BlackBerry Enterprise Server

BlackBerry Administration Service Roles and Permissions

Version: 5.0
Service Pack: 4

Reference Guide

BlackBerry

Published: 2013-03-28
SWD-20130328143914668

Contents

Administrative roles and permissions

1

You create roles for administrator accounts or assign preconfigured roles to administrator accounts so that you can specify what tasks an administrator can perform on the BlackBerry Enterprise Server.

You can specify the actions that administrators can perform by changing the permission that you assign to administrative roles. Permissions specify the information that administrators can view and the tasks that they can perform using the BlackBerry Administration Service. Each action that you perform in the BlackBerry Administration Service is associated with a specific permission. You can specify the actions that administrators can perform by changing the permission that you assign to administrative roles. For more information about performing specific tasks that are associated with the permissions, see the *BlackBerry Enterprise Server Administration Guide*. Roles do not apply to tasks that an administrator can perform using the BlackBerry Configuration Panel.

You can assign multiple roles to administrator accounts. If you assign multiple roles to an administrator account, the administrator is assigned all the permissions that are turned on for each of the roles.

You can also assign roles to groups and add administrator accounts to groups. This allows you to specify administrative role permissions at a group level instead of at an individual level. If the group contains BlackBerry device users, the roles are also assigned to the users and the users become administrators.

Creating roles

2

You can create roles for administrator accounts so that administrators in your organization can perform specific tasks and view specific information in the BlackBerry Administration Service and BlackBerry Web Desktop Manager. For example, you can create a role that has all permissions turned off by default and you can customize the role by turning on specific permissions. You can also create a role that is based on a preconfigured role and customize the role that you create.

Preconfigured roles

3

The BlackBerry Enterprise Server installation process includes preconfigured administrative roles. You can use the preconfigured roles in your organization's environment instead of creating customized roles.

The preconfigured roles make sure that users that do not have specific administrative permissions cannot escalate their permissions, for example, junior helpdesk administrators cannot escalate their roles to senior helpdesk roles. You can configure additional permissions in the preconfigured roles or turn off any of the permissions.

Preconfigured role	Description of the preconfigured role
Security	The Security role allows administrators to have complete access to all components of the BlackBerry Administration Service.
Enterprise	The Enterprise role allows administrators to have complete access to all components of the BlackBerry Administration Service, but they cannot create or change administrative roles.
Senior Helpdesk	The Senior Helpdesk role allows administrators to perform common administrative tasks such as creating and deleting user accounts, creating and administering groups and assigning BlackBerry devices to user accounts.
Junior Helpdesk	The Junior Helpdesk role allows administrators to perform basic administrative tasks such as adding users to groups and assigning devices to user accounts.
Server Only	The Server only role allows administrators to configure and maintain the BlackBerry Enterprise Server environment. The Server only role only has access to the Servers and Components section of the BlackBerry Administration Service.
User Only	The User only role only allows administrators to manage user accounts and the majority of tasks required to manage user accounts and the associated devices. This role does not allow administrators to configure and maintain the BlackBerry Enterprise Server environment.
Monitoring System	The Monitoring System role allows administrators to perform all actions in the BlackBerry Monitoring Service console, and view user accounts and the associated devices using the BlackBerry Administration Service.
Monitoring View	The Monitoring View role allows administrators to view the BlackBerry solution topology, including servers and BlackBerry Enterprise Server components, but they cannot perform any actions using the BlackBerry Administration Service.

Administrative permissions for preconfigured roles

4

Administrative permissions specify the information that administrators can view and the tasks that they can perform using the BlackBerry Administration Service and BlackBerry Monitoring Service. Each preconfigured role contains multiple permissions that are turned on.

Permission name	Security role	Enterprise role	Senior Helpdesk role	Junior Helpdesk role	Server only role	User only role
Create a group	X	X	X			X
Delete a group	X	X				X
View a group (across Group)	X	X	X	X		X
Edit a group (across Group)	X	X	X	X		X
Create a user	X	X	X			X
Delete a user	X	X	X			X
View a user (across Group)	X	X	X	X		X
Edit a user (across Group)	X	X	X	X		X
View a device (across Group)	X	X	X	X		X
Edit a device (across Group)	X	X	X	X		X
View device activation settings	X	X				X
Edit device activation settings	X	X				X
Create an IT policy	X	X				X
Delete an IT policy	X	X				X
View an IT policy	X	X	X	X		X
Edit an IT policy	X	X				X

