIV_DHCP_CRITERIA_READ	Enables viewing a DHCP Criteria object and all of its properties. Enables the selection of DHCP Criteria objects.
PRIV_DHCP_CRITERIA_UPDATE	Enables modifying any property of a DHCP Criteria object.
PRIV_DHCP_CRITERIA_DELETE	Enables deleting a DHCP Criteria object from the system.
Files	
PRIV_FILE_GENERIC_CREATE	Enables adding generic files into the system.
PRIV_FILE_GENERIC_READ	Enables viewing, searching, selecting, and exporting properties and data of generic files.
PRIV_FILE_GENERIC_UPDATE	Enables replacing a generic file.
PRIV_FILE_GENERIC_DELETE	Enables deleting a generic from the system.

Table 13-2 **Default Privileges (continued)**

Privileges	Description
PRIV_FILE_CABLELABS_CONF_SCRIPT_CREATE	Enables adding CableLabs script file into the system.
PRIV_FILE_CABLELABS_CONF_SCRIPT_READ	Enables viewing, searching, selecting, and exporting properties and data of CableLabs script file.
PRIV_FILE_CABLELABS_CONF_SCRIPT_UPDATE	Enables replacing a CableLabs script file.
PRIV_FILE_CABLELABS_CONF_SCRIPT_DELETE	Enables deleting a CableLabs script file from the system.
PRIV_FILE_CABLELABS_CONF_TMPL_CREATE	Enables adding CableLabs template file into the system.
PRIV_FILE_CABLELABS_CONF_TMPL_READ	Enables viewing, searching, selecting, and exporting properties and data of CableLabs template file.
PRIV_FILE_CABLELABS_CONF_TMPL_UPDATE	Enables replacing a CableLabs template file.
PRIV_FILE_CABLELABS_CONF_TMPL_DELETE	Enables deleting a CableLabs script template from the system.
PRIV_FILE_CABLELABS_STATIC_CONF_CREATE	Enables adding CableLabs static config file into the system.
PRIV_FILE_CABLELABS_STATIC_CONF_READ	Enables viewing, searching, selecting, and exporting properties and data of CableLabs static config file.
PRIV_FILE_CABLELABS_STATIC_CONF_UPDATE	Enables replacing a CableLabs static script config file.
PRIV_FILE_CABLELABS_STATIC_CONF_DELETE	Enables deleting a CableLabs static script config file from the system.
PRIV_FILE_DCFG_CREATE	Enables adding a Dynamic Configuration Filename Generation (DCFG) script into the system.
PRIV_FILE_DCFG_READ	Enables viewing, searching, selecting, and exporting properties and data of DCFG script.
PRIV_FILE_DCFG_UPDATE	Enables replacing a DCFG script.
PRIV_FILE_DCFG_DELETE	Enables deleting a DCFG script from the system.
PRIV_FILE_FIRMWARE_CREATE	Enables adding a firmware image into the system.
PRIV_FILE_FIRMWARE_READ	Enables viewing, searching, selecting, and exporting properties and data of firmware image.
PRIV_FILE_FIRMWARE_UPDATE	Enables replacing firmware image.
PRIV_FILE_FIRMWARE_DELETE	Enables deleting a firmware image from the system.
PRIV_FILE_JAR_CREATE	Enables adding a JAR file into the system.
PRIV_FILE_JAR_READ	Enables viewing, searching, selecting, and exporting properties and data of a JAR file.
PRIV_FILE_JAR_UPDATE	Enables replacing a JAR file.
PRIV_FILE_JAR_DELETE	Enables deleting a JAR file.

Table 13-2 Default Privileges (continued)

Privileges	Description
PRIV_FILE_MIB_CREATE	Enables adding a MIB file into the system.
PRIV_FILE_MIB_READ	Enables viewing, searching, selecting, and exporting properties and data of a MIB file.
PRIV_FILE_MIB_UPDATE	Enables replacing a MIB file.
PRIV_FILE_MIB_DELETE	Enables deleting a MIB file from the system.
Devices, DeviceType	
PRIV_DEVICE_CREATE	Enables adding a new device into the system.
PRIV_DEVICE_READ	Enables viewing device properties, searching for devices, and selecting devices. Also permits the use of show device-config in the DPE CLI
PRIV_DEVICE_UPDATE	Enables changing any property of a device object.
PRIV_DEVICE_DELETE	Enables deleting a device from the system.
PRIV_DEVICE_REGEN	Enables invoking regeneration of the device configuration.
PRIV_DEVICE_OPERATION	Enables operations on this device.
RDU	
PRIV_RDU_READ	Enables viewing RDU status.
PRIV_RDU_EVENT	Required to register for RDU events.
Node Type and Node	
PRIV_GROUP_CREATE	Enables creating a group.
PRIV_GROUP_READ	Enables viewing and selecting all groups.
PRIV_GROUP_UPDATE	Enables updating a group.
PRIV_GROUP_DELETE	Enables deleting a group.
LicenseKey	
PRIV_LICENSE	Enables adding, updating, and deleting all the license keys. Viewing license is not protected.
Publishing	
PRIV_PUBLISHING	Enables all, read, and update.
CRS	
PRIV_CRS_CREATE	Enables creating CRS
PRIV_CRS_READ	Enables viewing and searching of the requests queued by CRS.
PRIV_CRS_UPDATE	Enables a user to pause or resume a CRS job
PRIV_CRS_DELETE	Enables a user to delete a CRS job.
ProvGroup	
PRIV_PROVGROUP_READ	Enables viewing Provisioning Group properties
PRIV_PROVGROUP_UPDATE	Enables updating ProvGroup properties
PRIV_PROVGROUP_DELETE	Enables deleting a provisioning group from Prime Cable Provisioning.
DPE	