Permission name	Security role	Enterprise role	Senior Helpdesk role	Junior Helpdesk role	Server only role	User only role
Import an IT policy	X	X				X
Export an IT policy	X	X				X
Create a user-defined IT policy template	X	X				X
Delete a user-defined IT policy template	X	X				X
Edit a user-defined IT policy template	X	X				X
Import an IT policy template	X	X				X
Resend data to devices	X	X	X			
Create a software configuration	X	X				X
View a software configuration	X	X	X	X		X
Edit a software configuration	X	X				X
Delete a software configuration	X	X				X
View BlackBerry Administration Service software management	X	X			X	
Edit BlackBerry Administration Service software management	X	X				
Create an application	X	X				X
View an application	X	X	X	X		X
Edit an application	X	X				X
Delete an application	X	X				X
Create an administrator user	X					
Specify an activation password	X	X	X	X		X

Permission name	Security role	Enterprise role	Senior Helpdesk role	Junior Helpdesk role	Server only role	User only role
Generate an activation email	X	X	X	X		X
Assign the current device to a user	X	X	X	X		X
Turn off and on external services	X	X	X			X
Clear activation password	X	X	X	X		X
Clear synchronization backup data	X	X	X			X
Clear user statistics	X	X	X	X		X
Export statistics	X	X				X
Reset user field mapping	X	X	X			X
Turn on redirection	X	X	X			X
Turn off redirection	X	X	X			X
Refresh available user list from company directory	X	X				X
Add User from Company Directory	X	X	X			X
Synchronize GroupWise System Address Book	X	X			X	
Clear and synchronize GroupWise System Address Book	X	X			X	
View a server	X	X			X	
Edit a server	X	X			X	
View a component	X	X			X	
Edit a component	X	X			X	
View an instance	X	X			X	
Edit an instance	X	X			X	

Permission name	Security role	Enterprise role	Senior Helpdesk role	Junior Helpdesk role	Server only role	User only role
Change the status of an instance	X	X			X	
Edit an instance relationship	X	X			X	
View a job	X	X				X
Edit a job	X	X				X
Manage deployment job tasks	X	X				X
Change the status of a job task	X	X				X
Update peer-to-peer encryption key	X	X			X	
View job distribution settings	X	X				X
Edit job distribution settings	X	X				X
Delete an instance	X	X			X	
Edit license keys	X	X			X	
View license keys	X	X			X	
Manually fail a job	X	X				X
Clear instance statistics	X	X			X	
View push rules for the BlackBerry MDS Connection Service	X	X	X	X	X	X
View pull rules for the BlackBerry MDS Connection Service	X	X	X	X		X
Send message (across Group)	X	X	X	X		X
Create a role	X					
Delete a role	X					
View a role	X	X	X	X		X

Permission name	Security role	Enterprise role	Senior Helpdesk role	Junior Helpdesk role	Server only role	User only role
Edit a role	X					
Add or remove role	X					
Import or export groups within roles	X					
View BlackBerry Monitoring Service information	X					
Edit BlackBerry Monitoring Service settings	X					
Import new users	X	X				X
Import or export users	X	X	X			X
Import user updates	X	X				X
Import or export email message filters for a user	X	X				X
Export asset summary data	X	X				X
Add or remove to user configuration	X	X	X			X
Delete all device data and remove device	X	X	X	X		X
Delete only the organization data and remove device	X	X	X	X		X

User and device permissions

Basic permissions

Create a group

This permission specifies whether you can create a group in the BlackBerry Administration Service. You can create user groups and assign user accounts to groups based on specific criteria such as BlackBerry device user location, organizational group, or BlackBerry device model. User accounts and administrator accounts that are part of a user group can exist on multiple BlackBerry Enterprise Server instances in the BlackBerry Domain.

By default, the Create a group permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

Delete a group

This permission specifies whether you can delete a group in the BlackBerry Administration Service.

By default, the Delete a group permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

View a group

This permission specifies whether you can view a group and information about the group in the BlackBerry Administration Service. For example, you can view a group and the child groups that are assigned to the group.

By default, the View a group permission is enabled for the following preconfigured roles:

- Security

- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

Edit a group

This permission specifies whether you can cha.nge the properties of a group in the BlackBerry Administration Service. For example, you can reduce the time that you spend managing user accounts by adding similar user accounts to a group, and assigning shared properties, such as software configurations or IT policies, to the group. Properties that you assign to a group are assigned to all user accounts in the group.

By default, the Edit a group permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

Create a user

This permission specifies whether you can add a user account to the BlackBerry Enterprise Server, assign a BlackBerry device to a user account, and activate the device. The user account must exist on your organization's messaging server.

By default, the Create a user permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

Delete a user

This permission specifies whether you can delete a user account using the BlackBerry Administration Service.

By default, the Delete a user permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

View a user

This permission specifies whether you can view a user account in the BlackBerry Administration Service. You can also view the email message filters and mail information that are assigned to the user account if this permission is turned on.

By default, the View a user permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only
- Monitoring System
- Monitoring View

Edit a user

This permission specifies whether you can change the properties of a user account in the BlackBerry Administration Service. For example, you can assign a software configuration to a user account, or create an email filter that applies to a specific user account.

By default, the Edit a user permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

View a device

This permission specifies whether you can view information about a BlackBerry device using the BlackBerry Administration Service. For example, you can view the user account and PIN number that is associated with a device.

By default, the View a device permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

- Monitoring System
- Monitoring View

Edit a device

This permission specifies whether you can change the settings on BlackBerry devices. For example, you can set owner information and lock a device. You cannot delete all device data using the Edit a device permission, you require either the Delete all device data and remove device permission or Delete only the organization data and remove device permission to delete all device data.

By default, the Edit a device permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

View device activation settings

This permission specifies whether you can view the activation settings for a BlackBerry device. For example, you can view the password activation settings and initialization message.

By default, the View device activation settings are enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Edit device activation settings

This permission specifies whether you can change the activation settings for a BlackBerry device. For example, you can specify the password activation settings and initialization message.

By default, the Edit device activation settings permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Create an IT policy

This permission specifies whether you can create an IT policy using the BlackBerry Administration Service. You can use IT policy rules to customize and control the actions that you can use the BlackBerry Enterprise Server can perform. For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

By default, the Create an IT policy permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Delete an IT policy

This permission specifies whether you can delete an IT policy using the BlackBerry Administration Service. If you delete an IT policy that you assigned to the user account or group, the Default IT policy will be re-assigned to the user account if no other IT policies are applied to that user account. The Default IT policy includes all the standard IT policy rules that are set on the BlackBerry Enterprise Server. For more information see the *BlackBerry Enterprise Server Policy Reference Guide*.

By default, the Delete an IT policy permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

View an IT policy

This permission specifies whether you can view an IT policy using the BlackBerry Administration Service.

By default, the View an IT policy permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

Edit an IT Policy

Description

This permission specifies whether you can change an IT policy using the BlackBerry Administration Service. You can use IT policy rules to customize and control the actions that you can use the BlackBerry Enterprise Solution can perform. For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

By default, the Edit an IT Policy permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Import an IT policy

This permission specifies whether you can import a list of IT policies using the BlackBerry Administration Service. Before you can import an IT policy, you must first export IT policy data from a different BlackBerry Domain. For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

By default, the Import an IT policy permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Export an IT policy

This permission specifies whether you can export a list of IT policies to a data file using the BlackBerry Administration Service. You can import the data file at a later time to another BlackBerry Domain.

By default, the Export an IT policy permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Create a user-defined IT policy template

This permission specifies whether you can create new IT policy rules to control the applications that your organization configures for BlackBerry devices. After you create an IT policy rule, it is automatically added to all existing IT policies. You can assign a value to it in a new or existing IT policy. For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

By default, the Create a user-defined IT policy is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Delete a user-defined IT policy template

This permission specifies whether you can delete IT policy rules that are created by your organization to control applications running on BlackBerry devices.

By default, the Delete a user-defined IT policy template is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Resend data to devices

This permission specifies whether you can resend data to a BlackBerry device using the BlackBerry Administration Service. For example, you can resend service books or IT policy data to a device.

By default, the Resend data to devices is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

Edit a user-defined IT policy template

This permission specifies whether you can change IT policy rules that were created by your organization to control applications that are running on BlackBerry devices.