Table 13-2 *Default Privileges (continued)*


Privileges	Description
PRIV_DPE_READ	Enables viewing DPE status. For DPE CLI, permits Disabled Mode.
PRIV_DPE_UPDATE	Permits DPE CLI Enabled Mode
PRIV_DPE_DELETE	Permits deleting a DPE.
PRIV_DPE_SECURITY	All security related admin operations including changing dpe admin password and configuring authentication.
NR	
PRIV_NR_READ	Enables viewing CNR status.
PRIV_NR_UPDATE	Enables updating NR extension point
PRIV_NR_DELETE	Enables deleting a CNR from Prime Cable Provisioning.
User	
PRIV_USER_CREATE	Enables adding users.
PRIV_USER_READ	Enables viewing or searching users.
PRIV_USER_UPDATE	Enables changing user properties.
PRIV_USER_DELETE	Enables deleting users.
PRIV_USER_SECURITY	Enables assigning roles, user group to users. Also allows the setting of a user's number of allowed sessions.
	 Note PRIV_USER_SECURITY is a powerful privilege and must be used with caution.
Role	
PRIV_ROLE_CREATE	Enables adding roles.
PRIV_ROLE_READ	Enables reading or search roles and privileges.
PRIV_ROLE_UPDATE	Enables changing role properties.
PRIV_ROLE_DELETE	Enables deleting roles.
Domain	
PRIV_DOMAIN_CREATE	Enables adding domains.
PRIV_DOMAIN_READ	Enables viewing and selecting operations on domains.
PRIV_DOMAIN_UPDATE	Enables updating operations.
PRIV_DOMAIN_DELETE	Enables deleting operations.
Custom Property	
PRIV_PROPERTY_CREATE	Enables adding a new customer property.
PRIV_PROPERTY_READ	Enables viewing of RDU Defaults and custom property.
PRIV_PROPERTY_UPDATE	Enables modifying a custom property.
PRIV_PROPERTY_DELETE	Enables deleting a custom property.
System Defaults	
PRIV_SYSDEF_READ	Enables viewing system properties e.g. GetRDUDefaults.

Table 13-2 *Default Privileges (continued)*

Privileges	Description
PRIV_SYSDEF_UPDATE	Enables modifying system properties e.g. ChangeRDUDefaults
Logging	
PRIV_LOGGING	Setting logging/debug levels. Viewing logs.
PRIV_AUDIT_LOGGING	Enables viewing Audit logs.
User Group	
PRIV_USERGROUP_CREATE	Enables create operations
PRIV_USERGROUP_READ	Enables all read and selection operations
PRIV_USERGROUP_UPDATE	Enables update operations
PRIV_USERGROUP_DELETE	Enables delete operations


Default Roles

Table 13-3 lists the default roles in Prime Cable Provisioning.

Table 13-3 *Default Roles*

Role Name	Description
Admin	Admin is the super administrator and has all capabilities, including modifying device property value.
COSAdmin	COS admin can add, delete, update, search, and export all COS and their properties.
DeviceAdmin	Device admin can add, delete, search, relate, un-relate, regenerate, and device operation privileges on all available devices. DeviceAdmin also has permissions to read and modify all attributes and properties.
DHCPAdmin	DHCP admin can add, delete, update, and search all DHCP Criteria and their properties.
FileAdmin	File admin can add, delete, update, search, and export all files and their properties.
ProvGroupAdmin	Provisioning Group admin can view and update Provisioning Group properties. ProvGroupAdmin can also view, update, and delete servers of a Provisioning Group as well as their properties. This role permits all operations on the DPE CLI.
RDUAdmin	RDUAdmin can view, add, and delete all RDU default and system properties. This role can read, add, and delete permissions on license, read and modify permissions on all available publishing plug-in, manage CRS, and manage MIBs.
ReadOnly	ReadOnly has read permission on all available resources, except user, user group, domain, and roles.
ReadWrite	ReadWrite has create, read, modify, and delete permission on all available resources except user, user group, domain, and roles.

Table 13-3 *Default Roles (continued)*

Role Name	Description
ReadOnly and ReadWrite roles are provided for backward compatibility only. These roles do not have access to any security related features like user, user-group, domain, role, and user-group-mapping that are introduced in Prime Cable Provisioning 5.0.	
 Note If instance level is enabled, ReadWrite will not add any resource which supports instance level check.	
SecurityAdmin	SecurityAdmin has add, delete, relate, un-relate permissions on all available groups and modify permission on all attributes.
UserAdmin	UserAdmin can add, delete, modify, read, relate, un-relate all available users and properties for user.

Default User Groups

Table 13-4 lists the default user groups in Prime Cable Provisioning.

Table 13-4 *Default User Groups*

User Group	Description	Role
Administrators	This user group consists super users.	Admin

Default Domains

Table 13-5 lists the default domains in Prime Cable Provisioning.

Table 13-5 *Default Domains*

Domain	Members
RootDomain	All current objects

Default Users

Table 13-6 lists the default user in Prime Cable Provisioning.

Table 13-6 *Default Users*

User	Assigned Role	Assigned User Group	Assigned Domain
admin	Admin	Administrators	RootDomain