By default, the Edit a user-defined IT policy template is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Import an IT policy template

This permission specifies whether you can import IT policy rules that were created by your organization from a different BlackBerry Domain.

By default, the Import an IT policy template permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Create a software configuration

Description

This permission specifies whether you can create a software configuration, which you can assign to a group, multiple user accounts, or a single user account. After you assign a software configuration, you can change the software configuration settings to manage the BlackBerry Java Applications, BlackBerry Device Software, and standard application settings on devices.

By default, the Create a software configuration permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

View a software configuration

This permission specifies whether you can view software configurations in the BlackBerry Administration Service.

By default, the View a software configuration permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

Edit a software configuration

This permission specifies whether you can change software configurations that you want to install on, update on, or remove from BlackBerry devices. You can configure settings in the BlackBerry Administration Service to control how the BlackBerry Administration Service sends BlackBerry Java Applications, BlackBerry Device Software, and standard application settings in software configurations to devices.

By default, the Edit a software configuratio is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Delete a software configuration

This permission specifies whether you can delete software configurations from the BlackBerry Administration Service.

By default, the Delete a software configuration permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Create an application

This permission specifies whether you can create a BlackBerry Java Application that you can install on BlackBerry devices. The BlackBerry Administration Service includes a standard application control policy for BlackBerry Java Applications that you can use to classify BlackBerry Java Applications as required, optional, or not permitted.

By default, the Create an application permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

View an application

This permission specifies whether you can view a BlackBerry Java Application in the BlackBerry Administration Service.

By default, the View an application permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

Edit an application

This permission specifies whether you can update BlackBerry Java Applications that you can install on BlackBerry devices. The BlackBerry Administration Service includes a standard application control policy for BlackBerry Java Application that you can use to classify BlackBerry Java Applications as required, optional, or not permitted.

By default, the Edit an application permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Delete an application

This permission specifies whether you can remove a BlackBerry Java Application from a device using the BlackBerry Administration Service.

By default, the Delete an application permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Create an administrator user

This permission specifies whether you can create an administrator account in the BlackBerry Administration Service. You create an administrator account so that administrators can log in to the BlackBerry Administration Service and manage the BlackBerry Enterprise Server. When you create an administrator account, you assign the account to one or more administrator roles. The roles control the actions that an administrator can perform in the BlackBerry Administration Service.

By default, the Create an administrator user permission is enabled for the Security role.

Add or remove to user configuration

This permission specifies whether you can add software configurations to or remove software configurations from user accounts and groups. You can add or remove the following objects from user accounts or groups:

- push and pull rules
- software configurations
- Wi-Fi profiles
- VPN profiles
- IT policies

By default, the Add or remove to user configuration permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

Export asset summary data

This permission specifies whether you can generate a list of all BlackBerry devices that are activated in your organization's environment and the data that is associated with the devices. Examples of data might include the PIN, device model, platform version, phone number, serial number, wireless service provider, and so on.

By default, the Export asset summary data permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Import or export users

This permission specifies whether you can export or import a list of user accounts from a BlackBerry Enterprise Server to a .csv file. The .csv file contains information about the user accounts, such as the user ID, display name, PIN, and email address and so on. You can export and then import the list of user accounts to another BlackBerry Enterprise Server.

By default, the Import or export users permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

Export statistics

This permission specifies whether you can export user-account settings and data that are wirelessly backed up from BlackBerry devices to a specific BlackBerry Enterprise Server automatically. By default, user-account settings and data are wirelessly backed up to the BlackBerry Enterprise Server automatically.

By default, the Export statistics permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Import user updates

This permission specifies whether you can import user updates to the BlackBerry Enterprise Server.

By default, the Import user updates permission is enabled for the following preconfigured roles:

- Security

- Enterprise
- User only

Assign the current device to a user

This permission specifies whether you can assign and activate BlackBerry devices before you distribute them to BlackBerry device users. You can determine whether you can assign and activate devices by connecting the devices to a computer and logging into the BlackBerry Administration Service.

By default, the Assign the current device to a user permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Juniopr Helpdesk
- User only

Delete all device data and remove device

This permission specifies whether you can permanently delete all BlackBerry device user information and application data from a BlackBerry device. You can perform the following actions:

- specify a delay, in hours, that must occur before the device starts to delete user information and application data
- require that the device return to its default settings when it receives this command
- specify whether to permit the user to stop permanently deleting data from the device and make the device unavailable during the delay period

By default, the Delete all device data and remove device permissions is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

Delete only the organization data and remove device

This permission specifies whether you can permanently delete all application data that is specific to your organization that the BlackBerry device stores but leave personal data on the device.

By default, the Delete only the organization data and remove device permissions is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

BlackBerry Enterprise Server permissions

Specify an activation password

This permission specifies whether you can specify an activation password for the user account.

By default, the Specify an activation password is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

Turn off and on external services

Turn off BlackBerry services that the BlackBerry MDS Connection Service, BlackBerry Collaboration Service, and BlackBerry MVS provide. For example, you can prevent BlackBerry device users that you associate with a BlackBerry Enterprise Server from browsing the intranet or Internet, running applications that communicate with application servers and content servers, sending or receiving instant messages, or making calls using VoIP.

By default, the Turn off and on external services permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

Generate an activation email

This permission specifies whether you can create and send an activation email to BlackBerry device users when they activate BlackBerry devices.

By default, the Generate an activation email permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

Synchronization permissions

Clear synchronization backup data

This permission specifies whether you can delete user-account settings and data from BlackBerry devices. By default, user-account settings and data are wirelessly backed up to the BlackBerry Enterprise Server automatically.

By default, the Clear synchronization backup data permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

Email permissions

Clear user statistics

This permission specifies whether you can clear the statistics that the BlackBerry Messaging Agent writes to each user's Microsoft Exchange mailbox when it processes email messages. By default, to reduce the workload on the Microsoft Exchange Server, the BlackBerry Messaging Agent 5.0 SP2 or later does not write statistics to each user's Microsoft Exchange mailbox when it processes email messages. This permission only applies to the BlackBerry Enterprise Server for Microsoft Exchange.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

Reset user field mapping

This permission specifies whether you can reset the contact information fields on BlackBerry devices. For example, you can reset the global and field mappings that BlackBerry device users specify in the contact information on their computers to their devices.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

Turn on redirection

This permission specifies whether you can specify message forwarding settings for user accounts and groups that are associated with the BlackBerry Enterprise Server. The settings control how the BlackBerry Enterprise Server forwards email messages from BlackBerry device users' email applications to their BlackBerry devices.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

Turn off redirection

This permission specifies whether you can stop the BlackBerry Enterprise Server from forwarding email messages to user accounts. When you turn off message forwarding for user accounts, BlackBerry device users can send email messages from their BlackBerry devices, but cannot receive email messages.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

Add user from company directory

This permission specifies whether you can create a user account if the user account is not synchronized with the contact list in the BlackBerry Configuration Database.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- User only

Import new users

This permission specifies whether you can import a list of user accounts to a BlackBerry Enterprise Server. You can add multiple user accounts to a BlackBerry Enterprise Server by importing a .csv file that contains a list of user accounts and the information that you need to activate the user accounts on a BlackBerry Enterprise Server.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Refresh available user list from company directory

This permission specifies whether you can update and refresh the contact list in the BlackBerry Configuration Database so that you can include any organizational changes or updates in the contact list in the BlackBerry Administration Service.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Import or export email message filters for a user

This permission specifies whether you can copy existing email filters for a specific user account and apply them to other user accounts by exporting the email message as a .xml file. You can then import the .xml file so that you can use it with another instance of the BlackBerry Enterprise Server.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Topology permissions

Basic permissions

View a server

This permission specifies whether you can view the BlackBerry Enterprise Server and BlackBerry Enterprise Server components in your organization's environment using the BlackBerry Administration Service.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Edit a server

This permission specifies whether you can change the settings and options for the BlackBerry Enterprise Server components.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Edit a component

This permission specifies whether you can view and manage BlackBerry Enterprise Server components using the server view or component view in the BlackBerry Administration Service.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

View a component

This permission specifies whether you can view BlackBerry Enterprise Server components using the server view or component view in the BlackBerry Administration Service.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

View an instance

This permission specifies whether you can view a BlackBerry Enterprise Server instance in a BlackBerry Domain.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Edit an instance

This permission specifies whether you can use the BlackBerry Administration Service to change the BlackBerry Enterprise Server instance and remote BlackBerry Enterprise Server components that use a BlackBerry Configuration Database.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Change the status of an instance

This permission specifies whether you can manually change the availability state and failover status of a BlackBerry Enterprise Server instance.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Edit an instance relationship

This permission specifies whether you can identify which BlackBerry Enterprise Server is the primary BlackBerry Enterprise Server instance and which BlackBerry Enterprise Server is the standby instance. This permisstion also permits you to add or remove:

- BlackBerry MDS Connection Service or BlackBerry Collaboration Service instance to a BlackBerry Enterprise Server
- BlackBerry Attachment Connector to a BlackBerry Attachment Service instance

For more information about high availability, see the *BlackBerry Enterprise Server Administration Guide*.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

View a job

This permission specifies whether you can view the status of a deployment job. A deployment job consists of multiple tasks that manage the delivery of an object (for example, a BlackBerry Java Application, an application control policy, or an IT policy) to BlackBerry devices.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Edit a job

This permission specifies whether you can change a job to control how the BlackBerry Administration Service processes a job task. A job consists of multiple tasks. Each task delivers a specific object or setting to a BlackBerry device.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Manage deployment job tasks

This permission specifies whether you can view deployment job tasks that will be delivered to a user's BlackBerry device. A deployment job rconsists of multiple tasks that manage the delivery of an object (for example, a BlackBerry Java Application, an access control policy, or an IT policy) to a BlackBerry device.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Edit default distribution settings for a job

This permission specifies whether you can change the default settings for a deployment job to control how the BlackBerry Administration Service processes jobs. A deployment job consists of multiple tasks that manage the delivery of an object (for example, a BlackBerry Java Application, an access control policy, or an IT policy) to BlackBerry devices.

If you change the default settings for a job, your organization's environment might experience a performance impact.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Update peer-to-peer encryption key

This permission specifies whether you can generate a PIN encryption key. For example, you should generate a new PIN encryption key if you know that your organization's current PIN encryption key is compromised. You can generate a new PIN encryption key that is stored on and known only to BlackBerry devices in your organization's environment.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Manage deployment job tasks

This permission specifies whether you can change the default settings for when a deployment job task is delivered to a BlackBerry device. A deployment job consists of multiple tasks that manage the delivery of an object (for example, a BlackBerry Java Application, an access control policy, or an IT policy) to a BlackBerry device.

- Security

- Enterprise
- Server only

Change the status of a job task

This permission specifies whether you can change the status of a specific task in an deployment job. A job consists of multiple tasks and each task delivers a specific object or setting to a BlackBerry device. If the BlackBerry MDS Connection Service did not complete a request to install, update, or remove an application, you can cancel the job task request.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Delete an instance

This permission specifies whether you can delete a BlackBerry Enterprise Server instance from the BlackBerry Administration Service.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Edit license keys

This permission specifies whether you can manage BlackBerry CAL keys to control how many user accounts can exist on a BlackBerry Enterprise Server at the same time. You can add, copy or delete BlackBerry CAL keys. For example, to help transfer BlackBerry CAL keys to computers in other BlackBerry Domain instances or troubleshoot BlackBerry CAL key issues, you can copy the BlackBerry CAL keys from the BlackBerry Administration Service to a text file.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

View license keys

This permission specifies whether you can view BlackBerry CAL keys. BlackBerry CAL keys control how many user accounts can exist on a BlackBerry Enterprise Server at the same time.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Email permissions

Clear instance statistics

This permission specifies whether you can clear the statistics on an email instance. Each email instance maintains statistics about the number of forwarded email message, sent email messages, expired email messages, filtered email messages, failed email messages and pending data packets.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

Import or export users

This permission specifies whether you can import or export a list of user accounts from a BlackBerry Enterprise Server to a csv file. The .csv file contains information about the user accounts, such as user IDs, display names, PINs, email addresses, and so on. You can export the list of user accounts and then import the list to another BlackBerry Enterprise Server.

- Security
- Enterprise
- Server only

MDS Connection Service permissions

View rules for the BlackBerry MDS Connection Service

This permission specifies whether you can view push rules for the BlackBerry MDS Connection Service and verify that the central push server appears in the list of BlackBerry MDS Connection Service instances that are available to the BlackBerry MDS Integration Service. You can configure BlackBerry Enterprise Server instances in your organization's BlackBerry Domain to use the BlackBerry MDS Connection Service instances that you specify as central push servers. By default, a BlackBerry MDS Connection Service sends push requests from server-side push applications to applications on BlackBerry devices.

Enabled for the following preconfigured roles:

- Security
- Enterprise
- Server only

BlackBerry Administration Service setup permissions

Basic permissions

Send message

This permission specifies whether you can send email messages to user accounts in a group, multiple user accounts, or a single user account.

By default, the Send message permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

Create a role

This permission specifies whether you can create a specific role for an administrator account or group. By default, you can create a role that has all permissions turned off so that you can add permissions to it, or you can create a role that is based on a preconfigured role and configure it.

By default, the Create a role permission is enabled for the Security role.

Delete a role

This permission specifies whether you can delete a role from the BlackBerry Administration Service.

By default, the Delete a role permission is enabled for the Security role.

View a role

This permission specifies whether you can view a role and the permissions that is associated with the role.

By default, the View a role permission is enabled for the following preconfigured roles:

- Security
- Enterprise
- Senior Helpdesk
- Junior Helpdesk
- User only

Edit a role

This permission specifies whether you can change a role and the permissions that are associated with the role. You can assign multiple roles to administrator accounts. If you assign multiple roles to an administrator account, the administrator is assigned all the permissions that are turned on for all the roles. You can also assign roles to groups and add administrator accounts to the groups. If you add an administrator account to one or more groups, you can manage role permissions at a group level instead of at an individual level.

By default, the Edit a role permission is enabled for the Security role.

Add or remove a role

This permission specifies whether you can add a role, or remove a role that was assigned to a group. When you add administrator accounts to a group that has a role assigned to it, you can manage the administrators at a group level instead of at an individual level.

By default, the Add or remove a role permission is enabled for the Security role.

View BlackBerry Administration Service software management

This permission specifies whether you can view the information about BlackBerry Device Software updates that your organization configured. For example, you can view the BlackBerry Administration Service application shared network drive and view whether you can manage the BlackBerry Software deployment in the BlackBerry Administration Service.

By default, the View BlackBerry Administration Service software management role is enabled for the following preconfigured roles:

- Security
- Enterprise
- User only

Edit BlackBerry Administration Service software management

This permission specifies whether you can use the BlackBerry Administration Service to manage BlackBerry Device Software updates. For example, you can specify the BlackBerry Administration Service application shared network drive and select whether you can manage the BlackBerry Software deployment using the BlackBerry Administration Service.

By default, the Edit BlackBerry Administration Service software management permission is enabled for the following preconfigured roles:

- Security
- Enterprise

Import or export groups within roles

This permission specifies whether you can import or export a list of administrator accounts that are associated with a specific role at the group level. You can export a list of groups that are associated with a specific role to a different group or import a list of groups to a different group.

By default, the Import or export groups within roles permission is enabled for the Security role.

Monitoring permisssions

View BlackBerry Monitoring Service information

This permission specifies whether you can use the BlackBerry Monitoring Service to monitor the BlackBerry Enterprise Server in your organization's environment to view the activity of the BlackBerry device users that are associated with the BlackBerry Enterprise Server.

By default, the View BlackBerry Monitoring Service information permission is enabled for the following preconfigured roles:

- Security
- Monitoring System
- Monitoring View

Edit BlackBerry Monitoring Service settings

This permission specifies whether you can use the BlackBerry Monitoring Service to monitor and troubleshoot issues with a BlackBerry Enterprise Server in your organization's environment. This permission also specifies whether you can monitor the activity of the BlackBerry device users that are associated with a BlackBerry Enterprise Server.

By default, the Edit BlackBerry Monitoring Service settings permission is enabled for the following preconfigured roles:

- Security
- Monitoring System

Provide feedback

5

To provide feedback on this deliverable, visit www.blackberry.com/docsfeedback.

Legal notice

6

PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF RIM OR ANY AFFILIATES OF RIM HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with RIM's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with RIM's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by RIM and RIM assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

Certain features outlined in this documentation require a minimum version of BlackBerry Enterprise Server, BlackBerry Desktop Software, and/or BlackBerry Device Software.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR

WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

Certain features outlined in this documentation might require additional development or Third Party Products and Services for access to corporate applications.

This product includes software developed by the Apache Software Foundation (www.apache.org/) and/or is licensed pursuant to one of the licenses listed at (www.apache.org/licenses/). For more information, see the NOTICE.txt file included with the software.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada