BlackBerry Enterprise Server for Microsoft Exchange

Version: 5.0
Service Pack: 3

Administration Guide

BlackBerry®

Published: 2012-09-24
SWD-20120924140022907

Contents

Overview: BlackBerry Enterprise Server

1

The BlackBerry Enterprise Server is designed to be a secure, centralized link between an organization's wireless network, communications software, applications, and BlackBerry smartphones. The BlackBerry Enterprise Server integrates with your organization's existing infrastructure to provide smartphone users with mobile access to your organization's resources.

You can manage the BlackBerry Enterprise Server, smartphones, and user accounts using the BlackBerry Administration Service. You can access the BlackBerry Administration Service web application from any computer that can access the computer that hosts the BlackBerry Administration Service.

You can optionally install BlackBerry Mobile Fusion Studio in your organization's environment to provide a simplified administrative console for your organization's helpdesk administrators and an integrated view of the BlackBerry Enterprise Server and other MDM domains. For more information, visit http://www.blackberry.com/go/serverdocs to see the *BlackBerry Mobile Fusion Studio Feature and Technical Overview*.

Document revision history

Date	Description
17 September 2012	Updated the following topics: • Create an administrator account • Permit users to perform administrative tasks using the BlackBerry Web Desktop Manager • Add a retrieved certificate for a web server to the key store • Changing password settings for BlackBerry Administration Service authentication • Permit a BlackBerry Enterprise Server to connect to a remote BlackBerry Router • Use the BlackBerry Administration Service to delete device data and disable the device before assigning the device to a new user

Date	Description
14 September 2011	Updated the following topics: • Import IT policy data • Reconciliation rules for conflicting IT policies when you apply multiple IT policies to a user account • Reconciliation rules for conflicting IT policies when you apply one IT policy to the user account • Troubleshooting: IT policies • Mapping contact information fields for synchronization and contact lookups • Map a contact information field in an email application to a contact list field on BlackBerry devices • Permit users to create activation passwords using the BlackBerry Web Desktop Manager
3 August 2011	Added the following topic: • Import IT policy rules from an IT policy pack
14 June 2011	Updated the following topics: • Configuring a new mirror BlackBerry Configuration Database • Configure the certificate information using IT policies
07 March 2011	Initial version

Getting started in your BlackBerry Enterprise Server environment

The following table lists the tasks that administrators typically perform after installing a BlackBerry Enterprise Server, and the chapter or section in the *BlackBerry Enterprise Server Administration Guide* that contains the information required to complete the task. Some of the tasks might not be required in your organization's environment.

Task	Chapter
Create administrator accounts.	Creating administrator accounts

Task	Chapter
Review the default IT policies. If necessary, change existing IT policies or create new IT policies.	Configuring security options • Section: Using an IT policy to manage BlackBerry Enterprise Solution security
Add user accounts to the BlackBerry Enterprise Server.	Configuring user accounts • Section: Adding a user account to the BlackBerry Enterprise Server
Create groups.	Configuring user accounts • Section: Creating groups
Add user accounts to groups.	Configuring user accounts • Section: Add a user account to a group
Review the default distribution settings for IT policies. If necessary, change the default distribution settings.	Managing the delivery of BlackBerry Java Applications, BlackBerry Device Software, and device settings to BlackBerry devices • Section: Change how IT policies are sent to BlackBerry devices
Assign IT policies to groups or user accounts.	Setting up security options • Section: Assign an IT policy to a group • Section: Assign an IT policy to a user account
Assign BlackBerry devices to user accounts.	Assigning BlackBerry devices to users
If necessary, change the default messaging settings for your organization's environment.	Setting up the messaging environment Managing your messaging environment and attachment support
Prepare to distribute BlackBerry Java Applications.	Sending software and BlackBerry Java Applications to BlackBerry devices • Section: Preparing to distribute BlackBerry Java Applications
Review the default distribution settings for BlackBerry Java Applications. If necessary, change the default distribution settings.	Managing the delivery of BlackBerry Java Applications, BlackBerry Device Software, and device settings to BlackBerry devices

Task	Chapter
	- Section: Change how to install, update, or remove BlackBerry Java Applications on BlackBerry devices
Review the default application control policies and application control policies for unlisted applications. If necessary, change the existing application control policies.	Sending software and BlackBerry Java Applications to BlackBerry devices - Section: Configuring application control policies - Section: Application control policies for unlisted applications
Create software configurations for BlackBerry Java Applications.	Sending software and BlackBerry Java Applications to BlackBerry devices - Section: Creating software configurations
Assign software configurations for BlackBerry Java Applications to groups, multiple user accounts, or individual user accounts.	Sending software and BlackBerry Java Applications to BlackBerry devices - Section: Assign a software configuration to a group - Section: Assign a software configuration to multiple user accounts - Section: Assign a software configuration to a user account
Configure BlackBerry Enterprise Server high availability.	Configuring BlackBerry Enterprise Server high availability

Optional tasks

Task	Chapter
Update BlackBerry Device Software on BlackBerry devices.	Visit www.blackberry.com/go/serverdocs to see the *BlackBerry Device Software Update Guide*.
Make the BlackBerry Web Desktop Manager available to users and configure the BlackBerry Web Desktop Manager.	Making the BlackBerry Web Desktop Manager available to users Configuring the BlackBerry Web Desktop Manager
Change the default settings for your instant messaging environment.	Managing instant messaging
Create and configure Wi-Fi and VPN profiles.	Creating and configuring Wi-Fi profiles and VPN profiles
Configure BlackBerry devices to enroll certificates.	Configuring BlackBerry devices to enroll certificates

Task	Chapter
Configure high availability for BlackBerry Enterprise Server components and for the BlackBerry Configuration Database.	Configuring BlackBerry Enterprise Server high availability Configuring BlackBerry Configuration Database high availability
Use the BlackBerry Monitoring Service to troubleshoot issues and monitor the health of a BlackBerry Enterprise Server.	Visit www.blackberry.com/go/serverdocs to see the *BlackBerry Enterprise Server Monitoring Guide*.
Change how the BlackBerry Enterprise Server creates log files.	BlackBerry Enterprise Server log files

Log in to the BlackBerry Administration Service for the first time

To open the BlackBerry Administration Service, you can use a browser on any computer that has access to the computer that hosts the BlackBerry Administration Service.

Before you begin: To manage a BlackBerry device using the BlackBerry Administration Service while the BlackBerry device is connected to the computer, the browser must permit Microsoft ActiveX controls.

1. In the browser, type **https://*<server_name>*/webconsole/app**, where <*server_name*> is the name of the computer that hosts the BlackBerry Administration Service.
2. In the **User name** field, type **admin**.
3. In the **Password** field, type the password that you created during the installation process.
4. In the **Log in using** drop-down list, click **BlackBerry Administration Service** or **Active Directory Authentication**.
5. Click **Log in**.

Related information

Best practice: Running the BlackBerry Enterprise Server, 71

The web browser displays an HTTP 404 or HTTP 504 error message when it tries to connect to a BlackBerry Administration Service instance, 470

There is a problem with this website's security certificate

Description

The browser displays this error message when you try to navigate to the BlackBerry Administration Service using Windows Internet Explorer version 7 or later.

Possible solution

Add the web address for the BlackBerry Administration Service to the list of trusted web sites in Windows Internet Explorer, and install the certificate for the BlackBerry Administration Service in the certificate store of your computer.

1. In Windows Internet Explorer, navigate to the BlackBerry Administration Service console.
2. Click **Continue to this website (not recommended)**.
3. On the **Tools** menu, click **Internet Options**.
4. On the **Security** tab, click **Local Intranet**.
5. Click **Sites**.
6. Click **Add** to add the console to the list of trusted web sites.
7. Click **Close**.
8. Click **OK**.
9. In the browser window, on the toolbar, click **Certificate Error**.
10. Click **View certificates**.
11. Click **Install certificate**. The Certificate Import Wizard opens.
12. Complete the instructions in the Certificate Import Wizard. If you are trying to log in to the BlackBerry Administration Service using a computer that runs Windows Vista, perform the following actions in the Certificate Import Wizard.

    a In the Certificate Store dialog box, click **Place all certificates in the following store**.

    b Click **Browse**.

    c Click **Trusted Root Certification Authorities**.

    d Click **OK**.

13. Close and reopen the browser.

This connection is untrusted

Description

The browser displays this error message when you try to navigate to the BlackBerry Administration Service or BlackBerry Monitoring Service using Mozilla Firefox 3.6.

Possible solution

Install the certificate for the BlackBerry Administration Service or BlackBerry Monitoring Service in the certificate store of your computer.

1. In Firefox, navigate to the BlackBerry Administration Service console or BlackBerry Monitoring Service console.

2. Click **I Understand the Risks**.
3. Click **Add Exception**.
4. Click **Confirm Security Exception**.
5. Close and reopen the browser.

Creating administrator accounts

3

Administrative roles and permissions

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 and BlackBerry Monitoring 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.

Preconfigured administrative roles

The BlackBerry Enterprise Server installation process includes preconfigured administrative roles. You can use the preconfigured administrative roles in your organization's environment instead of creating customize administrative roles. Each preconfigured administrative role contains multiple permissions that are turned on. The preconfigured administrative 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 administrator roles. You can configure additional permissions in the preconfigured administrative roles or turn off any of the permissions.

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
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

Permission name	Security role	Enterprise role	Senior Helpdesk role	Junior Helpdesk role	Server only role	User only role
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
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

Permission name	Security role	Enterprise role	Senior Helpdesk role	Junior Helpdesk role	Server only role	User only role
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	
Change the status of an instance	X	X			X	
Edit an instance relationship	X	X			X	
View a job	X	X				X

Permission name	Security role	Enterprise role	Senior Helpdesk role	Junior Helpdesk role	Server only role	User only role
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					X
Delete a role	X					X
View a role	X	X				X
Edit a role	X					X
Add or remove role	X					

Permission name	Security role	Enterprise role	Senior Helpdesk role	Junior Helpdesk role	Server only role	User only role
Import or export groups within roles	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

Creating roles

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, BlackBerry Monitoring 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.

Create a role

You can create a role for an administrator account if existing roles do not fulfill the criteria that your organization specified for the type of administrator account that you want to create. It is worthy to note that by default, when a new role is created all permissions for that role are turned off.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Role**.

2. Click **Create a role**.
3. Type a name and description for the role.
4. Click **Save**.
5. In the **Role information** section, click the name of the role that you created.
6. Click **Edit role**.
7. Switch the appropriate tabs to turn on the appropriate permissions.
8. Click **Save all**.

After you finish: Assign the role to an administrator account or group.

Create a role based on an existing role

To create a new role for an administrator account that is similar to an existing role, you can simply copy the existing role, use it to make a new role, and then make the appropriate changes to the new role.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Role**.
2. Click **Manage roles**.
3. In the list of existing roles, click the role that you want to copy.
4. Click **Copy role**.
5. Type a name and description for the role.
6. Click **Copy role**.
7. In the **Role information** section, click the name of the role that you created.
8. Click **Edit role**.
9. Switch the appropriate tabs to change the appropriate permissions.
10. Click **Save all**.

After you finish: Assign the role to an administrator account or group.

Create an administrator account

You can create an account for administrators so that they can log in to the BlackBerry Administration Service and manage the BlackBerry Enterprise Server. You create an administrator account and assign the account to one or more roles. The roles control the actions that an administrator can perform in the BlackBerry Administration Service.

If your environment includes a Microsoft Exchange resource forest, you must create the administrator account in the resource forest.

Before you begin: Verify that you can configure the authentication type and roles for an administrator account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Administrator user**.
2. Click **Create an administrator user**.
3. Type the required information. Consider using the minimum rules for password complexity when you create the password for the administrator account. The password should be at least 8 characters in length and contain at least one number, letter, and special character, and should not contain dictionary words.
4. In the **Role** drop-down list, click the role that you want to assign to the administrator account.
5. Click **Create an administrator user**.

After you finish: To configure the administrator account, provide the login information to the administrator and add the administrator account to a group, or you can assign additional roles to the administrator account.

Related information

Assigning BlackBerry devices to user accounts, 92

Managing administrator accounts, 282

Add an administrator account to a group

When 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. If you use groups to manage administrator roles and administrator accounts in your organization's environment, you can add multiple administrator accounts to specific groups and assign the appropriate roles to each group.

Note: If you add a role to a group, all accounts in the group become administrator accounts and have all of the permissions that are assigned to that role, even if the accounts are user accounts for BlackBerry device users.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for an administrator account.
4. In the search results, click the display name for the administrator account.
5. Click **Edit user**.
6. On the **Groups** tab, in the **Available groups** list, click the group that you want to add the administrator account to.
7. Click **Add**.
8. Click **Save all**.

Related information

Create a group to manage similar user accounts, 84

Specify an email address for the BlackBerry Administration Service

You can specify the email address that the BlackBerry Administration Service sends BlackBerry Enterprise Server system messages or activation passwords from.

Before you begin: Create an email account on your organization's messaging server.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Wireless activations**.
2. Click **Device activation settings**.
3. Click **Edit activation settings**.
4. In the **Sender address** field, type the email address that you want the BlackBerry Administration Service to send system messages or activation passwords from.
5. Click **Save all**.

Permit an administrator to log in to the BlackBerry Administration Service using a messaging server account

You can permit an administrator to log in to the BlackBerry Administration Service using a user name and password for the messaging server.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. In the **Authentication type** section, click the **Edit icon**.

7. In the **User information** section, in the **Display name** field, type the user name.
8. In the **Authentication type** section, type and verify a password.
9. Click the **Update** icon.
10. Click **Save all**.

Assign a BlackBerry device to an administrator account

You can assign a BlackBerry device to an administrator without creating a separate user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for an administrator account.
4. Click the display name for the administrator account.
5. In the **BlackBerry Enterprise Server status** list, click **Enable as BlackBerry user**.
6. Search for the messaging server display name or email address of the administrator.
7. Select the check box beside the administrator account.
8. Click **Next**.
9. Click the BlackBerry Enterprise Server that you want to assign the administrator account to.
10. Click **Save all**.

Using an IT policy to manage BlackBerry Enterprise Solution security

You can use an IT policy to control and manage BlackBerry devices, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager in your organization's environment. An IT policy consists of multiple IT policy rules that manage the security and behavior of the BlackBerry Enterprise Solution. For example, you can use IT policy rules to manage the following security features and behaviors of the device:

- encryption (for example, encryption of user data and messages that the BlackBerry Enterprise Server forwards to message recipients) and encryption strength
- use of a password or pass phrase
- connections that use Bluetooth wireless technology
- protection of user data and device transport keys on the device
- control of device resources, such as the camera or GPS, that are available to third-party applications

The BlackBerry Enterprise Server includes preconfigured IT policies that you can use to manage the security of the BlackBerry Enterprise Solution. The Default IT policy includes IT policy rules that are configured to indicate the default behavior of the device or BlackBerry Desktop Software.

After a device user activates a device, the BlackBerry Enterprise Server automatically sends to the device the IT policy that you assigned to the user account or group. By default, if you do not assign an IT policy to the user account or group, the BlackBerry Enterprise Server sends the Default IT policy. If you delete an IT policy that you assigned to the user account or group, the BlackBerry Enterprise Server automatically re-assigns the Default IT policy to the user account and resends the Default IT policy to the device.

For more information, see the *BlackBerry Enterprise Server Policy Reference Guide.*

Using IT policy rules to manage BlackBerry Enterprise Solution security

You can use IT policy rules to customize and control the actions that the BlackBerry Enterprise Solution can perform.

To use an IT policy rule on a BlackBerry device, you must verify that the BlackBerry Device Software version supports the IT policy rule. For example, you cannot use the Disable Camera IT policy rule to control whether a BlackBerry device user can access the camera on the device if the BlackBerry Device Software version does not support the IT policy rule. For information about the BlackBerry Device Software version that is required for a specific IT policy rule, see the *BlackBerry Enterprise Server Policy Reference Guide*.

If you create a custom IT policy that does not permit users to change their user information on their devices, you can only apply this custom IT policy to devices running BlackBerry Device Software 5.0 or later.

The BlackBerry Administration Service groups the IT policy rules by common properties or by application. Most IT policy rules are designed so that you can assign them to multiple user accounts and groups.

Preconfigured IT policies

The BlackBerry Enterprise Server includes the following preconfigured IT policies that you can change to create IT policies that meet the requirements of your organization.

Preconfigured IT policy	Description
Default	This policy includes all the standard IT policy rules that are set on the BlackBerry Enterprise Server.
Individual-Liable Devices	Similar to the Default IT policy, this policy prevents BlackBerry device users from accessing organizer data from within the social networking applications on their BlackBerry devices. This policy permits users to access their personal calendar services and email messaging services (for example, their BlackBerry Internet Service accounts), update the BlackBerry Device Software using methods that exist outside your organization, make calls when devices are locked, and cut, copy, and paste text. Users cannot forward email messages from one email messaging service to another. You can use the Individual-Liable Devices IT policy if your organization includes users who purchase their own devices and connect the devices to a BlackBerry Enterprise Server instance in your organization's environment.
Basic Password Security	Similar to the Default IT policy, this policy also requires a basic password that users can use to unlock their devices. Users must change the passwords regularly. The IT policy includes a password timeout that locks devices.
Medium Password Security	Similar to the Default IT policy, this policy also requires a complex password that users can use to unlock their devices. Users must change the passwords regularly. This policy includes a maximum password history and turns off Bluetooth technology on devices.

Preconfigured IT policy	Description
Medium Security with No 3rd Party Applications	Similar to the Medium Password Security, this policy requires a complex password that a user must change frequently, a security timeout, and a maximum password history. This policy prevents users from making their devices discoverable by other Bluetooth enabled devices and prevents devices from downloading third-party applications.
Advanced Security	Similar to the Default IT policy, this IT policy also requires a complex password that users must change frequently, a password timeout that locks devices, and a maximum password history. This policy restricts Bluetooth technology on devices, turns on strong content protection, turns off USB mass storage, and requires devices to encrypt external file systems.
Advanced Security with No 3rd Party Applications	Similar to the Advanced Security IT policy, this IT policy requires a complex password that users must change frequently, a password timeout that locks devices, and a maximum password history. This policy restricts Bluetooth technology on devices, turns on strong content protection, turns off USB mass storage, requires devices to encrypt external file systems, and prevents devices from downloading third-party applications.

Default values for preconfigured IT policies

You can configure additional IT policy rules in the preconfigured IT policies or change any of the following values:

IT policy rule	Default IT policy	Individual-Liable Device IT policy	Basic Password Security IT policy	Medium Password Security IT policy	Medium Password Security with No 3rd Party Applications IT policy	Advanced Security IT policy	Advanced Security with No 3rd Party Applications IT policy
Device-Only Items							
Enable Long-Term Timeout	—	—	—	Yes	Yes	Yes	Yes
Maximum Security Timeout	—	—	30 minutes	10 minutes	10 minutes	10 minutes	10 minutes
Maximum Password Age	—	—	60 days	30 days	30 days	30 days	30 days
Password Pattern Checks	no restriction	—	no restriction	at least 1 alpha and 1	at least 1 alpha and 1	at least 1 alpha and 1	at least 1 alpha and 1

IT policy rule	Default IT policy	Individual-Liable Device IT policy	Basic Password Security IT policy	Medium Password Security IT policy	Medium Password Security with No 3rd Party Applications IT policy	Advanced Security IT policy	Advanced Security with No 3rd Party Applications IT policy
				numeric character	numeric character	numeric character	numeric character
Password Required	No	—	Yes	Yes	Yes	Yes	Yes
User Can Change Timeout	Yes	—	Yes	Yes	Yes	Yes	Yes
User Can Disable Password	Yes	—	No	No	No	No	No
Password policy group							
Maximum Password History	—	—	—	6	6	6	6
RIM Value-Added Applications policy group							
Disable Organizer Data Access for Social Networking Applications	Yes	Yes	—	—	—	—	—
Security policy group							
Allow Outgoing Call When Locked	No	Yes	—	—	—	—	—
Content Protection Strength	—	—	—	—	—	Strong	Strong
Disable Cut/Copy/Paste	No	No	—	—	—	—	—
Disable Forwarding	No	Yes	—	—	—	—	—

IT policy rule	Default IT policy	Individual-Liable Device IT policy	Basic Password Security IT policy	Medium Password Security IT policy	Medium Password Security with No 3rd Party Applications IT policy	Advanced Security IT policy	Advanced Security with No 3rd Party Applications IT policy
Between Services							
Disable USB Mass Storage	No	—	—	—	—	Yes	Yes
Disallow Third Party Application Download	No	—	—	—	Yes	—	Yes
External File System Encryption level	Not required	—	—	—	—	Encrypt to user password (excluding multimedia directories)	Encrypt to user password (excluding multimedia directories)
Force Lock When Holstered	No	—	—	Yes	Yes	Yes	Yes
Reset to Factory Defaults on Wipe	No	Yes	—	—	—	—	—
Service Exclusivity policy group							
Allow Other Calendar Services	Yes	Yes	—	—	—	—	—
Allow Other Message Services	Yes	Yes	—	—	—	—	—
Bluetooth policy group							
Disable Address Book Transfer	No	—	—	—	—	Yes	Yes
Disable Discoverable Mode	No	—	—	Yes	Yes	Yes	Yes

IT policy rule	Default IT policy	Individual-Liable Device IT policy	Basic Password Security IT policy	Medium Password Security IT policy	Medium Password Security with No 3rd Party Applications IT policy	Advanced Security IT policy	Advanced Security with No 3rd Party Applications IT policy
Disable File Transfer	No	—	—	—	—	Yes	Yes
Disable Serial Port Profile	No	—	—	—	—	Yes	Yes
Require LED Connection Indicator	No	—	—	—	—	Yes	Yes
Wi-Fi policy group							
Wi-Fi Allow Handheld Changes	Yes	—	No	No	No	No	No
Wireless Software Upgrades policy group							
Allow Non Enterprise Upgrade	No	Yes	—	—	—	—	—

Creating and importing IT policies

Create an IT policy

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Create an IT policy**.
3. Type a name and description for the IT policy.
4. Click **Save**.
5. To configure the IT policy, perform the following actions:
    a. In the **IT policy information** section, click the IT policy.

b. Click **Edit IT policy**.

c. On a tab for an IT policy group, configure values for the IT policy rules.

d. Click **Save All**.

After you finish: For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Create an IT policy based on an existing IT policy

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. In the list of IT policies, click the IT policy that you want to copy.
4. Click **Copy IT policy**.
5. Type a name and description for the new IT policy.
6. Click **Save**.
7. To change the IT policy settings, perform the following actions:
    a. In the **IT policy information** section, click the IT policy.
    b. Click **Edit IT policy**.
    c. On a tab for an IT policy group, change the appropriate values for the IT policy rules.
    d. Click **Save all**.

After you finish: For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Related information

Preconfigured IT policies, 40

Import IT policy data

CAUTION: For you to import IT policy data successfully, the IT policy data file must contain all of the IT policies that are assigned to user accounts and groups in the BlackBerry Domain that you are importing IT policy data to.

Before you begin: Export IT policy data from a different BlackBerry Domain.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. In the **Manage IT policies** section, click **Import IT policy list**.
4. In the **IT policy import** section, specify the following information:

- Location of the data source file
- File encryption password that you use to protect the data source file

5. Click **Next**.
6. Click **Add all IT policies**.

Related information

Preconfigured IT policies, 40

Import IT policy rules from an IT policy pack

You can import the IT policy rules that Research In Motion releases in an IT policy pack into your organization's BlackBerry Enterprise Server.

1. Download the IT policy pack to your computer and extract the contents of the file.
2. In the BlackBerry Administration Service, on the BlackBerry solution management menu, expand **Policy**.
3. Click **Manage IT policy rules**.
4. Click **Import IT policy definitions**.
5. Navigate to and select the XML file that contains the IT policy rules (for example, ITPolicyTemplate082409.xml).
6. Click **Save**.

Change the value for an IT policy rule

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. In the **IT policy information** section, click the IT policy.
4. Click **Edit IT policy**.
5. On a tab for an IT policy group, change the appropriate values for the IT policy rules.
6. Click **Save all**.

Assign an IT policy to a group

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. In the **Manage groups** section, click the group that you want to assign an IT policy to.
4. On the **Policies** tab, click **Edit group**.
5. In the drop-down list, click an IT policy.
6. Click **Save all**.

Related information

Adding a user account to the BlackBerry Enterprise Server, 85
Assigning IT policies and resolving IT policy conflicts, 49

Assign an IT policy to a user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name of the user account.
5. On the **Policies** tab, click **Edit user**.
6. In the drop-down list, click an IT policy.
7. Click **Save all**.

Related information

Adding a user account to the BlackBerry Enterprise Server, 85
Assigning IT policies and resolving IT policy conflicts, 49

Sending an IT policy over the wireless network

If your organization's environment includes C++ based BlackBerry devices that are running BlackBerry Device Software version 2.5 or later or Java based devices that are running BlackBerry Device Software version 3.6 or later, the BlackBerry Enterprise Server can send changes to IT policies to a device over the wireless network automatically. When the device receives an updated IT policy or a new IT policy, the device, BlackBerry Desktop Software, and BlackBerry Web Desktop Manager apply the configuration changes immediately.

By default, the BlackBerry Enterprise Server is designed to resend an IT policy to the device within a short period of time after you update the IT policy using the BlackBerry Administration Service. You can also resend an IT policy to a specific device manually. You can configure the BlackBerry Enterprise Server to resend the IT policy to the device at scheduled intervals regardless of whether you changed the IT policy.

Related information

Using IT policy rules to manage BlackBerry Enterprise Solution security, 39

Assigning IT policies and resolving IT policy conflicts, 49

Preconfigured IT policies, 40

Resend an IT policy to a BlackBerry device manually

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. On the **Policies** tab, click **View resolved IT policy data**.
6. Click **Resend IT policy to a device**.

Resend an IT policy to a BlackBerry device automatically

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology**.

2. Expand **BlackBerry Domain** > **Component view**.
3. In the **Policy** section, click an instance.
4. Click **Edit instance**.
5. In the **General** section, in the **Policy resend interval (hours)** field, type an interval that you want the BlackBerry device to resend the IT policy at.
6. Click **Save All**.

Assigning IT policies and resolving IT policy conflicts

You can assign IT policies directly to a user account or to a group. By default, if you do not assign an IT policy to a user account or a group that the user is a member of, the BlackBerry Enterprise Server applies the Default IT policy to the user account. If you assign an IT policy to a group that a user account is a member of, the BlackBerry Enterprise Server applies the group IT policy to the user account. If you assign an IT policy to the user account directly, the BlackBerry Enterprise Server applies this IT policy to the user account instead of the group IT policy or Default IT policy.

If a user account is a member of multiple groups that have different IT policies, the BlackBerry Enterprise Server must determine which IT policy to apply to the user account. You must use one of the following reconciliation options:

Method	Description
Apply one IT policy to the user account	The BlackBerry Enterprise Server applies one of the group IT policies to the user account. You specify rankings for the available IT policies using the BlackBerry Administration Service and the BlackBerry Enterprise Server applies the IT policy with the highest ranking. If you upgrade to BlackBerry Enterprise Server 5.0 SP2 or later from a previous version of the BlackBerry Enterprise Server, this is the default method for resolving IT policy conflicts.
Apply multiple IT policies to the user account	The BlackBerry Enterprise Server applies all of the group IT policies to the user account, resulting in a combined IT policy that has a unique ID. The BlackBerry Enterprise Server resolves conflicting IT policy rules using the ranking of the available IT policies that you specified using the BlackBerry Administration Service. If an IT policy rule is different in the multiple IT policies, the BlackBerry Enterprise Server applies the rule setting from the IT policy that you ranked the highest. If you install BlackBerry Enterprise Server 5.0 SP2 or later, this is the default method for resolving IT policy conflicts.

Related information

Option 1: Applying one IT policy to each user account

You can configure the BlackBerry Enterprise Server to apply only one IT policy to a user account when a user account is a member of multiple groups that have different IT policies. In this scenario, the BlackBerry Enterprise Server applies the IT policy that you ranked the highest in the BlackBerry Administration Service.

If you upgrade to BlackBerry Enterprise Server 5.0 SP2 or later from a previous version of the BlackBerry Enterprise Server, this is the default method for resolving IT policy conflicts. If you install BlackBerry Enterprise Server 5.0 SP2 or later, the default method for resolving IT policy conflicts is to apply multiple IT policies to each user account and create a combined IT policy that has a unique ID for the user account.

Reconciliation rules for conflicting IT policies when you apply one IT policy to the user account

The BlackBerry Enterprise Server can apply only one IT policy to a user account. Since you can assign IT policies to user accounts, groups, or the BlackBerry Domain, the BlackBerry Administration Service uses predefined rules to determine which IT policy it can apply to a user account.

The BlackBerry Administration Service might have to reconcile conflicting IT policies if you perform any of the following actions:

- add an IT policy to or remove an IT policy from a user account or group
- change an IT policy
- change the ranking of IT policies
- delete an IT policy

Scenario	Rule
You add a new user account to a BlackBerry Enterprise Server. You do not assign an IT policy directly to the user account and you do not add the user to a group.	The IT policy that you assigned to the BlackBerry Domain, or the Default IT policy that is assigned to the BlackBerry Domain, is assigned to the user account.
You assign an IT policy to a user account and a different IT policy to a group that the user account belongs to.	The IT policy that you assign to a user account takes precedence over an IT policy that you assign to a group. An IT policy that you assign to a group takes precedence over the IT policy that you assign to the BlackBerry Domain (or the Default IT policy).
A user account belongs to multiple groups. You assign multiple IT policies to the groups but do not assign an IT policy to the user account.	The BlackBerry Enterprise Server applies the IT policy that you ranked the highest in the BlackBerry Administration Service to the user account.

Change the method that the BlackBerry Enterprise Server uses to resolve conflicting IT policies

You can change the method that the BlackBerry Enterprise Server uses to determine what IT policy to apply to a user account when a user account belongs to multiple groups that have different IT policies. If you change the method used to resolve conflicting IT policies, the next IT policy reconciliation process that occurs might have a significant impact on the performance of your organization's BlackBerry Enterprise Server environment. It is a best practice to configure this feature during low usage periods.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service**.
3. At the bottom of the page, click **Switch method to resolve multiple IT policies**.
4. Click **Yes - Switch the method**.

Related information

Option 1: Applying one IT policy to each user account, 50
Option 2: Applying multiple IT policies to each user account, 51

Rank IT policies

You must rank the IT policies that you create so that the BlackBerry Enterprise Server can resolve IT policy conflicts when a user account is a member of multiple groups that have different IT policies.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. Click **Set priority of IT policies**.
4. To move the IT policies higher or lower in the list, click the **up arrow** icon or **down arrow** icon.
5. Click **Save**.

Option 2: Applying multiple IT policies to each user account

You can configure the BlackBerry Enterprise Server to apply multiple IT policies to a user account when a user account is a member of multiple groups that have different IT policies. The BlackBerry Enterprise Server creates a combined IT policy for the user account that has a unique ID by applying the policy rules from the multiple IT policies and resolving any conflicting rule settings. The BlackBerry Enterprise Server resolves conflicting rule settings by applying the rule setting from the IT policy that you ranked the highest in the BlackBerry Administration Service.

If you install BlackBerry Enterprise Server 5.0 SP2 or later, this is the default method for resolving IT policy conflicts. If you upgrade to BlackBerry Enterprise Server 5.0 SP2 or later from a previous version of the BlackBerry Enterprise Server, the default method for resolving IT policy conflicts is to assign one IT policy to each user account according to the rankings of the IT policies that you specify in the BlackBerry Administration Service.

Reconciliation rules for conflicting IT policies when you apply multiple IT policies to a user account

The BlackBerry Enterprise Server can apply multiple IT policies to a user account if the user account is a member of multiple groups that have different IT policies. Since you can assign IT policies to user accounts, groups, or the BlackBerry Domain, the BlackBerry Administration Service uses predefined rules to apply an IT policy to a user account.

The BlackBerry Administration Service might have to reconcile conflicting IT policies if you perform any of the following actions:

- add an IT policy to or remove an IT policy from a user account or group
- change an IT policy
- change the ranking of IT policies
- delete an IT policy

Scenario	Rule
You add a new user account to a BlackBerry Enterprise Server. You do not assign an IT policy directly to the user account and you do not add the user account to a group.	The Default IT policy (applied at the BlackBerry Domain level) is assigned to the user account.
You assign an IT policy to a user account and different IT policies to the groups that the user account belongs to.	The IT policy that you assign to a user account takes precedence over the IT policies that you assign to the groups that the user belongs to. An IT policy that you assign to a group takes precedence over the Default IT policy (applied at the BlackBerry Domain level).
A user account belongs to multiple groups. You assign multiple IT policies to the groups but you do not assign an IT policy to the user account.	If you assign multiple IT policies to the groups that the user account belongs to, the BlackBerry Enterprise Server resolves the IT policy rule settings in the multiple IT policies and assigns a combined IT policy that has a unique ID to the user account. The BlackBerry Enterprise Server resolves conflicting settings for IT policy rules by applying the rule setting from the IT policy that you ranked the highest in the BlackBerry Administration Service. For example, you configure the Disable Photo Camera IT policy rule to Yes in IT policy A and to No in IT policy B. If you rank IT policy A higher than IT policy B, the Yes setting is applied for this rule.
A user account belongs to two groups. You assign the first group IT policy A, which has the Allow Browser IT policy rule as blank (which means that it uses	When the BlackBerry Enterprise Server resolves conflicting rule settings, any rule settings that have been explicitly configured to a value take precedence over IT policy rule settings that are blank (these rules revert to the default value).

Scenario	Rule
the default value of Yes). You assign the second group IT policy B, which has the Allow Browser IT policy rule set to No. You ranked IT policy A higher than IT policy B in the BlackBerry Administration Service.	For example, in this scenario, the Allow Browser IT policy rule setting from IT policy B, No, is applied to the user account even though IT policy A is ranked higher than IT policy B, because the Allow Browser IT policy rule is blank in IT policy A. If the Allow Browser IT policy rule was configured to Yes in IT policy A, the Yes value would be applied to the user account.

Change the method that the BlackBerry Enterprise Server uses to resolve conflicting IT policies

You can change the method that the BlackBerry Enterprise Server uses to determine what IT policy to apply to a user account when a user account belongs to multiple groups that have different IT policies. If you change the method used to resolve conflicting IT policies, the next IT policy reconciliation process that occurs might have a significant impact on the performance of your organization's BlackBerry Enterprise Server environment. It is a best practice to configure this feature during low usage periods.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service**.
3. At the bottom of the page, click **Switch method to resolve multiple IT policies**.
4. Click **Yes - Switch the method**.

Related information

Option 1: Applying one IT policy to each user account, 50

Option 2: Applying multiple IT policies to each user account, 51

Rank IT policies

You must rank the IT policies that you create so that the BlackBerry Enterprise Server can resolve IT policy conflicts when a user account is a member of multiple groups that have different IT policies.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. Click **Set priority of IT policies**.
4. To move the IT policies higher or lower in the list, click the **up arrow** icon or **down arrow** icon.
5. Click **Save**.

Preview how the BlackBerry Enterprise Server resolves IT policy conflicts

You can preview how the BlackBerry Enterprise Server resolves conflicting settings for IT policy rules for multiple IT policies that you select. You can use this feature to determine which IT policies have conflicting IT policy rules and how the

BlackBerry Enterprise Server resolves the conflicting rules. The preview displays the conflicting IT policy rules and the resolved settings for each rule. If an IT policy rule is not conflicting in the multiple IT policies that you selected, the preview does not display the policy rule in the results.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. Click **Preview resolved IT policies**.
4. Select two or more IT policies.
5. Click **Preview**.

View the resolved IT policy rules that are assigned to a user account

If a user account belongs to multiple groups, and you assign a different IT policy to each group, the BlackBerry Enterprise Server resolves conflicting IT policies or IT policy rule settings using the reconciliation method that you select in the BlackBerry Administration Service. You can view the results of the IT policy reconciliation and the settings that the BlackBerry Enterprise Server resolves for each rule in the BlackBerry Administration Service. If an IT policy rule is not conflicting in the multiple IT policies that were applied to the user account, the preview does not display the IT policy rule.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for a user account.
5. On the **Policies** tab, in the **Resolved IT Policy name** section, click the name of the IT policy.

Deactivating BlackBerry devices that do not have IT policies applied

To prevent BlackBerry devices that do not have IT policies applied to them from remaining active on a BlackBerry Enterprise Server, you can change the Disable users with unapplied IT policy option to True. The Disable user time limit (hours) option specifies the amount of time that BlackBerry devices can be active on a BlackBerry Enterprise Server without having an IT policy applied to the BlackBerry devices.

If you change the Disable users with unapplied IT policy option to True, by default, the BlackBerry Enterprise Server sends the IT policy to the BlackBerry devices every 30 minutes until the BlackBerry devices apply the IT policy or the time limit expires. If the time limit expires, the BlackBerry Enterprise Server deactivates the BlackBerry device PINs. The permitted range for this option is 0 hours to 8760 hours. If you specify 0 hours, BlackBerry devices deactivate when the IT policy cannot apply automatically.

Deactivate BlackBerry devices that do not have IT policies applied

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry solution topology** > **BlackBerry Domain** > **Component view** > **Policy**.
2. Click the instance that you want to change.
3. In the **Disable Users with Unapplied IT Policy** drop-down list, click **True**.
4. In the **Disable user time limit (hours)** field, type the time (in hours) that can occur before the PINs for BlackBerry devices that you did not apply an IT policy to are deactivated on the BlackBerry Enterprise Server.
5. Click **Save All**.

After you finish: Before you re-activate the BlackBerry devices on the BlackBerry Enterprise Server, on the BlackBerry devices, in the **Security Options** list, instruct users to click **Wipe Handheld** or **Security Wipe** to delete all of the data on the BlackBerry devices.

Creating new IT policy rules to control third-party applications

You can create IT policy rules to control the applications that your organization creates for BlackBerry devices that are running in your organization's environment. After you create an IT policy rule, you can add it to a new or existing IT policy and assign a value to it. Only applications that your organization creates can use the IT policy rule that you create. You cannot create new IT policy rules to control device applications and features.

Create an IT policy rule for a third-party application

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Create an IT policy rule**.
3. Type a name and description for the IT policy rule.
4. In the **Type** drop-down list, click the type of value that the IT policy rule uses.

5. In the **Destination** drop-down list, choose whether you want the BlackBerry device, the BlackBerry Desktop Software, or both to be able to use the IT policy rule.
6. Click **Save**.

After you finish: Add the IT policy rule to an IT policy.

Change or delete IT policy rules for third-party applications

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policy rules**.
3. Click an IT policy rule.
4. Perform one of the following actions:
   - To change the IT policy rule, click **Edit IT policy rule**. Change the appropriate values.
   - To delete the IT policy rule, click **Delete IT policy rule**. Verify that you want to delete the IT policy rule.
5. Click **Save**.

Export all IT policy data to a data file

If you export all IT policy data to a data file, you must create an encryption password for the data file that you can use to protect the data file. You can import the data file at a later time to another BlackBerry Domain.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. Click **Export IT policy list**.
4. In the **File encryption password** field and **Confirm file encryption password** field, type a password so that the BlackBerry Enterprise Server can encrypt the IT policy data file.
5. Click **Export**.
6. Click **Download file**.
7. Click **Save**.
8. Browse to a location on a local or network drive where you want to save the data file.
9. Click **Save**.

10. Click **Close**.

Delete an IT policy

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. In the list of IT policies, click an IT policy.
4. Click **Delete IT policy**.
5. Click **Yes** – **Delete the IT policy**.

Related information

Assigning IT policies and resolving IT policy conflicts, 49

Configuring security options

5

Encrypting data that the BlackBerry Enterprise Server and a BlackBerry device send to each other

To encrypt data that is in transit between the BlackBerry Enterprise Server and a BlackBerry device in your organization, the BlackBerry Enterprise Solution uses BlackBerry transport layer encryption. BlackBerry transport layer encryption is designed to encrypt data from the time that a BlackBerry device user sends a message from the BlackBerry device to when the BlackBerry Enterprise Server receives the message, and from the time that the BlackBerry Enterprise Server sends a message to when the BlackBerry device receives the message.

Before the BlackBerry device sends a message, it compresses and encrypts the message using the device transport key. When the BlackBerry Enterprise Server receives a message from the BlackBerry device, the BlackBerry Dispatcher decrypts the message using the device transport key, and then decompresses the message.

Algorithms that the BlackBerry Enterprise Solution uses to encrypt data

The BlackBerry Enterprise Solution uses AES or Triple DES as the symmetric key cryptographic algorithm for encrypting data. By default, the BlackBerry Enterprise Server uses the strongest algorithm that both the BlackBerry Enterprise Server and the BlackBerry device support for BlackBerry transport layer encryption.

If you configure the BlackBerry Enterprise Server to support AES and Triple DES, by default, the BlackBerry Enterprise Solution generates device transport keys using AES encryption. If a BlackBerry device uses BlackBerry Device Software version 3.7 or earlier or BlackBerry Desktop Software version 3.7 or earlier, the BlackBerry Enterprise Solution generates the device transport keys of the BlackBerry device using Triple DES.

Change the symmetric key encryption algorithm that the BlackBerry Enterprise Solution uses

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **BlackBerry Enterprise Server**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. In the **Security information** section, in the **Encryption algorithm** drop-down list, click the encryption algorithm that you want the BlackBerry Enterprise Solution to use.
5. Click **Save All**.

After you finish: Re-activate all of the BlackBerry devices that are located in the BlackBerry Domain so that users can send and receive email messages on their BlackBerry devices.

Related information

Assigning BlackBerry devices to user accounts, 92

Managing device access to the BlackBerry Enterprise Server

You can use the Enterprise Service Policy to control which BlackBerry devices can connect to a BlackBerry Enterprise Server. By default, after you turn on the Enterprise Service Policy, the BlackBerry Enterprise Server permits connections from any device that you previously associated with the BlackBerry Enterprise Server. The BlackBerry Enterprise Server also prevents connections from any device that you associate with the BlackBerry Enterprise Server after you turn on the Enterprise Service Policy.

You can configure an allowed list to determine which devices can access a BlackBerry Enterprise Server. A device that meets the criteria that you specify in the allowed list can associate with the BlackBerry Enterprise Server when the device activates over the wireless network.

You can define the following types of criteria:

- specific device PINs
- range of device PINs
- specific manufacturers
- specific device models

The BlackBerry Administration Service includes lists of permitted manufacturers and models of devices that you associated with the BlackBerry Enterprise Server previously.

You can permit a user to override the Enterprise Service Policy so that a device can connect to the BlackBerry Enterprise Server even if you configure the allowed list with criteria that exclude that device.

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

Turn on the Enterprise Service Policy

You can turn on the Enterprise Service Policy to control which BlackBerry devices can connect to the BlackBerry Enterprise Server.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Enterprise Server**.
3. Click **Turn on Enterprise Service Policy**.
4. Click **Yes - Turn on enterprise service policy**.

Configure the Enterprise Service Policy

By default, when you turn on the Enterprise Service Policy, all BlackBerry devices that you activated can access the BlackBerry Enterprise Server. You must configure the Enterprise Service Policy to specify the BlackBerry devices that you want to access the BlackBerry Enterprise Server. To add a new BlackBerry device to the BlackBerry Enterprise Server, you must add the PIN for the BlackBerry device to the Enterprise Service Policy before a user can activate the BlackBerry device.

Before you begin: Turn on the Enterprise Service Policy.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Enterprise Server**.
3. Click **Edit component**.
4. In the **Enterprise Service Policy** section, in the **Allowed** drop-down lists, click **Yes** for each BlackBerry device model that you want to permit to access the BlackBerry Enterprise Server.
5. To add a new BlackBerry device, on the **Add new allowed PINs** tab, in the **New allowed PINs** field, type the PIN for the BlackBerry device. Click the **Add** icon.
6. To remove a BlackBerry device from the list, on the **Remove existing allowed PINs** tab, search for the PIN for the BlackBerry device. In the search results, select the PIN for the BlackBerry device.
7. Click **Save All**.

Permit a user to override the Enterprise Service Policy

Before you begin: Turn on the Enterprise Service Policy.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. Click the display name for the user account.
5. Click **Edit user**.
6. On the **Component information** tab, in the **BlackBerry Enterprise Server information** section, in the **Enterprise service policy override** drop-down list, click **Yes**.
7. Click **Save All**.

Extending messaging security to a BlackBerry device

If your organization's messaging environment supports highly secure messaging technology such as PGP encryption or S/MIME encryption, you can configure the BlackBerry Enterprise Solution to encrypt a message using PGP encryption or S/MIME encryption so that the message remains encrypted when the BlackBerry Enterprise Server forwards the message to the email applications of recipients. To extend messaging security, the sender and recipient must install highly secure messaging technology on the computers that host the email applications and on their BlackBerry devices, and you must configure the BlackBerry devices to use the highly secure messaging technology.

Extending messaging security using PGP encryption

You can extend messaging security for the BlackBerry Enterprise Solution and permit a BlackBerry device user to send and receive PGP protected email messages and PGP protected PIN messages on a BlackBerry device. The BlackBerry Enterprise Solution supports the OpenPGP format and PGP/MIME format on the BlackBerry device.

To extend messaging security, you must instruct the BlackBerry device user to install the PGP Support Package for BlackBerry smartphones on the BlackBerry device and to transfer the PGP private key of the BlackBerry device user to the BlackBerry device. The BlackBerry device user can use the PGP private key to digitally sign, encrypt, and send PGP protected messages from the BlackBerry device. If a BlackBerry device user does not install the PGP Support Package for BlackBerry smartphones, the BlackBerry device displays an error message when the BlackBerry device user tries to open PGP protected messages.

To require the BlackBerry device user to use PGP encryption when forwarding or replying to messages, you can configure the PGP Force Digital Signature IT policy rule and the PGP Force Encrypted Messages IT policy rule.

The PGP Support Package for BlackBerry smartphones is designed to support encoding and decoding Unicode messages and permits PGP encryption using keys or passwords. The PGP Support Package for BlackBerry smartphones permits the BlackBerry device to encrypt PGP protected email messages or PGP protected PIN messages using a password that the sender and recipient both know.

For more information about the OpenPGP format, see RFC 2440. For more information about the PGP/MIME format, see RFC 3156.

Configure the BlackBerry Enterprise Solution to support PGP encryption

1. Configure the PGP Universal Server Address IT policy rule in the IT policy that you assign to BlackBerry device users.
2. Instruct users to install the PGP Support Package for BlackBerry smartphones on BlackBerry devices.
3. Instruct users to enroll with the PGP Universal Server when the BlackBerry devices prompt them to so that the BlackBerry devices can process PGP protected messages.

Extending messaging security using S/MIME encryption

You can extend messaging security for the BlackBerry Enterprise Solution and permit a BlackBerry device user to send and receive S/MIME-protected email messages and S/MIME-protected PIN messages on a BlackBerry device.

To extend messaging security, you or the BlackBerry device user must install the S/MIME Support Package for BlackBerry smartphones on the BlackBerry device and transfer the S/MIME private key of the BlackBerry device user to the BlackBerry device. The S/MIME Support Package for BlackBerry smartphones is designed to work with email applications such as Microsoft Outlook, Microsoft Outlook Express, and IBM Lotus Notes, and with PKIs such as Netscape, Entrust Authority Security Manager version 5 and later, and Microsoft certification authorities.

The BlackBerry device user uses the S/MIME private key to decrypt S/MIME-protected messages on the BlackBerry device and to sign, encrypt, and send S/MIME-protected messages from the BlackBerry device. If the BlackBerry Enterprise Server receives an S/MIME-encrypted message but the BlackBerry device user did not install the S/MIME Support Package for BlackBerry smartphones, the BlackBerry Enterprise Server sends a message to the BlackBerry device to indicate that the BlackBerry device does not support S/MIME-encrypted messages.

After the BlackBerry device user installs the S/MIME Support Package for BlackBerry smartphones, the BlackBerry device user can synchronize and manage S/MIME certificates and S/MIME private keys using the certificate synchronization tool of the BlackBerry Desktop Manager. The BlackBerry Enterprise Server does not apply an appended disclaimer to S/MIME-protected messages that the BlackBerry device user sends from the BlackBerry device. Digital signatures on S/MIME-protected messages that the BlackBerry device sends are not valid if disclaimers are appended to the messages.

To require the BlackBerry device user to use S/MIME encryption when forwarding or replying to messages, you can configure the S/MIME Force Digital Signature IT policy rule and the S/MIME Force Encrypted Messages IT policy rule.

The S/MIME Support Package for BlackBerry smartphones is also designed to support the following features:

- Encoding and decoding of Unicode messages

- Ability to use a password, which the sender and recipient each know, to encrypt S/MIME-protected email messages or PIN messages
- Ability to read S/MIME certificates that are stored on a smart card

Configure the BlackBerry Enterprise Solution to support S/MIME encryption

1. Configure encryption options for S/MIME-protected messages on the BlackBerry Enterprise Server.
2. If required, configure message classifications for email messages.
3. If required, configure the BlackBerry MDS Connection Service to retrieve certificates and the status of certificates from LDAP servers, DSML certificate servers, OCSP servers, or CRL servers.
4. Instruct users to install the S/MIME Support Package for BlackBerry smartphones on BlackBerry devices.
5. Perform one of the following tasks:
    - Instruct users to add the Certificate Synchronization Manager to the BlackBerry Desktop Manager so that the BlackBerry Desktop Manager can manage certificates for the BlackBerry devices.
    - Configure the BlackBerry Enterprise Server to permit users to enroll certificates over the wireless network.

Related information

Configuring certificate server information for the BlackBerry MDS Connection Service, 193

Enforcing secure messaging using classifications, 65

Configuring BlackBerry devices to enroll certificates over the wireless network, 217

Configure encryption options for S/MIME-protected messages

You can configure encryption options to control how the BlackBerry Enterprise Server processes S/MIME-protected messages.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Security settings** section, perform any of the following actions:
    - To require that the BlackBerry Enterprise Server encrypts messages using S/MIME encryption for a second time when the BlackBerry Enterprise Server processes S/MIME-protected messages that an S/MIME-enabled application weakly encrypted or only signed, in the **Turn on S/MIME encryption on signed and weakly encrypted messages** drop-down list, click **True**.
    - To permit BlackBerry device users that have email applications that do not support S/MIME to read the text of an S/MIME-protected message, in the **Send S/MIME messages in clear-signed format** drop-down list, click **True**.

- To require that the BlackBerry Enterprise Server deletes attachment data from any signed-only S/MIME-protected messages so that the BlackBerry Enterprise Server conserves bandwidth, in the **Remove attachment data from signed S/MIME messages** drop-down list, click **True**.
- To require that the BlackBerry Enterprise Server sends encrypted S/MIME-protected messages using an updated MIME content-type that is in accordance with PKCS#7 instead of the default legacy MIME content-type, in the **Use PKCS #7 MIME type** drop-down list, click **True**.

5. Click **Save all**.
6. To make sure that the changes take effect immediately, perform the following actions to restart the BlackBerry Messaging Agent:
   a. On the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **BlackBerry Enterprise Server**.
   b. Click the BlackBerry Enterprise Server instance that includes the BlackBerry Messaging Agent.
   c. Click **Restart instance**.

Related information

Restarting BlackBerry Enterprise Server components, 392

Turn off support for processing S/MIME-protected messages on the BlackBerry Enterprise Server

By default, the BlackBerry Enterprise Server can process S/MIME-protected messages. You can turn off support for processing S/MIME-protected messages if the BlackBerry Enterprise Server experiences issues when it processes S/MIME-protected messages or if your organization does not use S/MIME encryption.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. On the **Messaging** tab, click **Edit instance**.
4. In the **Security settings** section, in the **Turn on S/MIME message processing** drop-down list, click **False**.
5. Click **Save All**.

Enforcing secure messaging using classifications

You can use message classifications to require S/MIME-enabled users or PGP enabled users to sign, encrypt, or sign and encrypt email messages that they send from the BlackBerry devices.

You use the Message Classification IT policy rule to configure one or more message classifications that users can apply to email messages. The message classification that the users select when they compose email messages determines the type of S/MIME message protection or PGP message protection that applies to the email messages.

If a user does not select a message classification, by default, the BlackBerry device applies the first classification in the message classification list on the BlackBerry device. You can change the order that the BlackBerry device lists the classifications in.

The message protection options on the BlackBerry device are limited to the types of encryption and digitial signing that the highly secure messaging packages on the BlackBerry device permit. When a user applies a message classification to an email message on a BlackBerry device, the user must select one type of message protection that the message classification permits, or accept the default type of message protection. If a user selects a message classification that requires signing, encryption, or signing and encryption of the email message, and the user did not install a highly secure messaging package on the BlackBerry device, the user cannot send the email message.

Create a message classification

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. In the list of IT policies, click an IT policy.
4. Click **Edit IT policy**.
5. On the **Security** tab, at the bottom of the screen, in the **Message Classification Display Name** field, type a display name that you want to appear in the Classifications list on BlackBerry devices.
6. Type a subject suffix that you want to append to the message subject in parentheses . For example, type the subject suffix (U) for a classification that is named Unclassified.
7. In the **Minimum Actions** drop-down list, click an action that a BlackBerry device user can perform to encode the message. For example, to permit users to select all of the encoding types for the secure messaging packages that they install on their BlackBerry devices, click **Signed**.
8. Click the **Add** icon.
9. Click **Save all**.

After you finish: If you create more than one message classification, order the message classifications in the list. By default, if a user does not select a message classification, the BlackBerry device applies the first message classification in the list.

Create a message classification based on an existing message classification

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. In the list of IT policies, click an IT policy.
4. Click **Edit IT policy**.
5. On the **Security** tab, at the bottom of the screen, click the **Copy** icon beside the message classification that you want to copy.
6. In the **Message classification display name** field, type a name for the message classification that you copied.
7. If necessary, change the subject suffix that you want to append, in parentheses, to the email message subject.
8. If necessary, click the minimum action for encoding the email message in the **Minimum Actions** drop-down list.
9. Click the **Add** icon.
10. Click **Save all**.

After you finish: Order the message classifications in the list. By default, if a user does not select a message classification, the BlackBerry device applies the first classification in the list.

Order message classifications

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. In the list of IT policies, click an IT policy.
4. Click **Edit IT policy**.
5. On the **Security** tab, at the bottom of the screen, click the **Up** or **Down** arrow icon beside the message classification that you want to move to prioritize the message classification.
6. Click **Save all**.

Delete a message classification

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. In the list of IT policies, click an IT policy.
4. Click **Edit IT policy**.
5. On the **Security** tab, at the bottom of the screen, click the **Delete** icon beside the message classification.
6. Click **Save all**.

Generating organization-specific encryption keys for PIN-message encryption

By default, all BlackBerry devices store a common PIN encryption key that they use to protect PIN messages. To limit the number of devices that can decrypt PIN messages that BlackBerry device users in your organization send from their devices, you can generate a new PIN encryption key that is stored on and known only to devices in your organization. A device that has a PIN encryption key that is specific to your organization can perform the following actions:

- can only encrypt PIN messages sent to other devices on your organization's network that use the same PIN encryption key
- can only decrypt PIN messages that are sent from devices that use the global PIN encryption key or PIN messages from other devices on your organization's network that use the same PIN encryption key
- cannot decrypt PIN messages sent from devices that use a PIN encryption key from another organization

You should generate a new PIN encryption key if you know that your current organization-specific PIN encryption key is compromised.

Generate a PIN encryption key

You can generate a PIN encryption key to make the BlackBerry devices in your organization use a PIN encryption key that is specific to your organization for PIN messaging.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology**.
2. Click **BlackBerry Domain**.

3. Click **Update peer-to-peer encryption key**.
4. Click **Create new key**.

Turn off BlackBerry services that the BlackBerry MDS Connection Service, BlackBerry Collaboration Service, and BlackBerry MVS provide

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. You can turn off the BlackBerry services if you want to enhance security, save bandwidth on the wireless network, or conserve system resources on the computer.

1. In the BlackBerry Administration Service, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **BlackBerry Enterprise Server**.
2. Click the instance that you want to change.
3. Click **Edit Instance**.
4. In the **External services turned on** drop-down list, click **No**.
5. Click **Save All**.
6. Restart the BlackBerry Enterprise Server.

Related information

Restarting BlackBerry Enterprise Server components, 392

When a BlackBerry device overwrites data in the BlackBerry device memory

A BlackBerry device continually runs the memory cleaner application during the Java based garbage collection process to overwrite data in the BlackBerry device memory that the BlackBerry device no longer uses.

The BlackBerry device runs the garbage collection process when any of the following conditions exist:

- You or a BlackBerry device user turns on content protection for the BlackBerry device.
- An application uses the RIM Cryptographic API to create a private key or symmetric key.
- A third-party application turns on the garbage collection process by registering with the memory cleaner application on the BlackBerry device. The memory cleaner application instructs applications to empty caches and to free the BlackBerry device memory that is associated with sensitive application data that the applications no longer use.
- A BlackBerry device user installs the S/MIME Support Package for BlackBerry smartphones on the BlackBerry device.
- A BlackBerry device user installs the PGP Support Package for BlackBerry smartphones on the BlackBerry device.

When the BlackBerry device runs the garbage collection process, the garbage collection process overwrites the data that the BlackBerry device no longer uses with zeroes, periodically runs the memory cleaner application, and overwrites the memory that the memory cleaner application frees.

Changing when a BlackBerry device cleans the BlackBerry device memory

By default, the memory cleaner application runs on a BlackBerry device when the BlackBerry device is inactive for a specified period of time. You or a BlackBerry device user can change when the memory cleaner application runs when any the following conditions exist:

- The BlackBerry device user synchronizes the BlackBerry device with a computer.
- The BlackBerry device user locks the BlackBerry device.
- The BlackBerry device locks after it is inactive for a specified period of time.
- The BlackBerry device user changes the time or time zone on the BlackBerry device.

To change when the memory cleaner application runs, you can use IT policies or the BlackBerry device user can turn on or turn off the memory cleaner application in the Security options on the BlackBerry device.

You or the BlackBerry device user cannot turn off the memory cleaner application on the BlackBerry device if any of the following conditions exist:

- You or the BlackBerry device user turns on content protection on the BlackBerry device.
- An application uses the RIM Cryptographic API to create a private key or symmetric key.
- An application that registers with the memory cleaner application requires that memory cleaning application be turned on.
- The BlackBerry device user installs the S/MIME Support Package for BlackBerry smartphones on the BlackBerry device and a private key exists on the BlackBerry device.
- The BlackBerry device user installs the PGP Support Package for BlackBerry smartphones on the BlackBerry device and a private key exists on the BlackBerry device.

If you or the BlackBerry device user turns on the memory cleaner application, Java based garbage collection process uses the memory cleaner application automatically. The garbage collection process overwrites data that the BlackBerry device no longer uses.

For more information about the IT policy rules that you can use to change when the memory cleaner application runs, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Best practice: Configuring additional memory cleaner settings for BlackBerry devices

Scenario	Recommendation
Remove decrypted content from BlackBerry device memory when the user holsters BlackBerry device.	Change the Force Memory Clean When Holstered IT policy rule to Yes.
Remove decrypted content from BlackBerry device memory when the BlackBerry device is idle.	Change the Force Memory Clean When Idle IT policy rule to Yes.
Start the memory cleaner after a specific amount of time has elapsed.	Set the Memory Cleaner Maximum Idle Time IT policy rule to the desired time (for example, 10 minutes).

For more information, see the *BlackBerry Enterprise Server Policy Reference Guide* and *S/MIME Support Package User Guide Supplement*.

Configuring the BlackBerry Enterprise Server environment

Best practice: Running the BlackBerry Enterprise Server

Best practice	Description
Do not change the startup type for the BlackBerry Enterprise Server services.	When you install or upgrade the BlackBerry Enterprise Server, the setup application configures the startup type for the BlackBerry Enterprise Server services to automatic or manual. For example, the setup application configures the startup type for the BlackBerry Mail Store Service, BlackBerry Policy Service, and BlackBerry Synchronization Service to manual. To avoid errors in the BlackBerry Enterprise Server, do not change the startup type for the BlackBerry Enterprise Server services.
Do not change the account information for BlackBerry Enterprise Server services.	When you install or upgrade the BlackBerry Enterprise Server, the setup application configures the account information for the BlackBerry Enterprise Server services. Do not change the account information for the BlackBerry Enterprise Server unless the BlackBerry Enterprise Server documentation specifies that you can.
Run the BlackBerry Configuration Panel as an administrator.	Consider the following guidelines if you are running the BlackBerry Configuration Panel on Windows Server 2008: • Log in to the computer with a user account that is in the Administrator group on the Windows Server. • Right-click the BlackBerry Configuration Panel icon and click Run as administrator.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configuring certain BlackBerry Enterprise Server components to use proxy servers

You can configure the BlackBerry MDS Connection Service and the BlackBerry Collaboration Service to use proxy servers to access web addresses on the Internet and your organization's intranet. You should use a proxy method that is consistent with the proxy method that other applications and servers in your organization use to access web content.

Proxy servers typically do not permit network traffic between servers that are on the same side of the firewall, so you can configure certain BlackBerry Enterprise Server components to use a .pac file, or to access the Internet directly through a proxy server. You can also configure multiple proxy servers to manage traffic to specific web addresses, and you can specify URLs that the BlackBerry Enterprise Server components can access without using a proxy server.

Related information

Configuring multiple BlackBerry Enterprise Server instances to use the same BlackBerry Enterprise Server component, 79

Configure a BlackBerry Enterprise Server component to use a .pac file

You can configure the BlackBerry MDS Connection Service and the BlackBerry Collaboration Service to use a .pac file. The BlackBerry Enterprise Server components support only one .pac file.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Expand the appropriate BlackBerry Enterprise Server component.
3. Click the instance that you want to change.
4. Click **Edit instance**.
5. On the **Proxy mappings** tab, in the **Universal resource locator** field, type the regular expression for the web address that you want the proxy mapping rule to control.
6. In the **Proxy type** drop-down list, perform one of the following actions:
   - To detect a .pac file automatically, click **AUTO**.
   - To specify the location of the .pac file, click **PAC**. In the **Proxy string** field, type the proxy server name, port number, and location of the .pac file using the following format: *<proxy_server>*:*<port>*/*<pac_filepath>*/*<pac_filename>*.

7. Click the **Add** icon for the proxy item. If you add more than one proxy item, use the **Up** and **Down** icons to set the priority of the proxy items.
8. Click the **Add** icon for the web address. If you add more than one web address, use the **Up** and **Down** icons to set the priority of the web addresses.
9. Click **Save all**.

Configure a BlackBerry Enterprise Server component to use a proxy server

You can configure the BlackBerry MDS Connection Service and the BlackBerry Collaboration Service to access web servers through a proxy server.

You can specify more than one proxy string in a proxy mapping rule for a web address. If the BlackBerry Enterprise Server component cannot access the web server using the first proxy string, it tries to access the web server using the subsequent proxy strings that you specify, until the component accesses the web server.

If the BlackBerry MDS Connection Service is configured to use a proxy server, BlackBerry device users can browse web sites that use HTTPS if the proxy server supports basic authentication only.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Expand the appropriate BlackBerry Enterprise Server component.
3. Click the instance that you want to change.
4. Click **Edit instance**.
5. On the **Proxy mappings** tab, in the **Universal resource locator** field, type the URL regular expression for the web address that you want the proxy mapping rule to control.
6. In the **Proxy type** drop-down list, perform one of the following actions:
   - To configure a proxy server, click **PROXY**. In the **Proxy string** field, type the proxy server name and port number using the following format: <*proxy_server*>:<*port*>.
   - To exclude the web address from routing through the proxy server, click **DIRECT**.
7. Click the **Add** icon for the proxy item. If you add more than one proxy item, use the **Up** and **Down** icons to set the priority for the proxy items.
8. Click the **Add** icon for the web address. If you add more than one web address, use the **Up** and **Down** icons to set the priority for the web addresses.
9. Click **Save all**.

Configure a BlackBerry Enterprise Server component to authenticate to a proxy server on behalf of BlackBerry devices

You can configure the BlackBerry MDS Connection Service and the BlackBerry Collaboration Service to authenticate to a proxy server on behalf of BlackBerry devices.

Before you begin: If you want to configure the BlackBerry MDS Connection Service to authenticate to a proxy server on behalf of BlackBerry devices, turn on authentication support for the BlackBerry MDS Connection Service.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Expand the appropriate BlackBerry Enterprise Server component.
3. Click the instance that you want to change.
4. Click **Edit instance**.
5. On the **Proxy mappings** tab, click the **Edit** button for a web address.
6. In the **Credentials** section, in the **User name** field, type the user name that the BlackBerry Enterprise Server component can use to connect to the proxy server that is defined for the web address.
7. In the **Password** and **Confirm password** fields, type the password for the user name.
8. Click the **Add** icon.
9. Click **Save all**.

Related information

Configure how BlackBerry devices authenticate to content servers, 181

Configuring the BlackBerry Administration Service to use a proxy server

If you want to allow the BlackBerry Administration Service to automatically download device.xml files, vendor.xml files, and information about BlackBerry Device Software bundles from the BlackBerry Infrastructure, and your organization uses a proxy server, you must configure the BlackBerry Administration Service to select and authenticate (if necessary) with the proxy server.

Configuring proxy selection for the BlackBerry Administration Service

You can configure the BlackBerry Administration Service to select a proxy server either manually or automatically.

To manually select a proxy server, you can use one of the following tools:

- Proxy Configuration Tool (proxycfg.exe) with Windows Server 2003 or earlier
- Network Shell Utility (netsh.exe) with Windows Server 2008
- Windows Internet Explorer

To automatically select a proxy server, you can use one of the following methods:

- enable the Web Proxy Autodiscovery Protocol using the BlackBerry Enterprise Trait Tool
- specify a URL for a PAC file using Windows Internet Explorer

Configuring manual proxy selection for a BlackBerry Administration Service instance

Depending on the operating system on the computer that hosts the BlackBerry Administration Service instance, you can use the Proxy Configuration Tool or the Network Shell Utility to manually select a proxy server for a BlackBerry Administration Service instance. You must configure manual proxy selection for all of the computers that host a BlackBerry Administration Service instance. Both the Proxy Configuration Tool and the Network Shell Utility store the proxy server settings in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\WinHttpSettings registry key. You must run both tools as an administrator.

The Proxy Configuration Tool works with Windows Server 2003 or earlier, and it is located in one of the following locations:

- For 32-bit Windows operating systems, the Proxy Configuration Tool is located at c:\Windows\system32\.
- For 64-bit Windows operating systems, the Proxy Configuration Tool is located at c:\Windows\sysWow64\.

For more information about the Proxy Configuration Tool, visit www.msdn.microsoft.com and search for proxycfg.exe.

The Network Shell Utility works with Windows Server 2008. For more information about the Network Shell Utility, visit technet.microsoft.com and search for Netsh.exe.

Configure manual proxy selection for the Windows account that runs the BlackBerry Administration Service

Perform this task on all of the computers that host a BlackBerry Administration Service instance.

1. On the computer that hosts the BlackBerry Administration Service, log in using the Windows account that runs the BlackBerry Administration Service.
2. Open Windows Internet Explorer.

3. Click **Tools** > **Internet Options**.
4. On the **Connections** tab, click **LAN settings**.
5. Select **Use a proxy server for your LAN**.
6. In the **Address** field, type the address for the proxy server.
7. In the **Port** field, type the port number for the proxy server.
8. Click **OK**.
9. Click **OK**.

Windows Internet Explorer stores the settings for the proxy server in the HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings registry key.

Configure the BlackBerry Administration Service to use the Web Proxy Autodiscovery Protocol to select a proxy server automatically

If you want to configure the BlackBerry Administration Service to use the Web Proxy Autodiscovery Protocol to select a proxy server automatically, you must use the BlackBerry Enterprise Trait Tool. The Web Proxy Autodiscovery Protocol uses DHCP and DNS to find a PAC file. Perform this task on any computer that hosts a BlackBerry Administration Service instance.

CAUTION: If the proxy server authenticates using HTTP basic authentication, the Web Proxy Autodiscovery Protocol file must be on a computer that is separate from the proxy server and uses Windows authentication or anonymous authentication.

1. On the computer that hosts the BlackBerry Administration Service, at the command prompt, navigate to the folder that contains the TraitTool.exe file.
2. To turn on Web Proxy Autodiscovery Protocol, type **traittool -global -trait BASIsProxyWPADOptionEnabled -set 1**.

Turn off Web Proxy Autodiscovery Protocol

Perform this task on any computer that hosts a BlackBerry Administration Service instance.

1. On the computer that hosts the BlackBerry Administration Service, at the command prompt, navigate to the folder that contains the TraitTool.exe file.
2. To turn off Web Proxy Autodiscovery Protocol, type **traittool -global -trait BASIsProxyWPADOptionEnabled -erase**.

Configure the BlackBerry Administration Service to use a PAC file to select a proxy server automatically

Before you begin:

Obtain the URL for the PAC file.

Perform this task on all of the computers that host a BlackBerry Administration Service instance.

CAUTION: If the proxy server authenticates using HTTP basic authentication, the PAC file must be on a computer that is separate from the proxy server and uses Windows authentication or anonymous authentication.

1. On the computer that hosts the BlackBerry Administration Service instance, log in using the Windows account that runs the BlackBerry Administration Service.
2. Open Windows Internet Explorer.
3. Click **Tools** > **Internet Options**.
4. On the **Connections** tab, click **LAN settings**.
5. Select **Use automatic configuration script**.
6. In the **Address** field, type the URL for the PAC file.
7. Click **OK**.
8. Click **OK**.

Configuring the BlackBerry Administration Service to authenticate with a proxy server

If your organization's proxy server requires authentication, you must configure the BlackBerry Administration Service to authenticate with the proxy server.

If the proxy server uses Windows authentication, you must configure the proxy server to authenticate the Windows account that runs the BlackBerry Administration Service.

If your proxy server uses HTTP basic authentication, you can configure the user name and password for HTTP basic authentication using the BlackBerry Enterprise Trait Tool. You can specify the credentials for either the entire BlackBerry Domain or for individual BlackBerry Administration Service instances. The BlackBerry Administration Service tries the credentials that you specify for the BlackBerry Administration Service instance first and then tries the credentials that you specify for the BlackBerry Domain.

Configure the BlackBerry Administration Service to use HTTP basic authentication

You use the BlackBerry Enterprise Trait Tool to configure the BlackBerry Administration Service to use HTTP basic authentication to authenticate with a proxy server. HTTP basic authentication requires a user name and password for authentication.

1. On the computer that hosts the BlackBerry Administration Service, at the command prompt, navigate to the folder that contains the TraitTool.exe file.
2. Perform one of the following tasks:

Task	Steps
Specify the credentials for HTTP basic authentication that your organization's BlackBerry Domain uses.	1. Type **traittool -global -trait BASProxyBasicAuthUID -set** <**user_name**>, where <*user_name*> is the user name (for example, user01@blackberry.com or blackberry.com\user01). 2. Type **traittool -global -trait BASProxyBasicAuthPassword -set** <**password**>, where <*password*> is the password.
Specify the credentials for HTTP basic authentication that a specific BlackBerry Administration Service instance uses.	1. Type **traittool -BASServer** <**name**> **-trait BASProxyBasicAuthUID -set** <**user_name**>, where <*name*> is the host name of the computer that hosts the BlackBerry Administration Service instance and <*user_name*> is the user name (for example, user01@blackberry.com or blackberry.com \user01) for that computer. 2. Type **traittool -BASServer** <**name**> **-trait BASProxyBasicAuthPassword -set** <**password**>, where <*name*> is the host name of the computer that hosts the BlackBerry Administration Service instance and <*password*> is the password for the computer.

Delete credentials for HTTP basic authentication

1. On the computer that hosts the BlackBerry Administration Service, at the command prompt, navigate to the folder that contains the TraitTool.exe file.
2. Perform one of the following tasks:

Task	Steps
Delete the user name and password that all of the BlackBerry Administration Service instances in your organization's BlackBerry Domain use for HTTP basic authentication.	1. Type **traittool -global -trait BASProxyBasicAuthUID -erase**. 2. Type **traittool -global -trait BASProxyBasicAuthPassword -erase**.
Delete the user name and password for the computer that a single BlackBerry Administration Service instance in your organization's BlackBerry Domain uses for HTTP basic authentication.	1. Type **traittool -BASServer** <**name**> **-trait BASProxyBasicAuthUID -erase**. 2. Type **traittool -BASServer** <**name**> **-trait BASProxyBasicAuthPassword -erase**.

Configuring multiple BlackBerry Enterprise Server instances to use the same BlackBerry Enterprise Server component

To help make a BlackBerry Domain more scalable, you can configure multiple BlackBerry Enterprise Server instances to use the same BlackBerry MDS Connection Service or BlackBerry Collaboration Service. If a BlackBerry Domain contains one BlackBerry Enterprise Server, all of the BlackBerry Enterprise Server components are associated with that BlackBerry Enterprise Server automatically.

Configure multiple BlackBerry Enterprise Server instances to use the same BlackBerry MDS Connection Service

You can configure multiple BlackBerry Enterprise Server instances to use the same central push server to transfer application data to and from BlackBerry devices and to manage HTTP requests from the BlackBerry Browser.

Before you begin: Specify a BlackBerry MDS Connection Service as a central push server.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Conection Service**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Supported Dispatcher instances** tab, in the **Available Dispatcher instances** list, click the BlackBerry Enterprise Server instance that you want to use the BlackBerry MDS Connection Service.
5. Click **Add**.
6. Repeat steps 4 and 5 for each BlackBerry Enterprise Server instance that you want to have use the BlackBerry MDS Connection Service.
7. Click **Save all**.

Related information

Specifying a BlackBerry MDS Connection Service as a central push server, 180

Configure multiple BlackBerry Enterprise Server instances to use the same BlackBerry Collaboration Service

You can configure multiple BlackBerry Enterprise Server instances to use the same BlackBerry Collaboration Service to connect to your organization's instant messaging server, and to manage requests from the collaboration client on users' BlackBerry devices.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Collaboration**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Supported Dispatcher instances** tab, in the **Available Dispatcher instances** list, click the BlackBerry Enterprise Server instance that you want to use the BlackBerry Collaboration Service.
5. Click **Add**.
6. Repeat steps 4 and 5 for each BlackBerry Enterprise Server instance that you want to use the BlackBerry Collaboration Service.
7. Click **Save all**.

Configuring support for Unicode languages

Configure support for Unicode languages

You can make sure that the messaging application can display the Unicode messages that the BlackBerry device sends by configuring the BlackBerry Enterprise Server to support Unicode languages (for example, Japanese, Korean, or Simplified Chinese).

1. On the computer that hosts the BlackBerry Enterprise Server, on the taskbar, click **Start** > **Run**.
2. Type **regedit**.
3. Click **OK**.
4. Perform one of the following actions:

- If you are running a 32-bit version of Windows, go to HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion \BlackBerry Enterprise Server\Agents.
- If you are running a 64-bit version of Windows, go to HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node \Research In Motion\BlackBerry Enterprise Server\Agents.

5. If the **MAPIEncoding** registry key exists, perform one of the following actions:
   - Delete the key.
   - Change the value of the key to **1**.
6. Perform one of the following actions:
   - If you are running a 32-bit version of Windows, go to HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion \BlackBerry Enterprise Server\Setup.
   - If you are running a 64-bit version of Windows, go to HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node \Research In Motion\BlackBerry Enterprise Server\Setup.
7. Verify that the **ConfigKeystoreCountry** registry key is set to one of the following values, depending on your organization's environment:
   - CN for Simplified Chinese
   - JP for Japanese
   - KR for Korean
8. In the Windows Services, restart the BlackBerry Dispatcher.

Related information

Restarting BlackBerry Enterprise Server components, 392

Change the character encoding that the BlackBerry Enterprise Server uses to send Unicode messages

By default, when the BlackBerry Enterprise Server receives Unicode messages from BlackBerry devices, it uses UTF-8 character encoding to process the Unicode messages. If email applications cannot correctly display Unicode messages that devices send (for example, if email applications cannot display attachment file names or contact lists correctly), you can configure the BlackBerry Enterprise Server to select another character encoding to use to process Unicode messages.

Before you begin: Configure support for Unicode languages.

1. On the computer that hosts the BlackBerry Enterprise Server, on the taskbar, click **Start** > **Run**.
2. Type **regedit**.

3. Click **OK**.
4. Perform one of the following actions:
   - If you are running a 32-bit version of Windows, go to HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion \BlackBerry Enterprise Server\Agents.
   - If you are running a 64-bit version of Windows, go to HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node \Research In Motion\BlackBerry Enterprise Server\Agents.
5. Create a DWORD value that is named **AutoSelectOutgoingEncoding**.
6. Double-click the new DWORD value.
7. In the **Value data** field, perform one of the following actions:
   - To configure the BlackBerry Enterprise Server to select the most appropriate character encoding when it encodes plain-text messages, type **1**. If the BlackBerry Enterprise Server cannot identify which character encoding to use, the BlackBerry Enterprise Server encodes plain-text messages in UTF-8.
   - To configure the BlackBerry Enterprise Server to select the most appropriate character encoding when it encodes email messages that use RTF or HTML, type **2**. If the BlackBerry Enterprise Server cannot identify which character encoding to use, the BlackBerry Enterprise Server encodes email messages that use RTF or HTML in UTF-8.
   - To configure the BlackBerry Enterprise Server to select the most appropriate character encoding when it encodes plain-text messages and email messages that use RTF or HTML, type **3**. If the BlackBerry Enterprise Server cannot identify which character encoding to use, the BlackBerry Enterprise Server encodes all email messages in UTF-8.
8. In the Windows Services, restart the BlackBerry Dispatcher.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configure support for Unicode text in calendars on BlackBerry devices in a Microsoft Exchange environment

You must complete this task for all Microsoft Exchange versions to ensure calendar items use the correct Unicode characters in fields such as subject, location, or notes.

Before you begin: In a Microsoft Exchange 2003 environment, install the following hotfixes for wireless calendar synchronization:

- Visit http://support.microsoft.com/kb/913643 to download and install the required hotfix on the messaging server.

- Visit http://support.microsoft.com/kb/923537/en-us to download and install the required hotfix on the computer that will host the BlackBerry Enterprise Server.

1. On the BlackBerry Enterprise Server, on the **Start** menu, click **Run**.
2. Type **regedit**.
3. Click **OK**.
4. Perform one of the following actions:
   - If you are running a 32-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\Research In Motion\BlackBerry Enterprise Server\Agents.
   - If you are running a 64-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\WOW6432Node\Research In Motion\BlackBerry Enterprise Server\Agents.
5. Create a DWORD value that is named **SetLocaleIDs**.
6. Set the value to **1**.
7. In the Windows Services, restart the BlackBerry Messaging Agent.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configuring user accounts

Creating user groups

You can create user groups and assign user accounts to user groups based on custom criteria, such as user location, organizational group, or BlackBerry device model. User accounts that are part of a user group can exist on multiple BlackBerry Enterprise Server instances in the BlackBerry Domain.

Create a group to manage similar user accounts

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.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Create a group**.
3. In the **Group information** section, type a name and description for the group.
4. Click **Save**.

After you finish:

- Add properties to the group.
- Add user accounts to the group.

Related information

Change the properties of a group, 287
Add user accounts to a group, 84

Add user accounts to a group

You can add user accounts to a group to assign the properties of the group to user accounts automatically.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for the user accounts.
4. Select the user accounts.
5. In the **Add to user configuration** list, click **Add group**.
6. In the **Available groups** list, click the group that you want to add the user accounts to.
7. Click **Add**.
8. Click **Save**.

Adding a user account to the BlackBerry Enterprise Server

If you add a user account to the BlackBerry Enterprise Server, you are not required to locate the Microsoft Exchange mailbox for the BlackBerry device that the user account is associated with or the routing group that the BlackBerry Enterprise Server is located in.

Related information

Assigning BlackBerry devices to users, 91

Add a user account

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

Before you begin: If required, create a group of user accounts so that you can manage user accounts that are similar.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Create a user**.
3. Search for a user account.
4. Select the check box beside the display name for the user account.
5. Click **Continue**.
6. If your organization's environment includes multiple BlackBerry Enterprise Server instances, select the BlackBerry Enterprise Server that you want to add the user account to.
7. If groups exist in the **Available groups** list, click at least one group that you want to add the user account to.

8. Click **Add**.
9. To select an activation option, perform one of the following actions:

Option	Step
Specify an activation password for the user account.	1. Click **Create a user with activation password**. 2. In the **Set activation password**, section, type and confirm an activation password. The password must not contain special characters. Some BlackBerry devices do not support special characters and do not unlock when a user types a password that contains special characters. 3. In the **Password expiration (hours)** field, type the amount of time, in hours, that you want to elapse before the activation password expires. 4. Click **Create user**.
Generate an activation password for the user account automatically.	Click **Create a user with generated activation password**.
Activate the user account without using an activation password.	Click **Create a user without activation password**.

Related information

Assigning BlackBerry devices to users, 91
Managing user accounts, 288

Create a user account that is not in the contact list in the BlackBerry Configuration Database

You can create a user account for a user even if the did not yet synchronize the contact information for the user account to the BlackBerry Configuration Database. If the BlackBerry Mail Store Service did not synchronize the contact information and you create a user account, the BlackBerry Administration Service does not display the user account in the search results.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User.**
2. Click **Create a user**.
3. Search for a user account.
4. Click **Add user from company directory**.
5. In the **Email address** field, type the email address, in SMTP format, of the user account that you want to add.
6. Click **Find user in company directory**.
7. Click **Save user to available user list and Create BlackBerry Enabled User**.

8. If you installed multiple BlackBerry Enterprise Server instances, select the BlackBerry Enterprise Server that you want to add the user account to.
9. Click **Continue.**
10. Type and confirm an activation password. The password must not contain special characters. Specific BlackBerry devices do not support special characters and do not unlock when a user types a password that contains special characters.
11. In the **Password expiration** field, type the amount of time, in hours, that can elapse before the activation password expires.
12. Click **Create user**.

Export a list of user accounts

You can 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 the user ID, display name, PIN and email address. You can import the list of user accounts to another BlackBerry Enterprise Server.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User.**
2. Click **Manage users**.
3. Search for one or more user accounts.
4. Select the checkboxes beside the display names of the appropriate user accounts.
5. In the **Export users** list, click **Export selected users**.
6. Click **Download file**.
7. Save the .csv file.

Importing 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 required information to activate the user accounts on a BlackBerry Enterprise Server.

The .csv file can include the following information:

- user accounts that you want to create
- names of the groups you want to add the user accounts to
- activation passwords and expiry times that you want to assign to the user accounts

The BlackBerry Administration Service processes actions in the order that they appear in the .csv file. If the BlackBerry Administration Service encounters an error that is specific to an action during the import process (for example, an action is incorrectly formatted in the .csv file), the BlackBerry Administration Service continues to process the remaining actions that are listed in the file and displays an error message for the action that the BlackBerry Administration Service could not process.

The import process can take a long time (more than 30 minutes) to complete if you add more than 2000 user accounts.

Fields in a .csv file that contain user account information

The BlackBerry Administration Service uses a .csv file to add user account information to the BlackBerry Enterprise Server. The following table lists the fields in the .csv file that might be populated when you import user account information.

Field	Description
Email Address	The field specifies the email address for the user account.
SRP ID	This field specifies the SRP ID for the BlackBerry Enterprise Server that you want to add the user account to.
Group Names	This field specifies the names of groups that you want to add the user account to.
Activation Password Operation	This field specifies whether an activation password is required to activate the user account and whether that password will be specified by the administrator or the BlackBerry Administration Service. The activation password value specified in this field can either be "specify", "none", or "generate" in lower case only. The activation password operation must be the same on each line in the .csv file. If the field is set to "specify", the activation password and the expiry time (in hours) are optional fields in the .csv file. If the activation password and the expiry time values are not included in the .csv file, you will be prompted to specify these values the after uploading the .csv file. If you specify the activation password and the expiry time for the user accounts, the values must be provided on every line of the csv file. If the field is set to "generate", the password is automatically generated by the BlackBerry Administration Service and the final two fields of each .csv line must be empty. The activation password will expire if the user does not activate the BlackBerry device on the BlackBerry Enterprise Server before the password timeout elapses. The default value is 48 hours. If the field is set to "none", the user account will be created without an activation password and the final two fields of each .csv line must be empty. To activate a BlackBerry device on the BlackBerry Enterprise Server over the wireless network, an activation password is required.
Activation Password	This field specifies the activation password for the user account if an activation password is required.

Field	Description
Activation Password Expiry	This field specifies the amount of time, in hours, that can elapse before the activation password expires if an activation password is required. The activation password will expire if the user does not activate the BlackBerry device on the BlackBerry Enterprise Server before a default value of 48 hours elapses.

Example: Importing user accounts to a BlackBerry Enterprise Server

```
"Email Address","SRP ID","Group Names","Activation Password Operation","Activation
Password","Activation Password Expiry"

"wbarichak@example.com","WBARICHAK0033","Admins","specify", "asdf","24"
"jbuac@example.com","JBUAC0011,"Admins","specify", "asdf","24"
```

Import multiple user accounts from a .csv file

You can import a list of user accounts from a .csv file to a BlackBerry Enterprise Server so that you can manage the user accounts.

Before you begin: Create a .csv file.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Click **Manage multiple users from an import list**.
4. In the **Manage multiple users from an import list** section, click **Browse**.
5. Navigate to the .csv file that contains the user accounts that you want to import.
6. Click **Next**.
7. Perform the appropriate actions for the user accounts.

Create multiple user accounts by importing the user accounts from a .csv file

You can import a list of user accounts from a .csv file and add them to a BlackBerry Enterprise Server. The user accounts must exist on your organizations messaging server.

Before you begin: Create the .csv file.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Create a user**.

3. Click **Import new users**.
4. In the **Import users from a list** section, click **Browse**.
5. Navigate to the .csv file that contains the user accounts that you want to import.
6. Click **Continue**.
7. Perform the appropriate actions for the user accounts.

Assigning BlackBerry devices to users

8

Preparing to distribute a BlackBerry device

Before you distribute a BlackBerry device to a user, you can configure the BlackBerry Enterprise Server to synchronize email messages that the user previously sent and received on a supported BlackBerry device. You can synchronize messages for a new user or for a user whose PIN changed when they received a replacement BlackBerry device.

When the BlackBerry Enterprise Server synchronizes messages onto a BlackBerry device, it applies the message filter rules and redirection settings that are specific to the user account.

Change how the BlackBerry Enterprise Server downloads a user's existing email messages onto the BlackBerry device

By default, the BlackBerry Enterprise Server synchronizes the headers of 200 email messages from the previous 5 days to a BlackBerry device when you activate it. If you change the BlackBerry Enterprise Server settings so that it synchronizes the headers and body of messages to a BlackBerry device when you activate it, the BlackBerry Enterprise Server can synchronize up to 3000 messages from the previous 30 days.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Message prepopulation settings** section, perform the following actions:
   - To specify if you want full message bodies delivered or just message headers, in the **Send headers only** field, select an option.

- To specify the number of previous days that you want to synchronize messages from, in the **Prepopulation By message age** field, type a number.
- To specify the maximum number of messages that you want to synchronize, in the **Prepopulation By message count** field, type a number.

5. Click **Save all**.

Prevent the BlackBerry Enterprise Server from synchronizing existing email messages onto a BlackBerry device

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Message prepopulation settings** section, perform the following actions:
   - In the **Prepopulation by message age** field, type **0**.
   - In the **Prepopulation by message count** field, type **0**.

5. Click **Save all**.

Assigning BlackBerry devices to user accounts

To assign BlackBerry devices to user accounts and activate the BlackBerry devices, you can use any of the following methods:

Method	Description
BlackBerry Administration Service	You can activate BlackBerry devices before you distribute them to users by connecting the BlackBerry devices to a computer and logging in to the BlackBerry Administration Service.

Method	Description
over the wireless network	New BlackBerry device users and users that are receiving replacement BlackBerry devices can activate the BlackBerry devices without requiring a physical connection to your organization's network.
over the LAN	New BlackBerry device users and users that are receiving replacement BlackBerry devices can activate the BlackBerry devices by connecting the BlackBerry devices to a computer that hosts the BlackBerry Desktop Manager.
BlackBerry Web Desktop Manager	New BlackBerry device users and users that are receiving replacement BlackBerry devices can activate the BlackBerry devices by connecting the BlackBerry devices to a computer that hosts the BlackBerry Web Desktop Manager.
over your organization's Wi-Fi network	You can activate Wi-Fi enabled BlackBerry devices over your organization's Wi-Fi network.

If you add a user account that was previously located on another BlackBerry Enterprise Server in a different BlackBerry Domain, or the user previously used the BlackBerry Desktop Redirector, you must assign a BlackBerry device to the user account using the BlackBerry Administration Service.

Related information

Managing BlackBerry Java Applications and BlackBerry Device Software, 136

Option 1: Activate a BlackBerry device using the BlackBerry Administration Service

Before you begin: If necessary, prepare a BlackBerry device so that you can redistribute it to a user.

1. Connect the BlackBerry device to a computer that can access the BlackBerry Administration Service.
2. On the **Devices** menu, expand **Attached devices**.
3. Click **Manage current device**.
4. Click **Assign current device**.
5. Search for a user account.
6. In the search results, click the display name for a user account.
7. Click **Associate user**.
8. Click **Assign current device**.

Option 2: Activating a BlackBerry device over the wireless network

To activate a BlackBerry device over the wireless network, you assign an activation password to a user account. The user receives the activation password in an email message and associates the BlackBerry device with the email account by typing the password on the BlackBerry device.

Save bandwidth by synchronizing organizer data over the LAN

When users activate BlackBerry devices over the wireless network, by default, the BlackBerry Enterprise Server synchronizes the initial download of organizer data over the wireless network. To save bandwidth, you can configure an IT policy to synchronize the initial download of organizer data through the BlackBerry Router and over your organization's LAN when users connect their BlackBerry devices to a computer that hosts the BlackBerry Device Manager.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. Click **Default**.
4. Click **Edit IT policy**.
5. On the **PIM Synchronization** tab, in the **Disable Wireless Bulk Loads** rule, in the drop-down list, click **Yes**.
6. Click **Save all**.

Wireless activation

The wireless activation process activates BlackBerry devices on the BlackBerry Enterprise Server over the wireless network. Neither you nor the users are required to connect the BlackBerry devices to a computer to complete the activation process.

You can use wireless activation process to activate a large number of BlackBerry devices over the wireless network. When users want to activate BlackBerry devices on the BlackBerry Enterprise Server over the wireless network, they must notify you. You can use the BlackBerry Administration Service to configure activation passwords and distribute the passwords to the users.

The BlackBerry Enterprise Solution can begin the wireless activation process automatically or when users open the activation application on the BlackBerry devices and type an activation password and email address. When the activation process completes, users can send email messages from and receive email messages on their BlackBerry devices.

When you initiate the wireless activation process, the BlackBerry Enterprise Server sends an email message with an etp.dat attachment from the blackberry.net domain to the user's email application. To make sure that the message is not blocked or modified, add the blackberry.net domain to the allowed list in the anti-virus and anti-spam software applications used by the messaging server or gateway.

Activation passwords

The BlackBerry Enterprise Server activates a BlackBerry device over the wireless network using the wireless activation authentication protocol and an activation password that is specific to the user account associated with the BlackBerry device.

Item	Description
length of the activation password	Typical activation passwords are four to eight characters long. Activation passwords are limited to the following character lengths: • BlackBerry device: 31 characters • BlackBerry Administration Service : 20 characters • KeyGenPassword field that stores the password in the BlackBerry Configuration Database: 50 characters
character support	Activation passwords can include any type of character
security	Wireless activation is designed so that short activation passwords do not compromise the security of the protocol. You must distribute the activation password to the authenticated user securely. If the user receives the activation password, but does not activate the BlackBerry device on the BlackBerry Enterprise Server, a potentially malicious user who can access the activation password can connect another BlackBerry device to the BlackBerry Enterprise Server and assume the identity of the intended user. When a user activates a BlackBerry device on the BlackBerry Enterprise Server, the activation password becomes inactive and a potentially malicious user cannot reuse it to activate another BlackBerry device. If a user receives an activation password, you cannot generate a new activation password for the user until the activation password expires. An activation password expires after 48 hours by default. You can configure an activation to password expire earlier than the default value of 48 hours.
expiry time	An activation password is no longer valid if any of the following events occur: • the user does not activate the BlackBerry device on the BlackBerry Enterprise Server before the default value of 48 hours elapses • the user types the activation password incorrectly five consecutive times • the BlackBerry Enterprise Server activates a BlackBerry device using the activation password

Customize the activation password

You can customize the type of activation password and the number of characters the password can contain that you send to BlackBerry devices in a BlackBerry Domain. You can also change the length of time that the activation password exists before it expires.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Wireless activations**.
2. Click **Device activation settings**.
3. Click **Edit activation settings**.
4. In the **Password settings** section, perform the following actions:
   - To change the activation password length, in the **Auto-generated password length** field, type a character length.
   - To change the activation password type, in the **Auto-generated password type** drop-down list, click a password type.
   - To change the length of time that the activation password exists before it expires, in the **Auto-generated password lifespan (hours)** field, type the number of hours.
5. Click **Save all**.

Customize the activation message

To provide information to help troubleshoot activation issues that a user might encounter or to make sure that the activation message that users receive on their computers conforms to your organization's messaging policies, you can customize the default activation message.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Wireless activations**.
2. Click **Device activation settings**.
3. Click **Edit activation settings**.
4. In the **Email initialization message** section, perform the following actions:
   - In the **Sender address** field, type the email address for the administrator account.
   - In the **Custom activation message** field, type the subject, and message.
5. Click **Save all**.

Send an activation password to a user

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.

4. In the search results, click the display name for the user account.
5. In the **Device activation** list, click **Specify an activation password**.
6. In the **Activation password** and **Confirm password** fields, type an activation password. The password must not contain special characters. Some BlackBerry devices do not support special characters and do not unlock when a user types a password that contains special characters.
7. In the **Password expiration (hours)** field, type the amount of time that can elapse before the activation password expires.
8. Click **Specify an activation password**.

Send an activation password to multiple users

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for one or more user accounts.
4. Select the checkboxes beside the display names of the appropriate user accounts.
5. In the **Device activation** list, click **Specify an activation password**.
6. In the **Activation password** and **Confirm password** fields, type an activation password. The password must not contain special characters. Some BlackBerry devices do not support special characters and do not unlock when a user types a password that contains special characters.
7. In the **Password expiration (hours)** field, type the amount of time, in hours, that can elapse before the activation password expires.
8. Click **Specify an activation password**.

Option 3: Activating BlackBerry devices over the LAN

Users can activate BlackBerry devices by connecting them to computers that the BlackBerry Desktop Manager is associated with. During the activation process, the BlackBerry Desktop Manager prompts users to associate the BlackBerry devices with their work email accounts and generate encryption keys.

When users complete the activation process, the BlackBerry Enterprise Server sends email messages and organizer data to the BlackBerry devices through the BlackBerry Router. If a connection to the BlackBerry Router is interrupted, the data transfer continues over the wireless network.

Option 4: Activating BlackBerry devices using the BlackBerry Web Desktop Manager

Users can activate their BlackBerry devices by connecting them to computers using a USB cable or Bluetooth connection and logging in to the BlackBerry Web Desktop Manager. During the activation process, the BlackBerry Web Desktop Manager prompts users to associate the BlackBerry device with their email accounts and generate encryption keys.

When users complete the activation process, the BlackBerry Enterprise Server synchronizes email messages and organizer data to BlackBerry devices through the BlackBerry Router. If a connection to the BlackBerry Router is interrupted, the data transfer continues over the wireless network.

Option 5: Activating BlackBerry devices over an enterprise Wi-Fi network

Users can activate Wi-Fi enabled BlackBerry devices over an enterprise Wi-Fi network in environments that have the following characteristics:

- BlackBerry devices can connect to the enterprise Wi-Fi network but cannot connect to the BlackBerry Infrastructure.
- Users did not install BlackBerry Desktop Manager on their computers and cannot access BlackBerry Web Desktop Manager.
- You want to deploy and activate a large number of BlackBerry devices.

To activate BlackBerry devices over the enterprise Wi-Fi network, you must configure the BlackBerry Router as an SMTP client (also known as a Mail User Agent). As an SMTP client, the BlackBerry Router communicates with an SMTP server, that sends an ETP message to the user. The ETP message is the email message that the BlackBerry Router sends to the user’s mailbox during the activation process.

You can configure the BlackBerry Router to act as a gateway for BlackBerry device activations over the enterprise Wi-Fi network and as a gateway for other network traffic such as email messages, data, or calendar synchronization, or to act only as a gateway for BlackBerry device activations over the enterprise Wi-Fi network. If you choose to configure the BlackBerry Router only as a gateway for BlackBerry device activations over the enterprise Wi-Fi network, you must configure the BlackBerry Router as part of a chain of BlackBerry Router instances and make sure that one or more BlackBerry Router instances in the chain can act as a gateway for other network traffic.

For more information about Wi-Fi enabled BlackBerry devices, see the *BlackBerry Enterprise Server Feature and Technical Overview*.

Prerequisites: Configuring a BlackBerry Router for BlackBerry device activations over the enterprise Wi-Fi network

- On the computer that you installed the BlackBerry Router, or on a remote computer, configure an SMTP service that the BlackBerry Router can use. For more information, see the documentation for the Windows Server.
- To restrict the BlackBerry Router so that it acts only as a gateway for BlackBerry device activations over the enterprise Wi-Fi network, on a computer that does not host a BlackBerry Enterprise Server, install a BlackBerry Router whose only purpose is to provide a connection to Wi-Fi enabled BlackBerry devices over the enterprise Wi-Fi network. Configure the BlackBerry Router as part of a chain of BlackBerry Router instances and make sure that one or more BlackBerry Router instances in the chain can act as a gateway for other network traffic such as email messages, data, or calendar synchronization.
- Verify that the wireless access points can connect to the BlackBerry Router that you configured for BlackBerry device activations over the enterprise Wi-Fi network.
- Verify that each BlackBerry Enterprise Server can connect to a BlackBerry Router that you configured for BlackBerry device activations over the enterprise Wi-Fi network.
- Create a user account and activation password on the BlackBerry Enterprise Server for each new BlackBerry device.

Configure a BlackBerry Router to permit BlackBerry device activations over the enterprise Wi-Fi network

1. On the computer that hosts the BlackBerry Router, on the taskbar, click **Start** > **Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. On the **OTA WIFI Activation** tab, select the **Permit wireless activation in your WLAN environment** check box.
3. Optionally, to restrict the BlackBerry Router so that it acts as a gateway for wireless activations over the enterprise Wi-Fi network and not as a gateway for other network traffic such as email messages, data, or calendar synchronization, select the **Prevent all serial bypass traffic through this router except WLAN activations** check box. Only restrict the BlackBerry Router if you configured more than one BlackBerry Router instance.
4. To specify how the BlackBerry Router locates the SMTP server, in the **Activation Gateway Settings** section, select one of the following options:
    - To permit the BlackBerry Router to determine which SMTP server it uses for ETP traffic based on the mail exchange record of the host domain, select **Use MX Lookup to obtain SMTP server**.
    - To provide the SMTP server name and port number for the BlackBerry Router, select **Explicitly provide SMTP server name and port**. Type the server name and the server port number for the SMTP server.
5. If the SMTP server requires authentication, specify the SMTP login name and SMTP password.
6. In the **From address for ETP messages** field, type the email address that you want to use as the From address. The ETP message is the email message that the BlackBerry Router sends to the users' mailboxes during the activation process.

7. Click **Apply**.
8. Click **OK**.
9. In the Windows Services, restart the BlackBerry Router.

After you finish: Instruct users to activate the Wi-Fi enabled BlackBerry devices.

Activate a Wi-Fi enabled BlackBerry device

If you want to activate a Wi-Fi enabled BlackBerry device using the enterprise Wi-Fi network, you can instruct a BlackBerry user to perform the following task on the BlackBerry device. If you want to reactivate a BlackBerry device, you must create a new activation password for the BlackBerry device.

1. On the BlackBerry device, in the device options, click **Advanced Options**.
2. Click **Enterprise Activation**.
3. Type the activation email address.
4. Type the activation password.
5. In the **Activation Server Address** field, type the IP address for the BlackBerry Router that the BlackBerry device can use to activate over the enterprise Wi-Fi network.
6. In the menu, click **Activate**.

After you finish:

- For more information, see the user guide for the BlackBerry device.
- To view the activation status, in the BlackBerry Administration Service, on the **Wireless** > **View activations** page, search for the user account. Confirm that the activation is successful.

Related information

Restarting BlackBerry Enterprise Server components, 392

Troubleshooting: Connections to the Wi-Fi network, 478

Configuring BlackBerry Enterprise Server high availability

9

Check the health of a BlackBerry Enterprise Server

If you configured BlackBerry Enterprise Server high availability, you can check the health of a BlackBerry Enterprise Server instance to verify that it is running as expected.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **High availability**.
2. Click **High availablity summary**.
3. In the **Host instance name** field, click the name of a BlackBerry Enterprise Server pair.
4. Click **More**.

The BlackBerry Administration Service displays the status of the health parameters.

Availability state and failover status of the BlackBerry Enterprise Server

When you check the health of a BlackBerry Enterprise Server instance in the BlackBerry Administration Service, you can also check the availability state and failover status of the BlackBerry Enterprise Server instance.

The availability state specifies whether the BlackBerry Enterprise Server instance is a primary instance or standby instance according to information from the BlackBerry Configuration Database. If you did not connect the BlackBerry Enterprise Server to the BlackBerry Configuration Database, the BlackBerry Administration Service might not display up-to-date information about the availability state.

The failover status specifies whether the BlackBerry Enterprise Server instance is a primary instance or standby instance and whether the BlackBerry Enterprise Server instance is running as expected. The BlackBerry Administration Service receives this information in real time from the BlackBerry Enterprise Server instance so that the failover status is always up-to-date.

How the BlackBerry Enterprise Server uses health parameters

The BlackBerry Enterprise Server uses health parameters to define the failover and promotion thresholds. The health parameters indicate if a BlackBerry Enterprise Server service or component is healthy or unhealthy. For example, the value for the Wireless network access health parameter indicates whether the BlackBerry Router can access the wireless network. The health parameters are identical for both the failover threshold and the promotion threshold. You can choose the health parameters for the services and components that are important to your organization.

After you choose the health parameters that you want the BlackBerry Enterprise Server to use to determine when an automatic failover process should occur, the failover process can occur automatically if all of the following conditions are present:

- The values for the health parameters that you define as part of the failover threshold for the primary BlackBerry Enterprise Server indicates whether a service or component is unhealthy.
- The values for the health parameters that you define as part of the promotion threshold for the standby BlackBerry Enterprise Server indicate whether all the required services and components are healthy.
- If you configure a health parameter for the primary BlackBerry Enterprise Server so that it is above the failover threshold, the health parameter value must indicate that the BlackBerry Enterprise Server service or component is healthy on the standby BlackBerry Enterprise Server before the automatic failover process can occur, even if you configure the health parameter to be below the promotion threshold line.

You must configure the health parameters that you choose for the primary BlackBerry Enterprise Server so that they are above the failover threshold. You must configure the health parameters that you choose for the standby BlackBerry Enterprise Server so that they are above the promotion threshold. The BlackBerry Enterprise Server ignores the health parameters that you configure to be below the thresholds.

The BlackBerry Enterprise Server updates the values of the health parameters periodically so that the BlackBerry Enterprise Server can determine automatically when a failover process should occur.

Defining when failover occurs

How you configure the failover threshold and promotion threshold impacts when failover occurs. You can configure the thresholds in any of the following ways:

- For failover to occur when the standby BlackBerry Enterprise Server is in an acceptable state, you can move the promotion threshold so that it is higher than the failover threshold. An acceptable state provides only the BlackBerry services that your organization considers essential.

- For failover to occur only when the standby BlackBerry Enterprise Server is in a healthier state than the primary BlackBerry Enterprise Server, you can move the promotion threshold so that it is lower than the failover threshold.
- For failover to occur when the standby BlackBerry Enterprise Server can provide the same services that the primary BlackBerry Enterprise Server can provide when it is healthy, you can move the promotion threshold so that it is equal to the failover threshold.

Configuring failover to occur when the standby BlackBerry Enterprise Server is in an acceptable state

By default, the thresholds are configured so that if the primary BlackBerry Enterprise Server loses its SRP connection or its messaging server connection, or the primary BlackBerry Enterprise Server cannot browse the Internet, the primary BlackBerry Enterprise Server must fail over. The standby BlackBerry Enterprise Server can promote itself if it can connect to the BlackBerry Infrastructure and messaging server. This default configuration is designed to make sure that the BlackBerry Enterprise Server remains in an acceptable state.

To maintain the BlackBerry Enterprise Server in an acceptable state, you configure the standby BlackBerry Enterprise Server to promote itself when it is sufficiently healthy to provide the BlackBerry services that your organization considers essential. The primary BlackBerry Enterprise Server cannot demote itself as long as it provides the BlackBerry services that your organization uses but does not consider essential.

For example, when the BlackBerry Enterprise Server pair uses the default configuration, if the primary BlackBerry Enterprise Server cannot connect to the messaging server, and the standby BlackBerry Enterprise Server cannot browse the Internet, the primary BlackBerry Enterprise Server must demote itself because one of its health parameters indicates that it is not sufficiently healthy. The standby BlackBerry Enterprise Server, even though it is experiencing an issue, can promote itself to become the primary BlackBerry Enterprise Server because all of the required health parameters indicate that it is healthy enough to become the primary instance.

Configuring failover to occur when the standby BlackBerry Enterprise Server can provide the same services that the primary BlackBerry Enterprise Server can provide

If you move the failover threshold and promotion threshold so that the identical health parameters are above both thresholds, the primary and standby BlackBerry Enterprise Server instances must meet the same requirements to be considered sufficiently healthy to run. You can move the promotion threshold to be the same as the failover thresholds if your organization requires that the failover process can promote a healthy standby BlackBerry Enterprise Server only.

In this scenario, you configure the standby BlackBerry Enterprise Server to promote itself when it can provide most of the BlackBerry services that your organization requires. The primary BlackBerry Enterprise Server demotes itself when it cannot provide most of the BlackBerry services that your organization considers essential.

For example, you can configure the failover threshold and the promotion threshold so that the primary and standby BlackBerry Enterprise Server instances must be able to connect to the BlackBerry Infrastructure and messaging server and browse the Internet. If the primary BlackBerry Enterprise Server cannot connect to the messaging server and the standby BlackBerry Enterprise Server cannot browse the Internet, the standby BlackBerry Enterprise Server cannot promote itself because it is not sufficiently healthy.

Configuring failover to occur when the standby BlackBerry Enterprise Server is in a healther state than the active BlackBerry Enterprise Server

If you move the failover threshold and promotion threshold so that the promotion threshold is lower than the failover threshold, failover occurs only if the standby BlackBerry Enterprise Server is healthier than the primary BlackBerry Enterprise Server that is sufficiently healthy to run. You can move the promotion threshold so that it is lower than the failover threshold if your organization wants to limit failover occurrences and requires that failover occurs only if the standby BlackBerry Enterprise Server meets all of your organization's requirements.

In this scenario, you configure the standby BlackBerry Enterprise Server to promote itself when it can provide most or all of the BlackBerry services that your organization requires. The primary BlackBerry Enterprise Server does not demote itself as long as it can provide at least the BlackBerry services that your organization considers essential.

For example, you configure the failover threshold so that the primary BlackBerry Enterprise Server must be able to connect to the BlackBerry Infrastructure and messaging server and browse the Internet. You configure the promotion threshold so that the standby BlackBerry Enterprise Server must be able to connect to the BlackBerry Infrastructure and messaging server, browse the Internet, and process attachments. If the primary BlackBerry Enterprise Server cannot connect to the messaging server and the standby BlackBerry Enterprise Server cannot process attachments, the standby BlackBerry Enterprise Server cannot promote itself because it does not meet all of its requirements.

Changing the promotion threshold and failover threshold

Each primary and standby BlackBerry Enterprise Server instance has a failover threshold and a promotion threshold. The BlackBerry Enterprise Server uses the failover threshold when it is an primary instance to determine when it needs to demote itself, and it uses the promotion threshold when it is a standby instance to determine whether it can promote itself to become the primary instance.

You can configure the thresholds for each BlackBerry Enterprise Server pair.

Change the promotion threshold and failover threshold and the order of the health parameters

You can change the promotion threshold and failover threshold and the order of the health parameters to meet the requirements of your organization.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **High availability** > **Highly available BlackBerry Enterprise Servers**.

2. Click the name of the BlackBerry Enterprise Server pair that you want to change the health parameters and thresholds for.
3. Click **Edit Automatic Failover settings**.
4. To change the order of the health parameters and thresholds, click the **Up** and **Down** icons.
5. Click **Save**.

Health parameters for the failover threshold and promotion threshold

Health parameter	Description
Wireless network access	This health parameter indicates whether the BlackBerry Router can access the wireless network. You cannot configure the failover threshold or promotion threshold so that they are above this health parameter.
BlackBerry Dispatcher	This health parameter indicates whether the BlackBerry Dispatcher can compress and encrypt all of the data that BlackBerry devices send and receive. You cannot configure the failover threshold or promotion threshold so that they are above this health parameter.
BlackBerry Messaging Agent	This health parameter indicates whether the BlackBerry Messaging Agent is available and connected to the BlackBerry Dispatcher.
User accounts	This health parameter indicates whether a preconfigured percentage of user accounts are started in the BlackBerry Messaging Agent.
Connection to the messaging server(s)	This health parameter indicates whether the BlackBerry Messaging Agent can connect to the messaging server. If your organization's environment includes multiple messaging servers and the BlackBerry Messaging Agent instances cannot connect to a preconfigured percentage of the messaging servers, the status of this health parameter changes to "Configured percentage not connected".
At least one user account	This health parameter indicates whether at least one user account is started in the BlackBerry Messaging Agent.
Access to web content and application content	This health parameter indicates whether the BlackBerry MDS Connection Service can provide users with access to content from BlackBerry Java Applications and content that is located on your organization's intranet or the Internet.
Address lookup	This health parameter indicates whether the BlackBerry Messaging Agent can look up addresses in the address book.
Calendar synchronization	This health parameter indicates whether the BlackBerry Messaging Agent can synchronize the calendar.

Health parameter	Description
Attachment viewing	This health parameter indicates whether the BlackBerry Messaging Agent can provide services for attachment viewing.
Connection to the BlackBerry Configuration Database	This health parameter indicates whether BlackBerry Enterprise Server components can connect to the BlackBerry Configuration Database.
Push application access	This health parameter indicates whether the BlackBerry MDS Connection Service can push application data to BlackBerry devices.
BlackBerry Collaboration Service	This health parameter indicates whether the BlackBerry Collaboration Service can provide services for the collaboration client on BlackBerry devices.
BlackBerry Policy Service	This health parameter indicates whether the BlackBerry Policy Service is available. You cannot set the failover threshold or promotion threshold below this health parameter.
BlackBerry Synchronization Service	This health parameter indicates whether the BlackBerry Synchronization Service is available. You cannot configure the failover threshold or promotion threshold so that they are below this health parameter.
Organizer data synchronization	This health parameter indicates whether the BlackBerry Synchronization Service can synchronize organizer data between BlackBerry devices and the messaging server over the wireless network. You cannot configure the failover threshold or promotion threshold so that they are below this health parameter.

Changing when automatic failover occurs by customizing the health parameters for user accounts and messaging servers

By default, the health parameters for user accounts and messaging servers use percentages to determine when a BlackBerry Enterprise Server instance is unhealthy. The User accounts health parameter indicates a BlackBerry Enterprise Server instance is unhealthy if less than 75% of the user accounts are started. The Connection to the messaging server(s) health parameter indicates that a BlackBerry Enterprise Server instance is unhealthy if the BlackBerry Enterprise Server instance cannot connect to at least 75% of the messaging servers in your organization.

If either of these health parameters indicate that the primary BlackBerry Enterprise Server is unhealthy and you turn on automatic failover, the BlackBerry Enterprise Server starts the failover process. You can change the percentages of these health parameters to customize when you want automatic failover to occur in your organization's environment.

For example, if your organization requires that all users can access email messages from BlackBerry devices at all times and that the BlackBerry Enterprise Server is connected to all of the messaging servers at all times, you can change the value of the Connection to the messaging server(s) health parameter to 100%.

If your organization's environment includes multiple BlackBerry Enterprise Server pairs, you can change the percentages of the health parameters for all of the BlackBerry Enterprise Server instances at the BlackBerry Domain level, or for each BlackBerry Enterprise Server pair. If you change the percentages of the health parameters at a BlackBerry Domain level and for a BlackBerry Enterprise Server pair, the percentage of the health parameters for the BlackBerry Enterprise Server pair overrides the percentage of the health parameters at the BlackBerry Domain level.

Change when automatic failover occurs by customizing the health parameters for user accounts and messaging servers

1. Copy the BlackBerry Enterprise Server installation media to the computer that hosts the primary BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to <*extracted_folder*>\tools .
4. To change the percentage of the User accounts health parameter, perform one of the following actions:
   - To change the percentage of the User accounts health parameter for all BlackBerry Enterprise Server instances, type **traittool.exe -global -trait UserHealthPercentage -set** ***<value>*** , where <*value*> is the percentage that you want to change the health parameter to.
   - To change the percentage of the User accounts health parameter for a BlackBerry Enterprise Server pair, type **traittool.exe -host** ***<instance_name>*** **-trait UserHealthPercentage -set** ***<value>*** , where <*instance_name*> is the name of the primary BlackBerry Enterprise Server instance and <*value*> is the percentage that you want to change the health parameter to.
5. To change the percentage of the health parameter for messaging servers, perform one of the following actions:
   - To change the percentage of the health parameter for messaging servers for all BlackBerry Enterprise Server instances, type **traittool.exe -global -trait ServerHealthPercentage -set** ***<value>*** , where <*value*> is the percentage that you want to change the health parameter to.
   - To change the percentage of the health parameter for messaging servers for a BlackBerry Enterprise Server pair, type **traittool.exe -host** ***<instance_name>*** **-trait ServerHealthPercentage -set <value>**, where <*instance_name*> is the name of the primary BlackBerry Enterprise Server instance and <*value*> is the percentage that you want to change the health parameter to.

Example: Changing the percentage of the User accounts health parameter

If you want to change the percentage of the User accounts health parameter to 80% for a BlackBerry Enterprise Server pair and the primary BlackBerry Enterprise Server instance is named server03, you can type **traittool.exe -host server03 -trait UserHealthPercentage -set 80**.

Example: Changing the percentage for Connection to the messaging server(s) health parameter

If you want to change the percentage of the Connection to the messaging server(s) health parameter to 60% for all BlackBerry Enterprise Server instances, you can type **traittool.exe -global -trait ServerHealthPercentage -set 60**.

Prerequisites: Configuring the BlackBerry Enterprise Server pair to fail over automatically

- Install a primary BlackBerry Enterprise Server.
- Install a standby BlackBerry Enterprise Server. For more information about installing a standby BlackBerry Enterprise Server, see the *BlackBerry Enterprise Server Installation and Configuration Guide*.
- Configure the health parameters to meet your organization's requirements.
- Specify the same proxy mappings for the BlackBerry MDS Connection Service instances on the primary and standby BlackBerry Enterprise Server instances.

Configure the BlackBerry Enterprise Server to fail over automatically

When you configure the BlackBerry Enterprise Server to fail over automatically, the BlackBerry Enterprise Server can start the failover process automatically depending on the health of the primary BlackBerry Enterprise Server and the standby BlackBerry Enterprise Server. The health parameters must be greater than the failover threshold and indicate that the primary BlackBerry Enterprise Server is unhealthy. The health parameters must also be greater than the promotion threshold and indicate that the standby BlackBerry Enterprise Server is healthy. After the failover process occurs, the BlackBerry Enterprise Server turns off automatic failover.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **High availability** > **Highly available BlackBerry Enterprise Servers**.
2. Click the name of the BlackBerry Enterprise Server pair that you want to turn on automatic failover for.
3. Click **Turn on automatic BlackBerry Enterprise Server failover**.

In the System status section, the value for the Automatic BlackBerry Enterprise Server failover mode field changes to True.

After you finish: To turn off automatic failover, click **Turn off automatic BlackBerry Enterprise Server failover**.

Monitoring the BlackBerry Enterprise Server for an automatic failover event

You can use the BlackBerry Monitoring Service, BlackBerry Enterprise Server Alert Tool, or another SNMP monitoring tool to monitor the BlackBerry Enterprise Server for an automatic failover event and notify you when an automatic failover event occurs.

When an automatic failover event occurs, the primary BlackBerry Enterprise Server and standby BlackBerry Enterprise Server write the time and reason at logging level 5 (Verbose) in the log files for the BlackBerry Dispatcher, BlackBerry Controller, and BlackBerry Messaging Agent. The BlackBerry Controller and BlackBerry Dispatcher instances for the primary BlackBerry Enterprise Server and standby BlackBerry Enterprise Server create SNMP alerts using the BlackBerry Enterprise Server Alert Tool. You can configure the SNMP tool that your organization uses to send automatic notifications when an automatic failover event occurs.

The BlackBerry Administration Service displays the time and reason for the last failover event that occurred.

Use the BlackBerry Administration Service to find the time and reason for the last automatic failover event

1. In the BlackBerry Administration Service, expand **High availability** > **Highly available BlackBerry Enterprise Servers**.
2. Click a BlackBerry Enterprise Server pair name.
3. If an automatic failover event occurred, in the **System status** section, the **Failover time** and **Failover reason** fields appear.

Fail over the BlackBerry Enterprise Server manually using the BlackBerry Administration Service

You can use the BlackBerry Administration Service to force a primary BlackBerry Enterprise Server to perform a failover process if it is not running as expected or if it requires maintenance.

Before you begin: Verify that the standby BlackBerry Enterprise Server is running.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **High availability** > **Highly available BlackBerry Enterprise Servers**.
2. Click the name of the BlackBerry Enterprise Server pair.
3. Click **Manual Failover**.
4. In the list, choose the standby BlackBerry Enterprise Server instance.
5. Click **Yes - Failover to standby instance**.
6. Verify that the failover event occured.

Fail over the BlackBerry Enterprise Server manually using the BlackBerry Configuration Panel

You can use the BlackBerry Configuration Panel to force the primary BlackBerry Enterprise Server to perform a failover process if it is not running as expected or if it requires maintenance.

Before you begin: Verify that the standby BlackBerry Enterprise Server is running.

1. In the BlackBerry Configuration Panel for the standby BlackBerry Enterprise Server, on the **BlackBerry Server** tab, click **Make Primary**.
2. Click **OK**.
3. Verify that the failover event occured.

Configuring high availability for BlackBerry Enterprise Server components

10

Creating a BlackBerry MDS Connection Service pool for high availability

To configure BlackBerry MDS Connection Service high availablity, you can create a BlackBerry MDS Connection Service pool for each BlackBerry Enterprise Server by associating multiple BlackBerry MDS Connection Service instances with each BlackBerry Enterprise Server. If the BlackBerry MDS Connection Service instance with the active connection stops responding, the BlackBerry Enterprise Server promotes the connection to the next instance in the pool list to an active connection.

If you configured central push servers, the BlackBerry MDS Connection Service pool should include at least two BlackBerry MDS Connection Service instances that you also configure as central push servers.

For more information, see the *BlackBerry Enterprise Server Planning Guide*.

Create a BlackBerry MDS Connection Service pool for high availability

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **BlackBerry Enterprise Server**.
2. If you configured BlackBerry Enterprise Server pairs, expand the pair name.
3. Click the name of the BlackBerry Enterprise Server instance that you want to assign the BlackBerry MDS Connection Service pool to.
4. Click **Edit instance**.
5. On the **Supported MDS Connection Service instances** tab, in the **Current MDS Connection Service instances** list, add the BlackBerry MDS Connection Service instances to the pool.

6. Click **Save all**.
7. Repeat steps 3 to 6 for each BlackBerry Enterprise Server instance in your organization's environment that you want to configure to use a BlackBerry MDS Connection Service pool.

Related information

Remove a BlackBerry MDS Connection Service instance from a pool, 122

Configure the BlackBerry MDS Connection Service and BlackBerry Collaboration Service to fail over automatically

You can configure the BlackBerry Enterprise Server to promote a standby connection to a BlackBerry MDS Connection Service or BlackBerry Collaboration Service automatically if the BlackBerry MDS Connection Service instance or BlackBerry Collaboration Service instance with the active connection stops responding. Configure the BlackBerry MDS Connection Service or BlackBerry Collaboration Service to fail over automatically to minimize interruptions to services for users.

Before you begin: Create the BlackBerry MDS Connection Service pool or BlackBerry Collaboration Service pool.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **High availability** > **Highly available BlackBerry Enterprise Servers**.
2. Click the name of the BlackBerry Enterprise Server pair that you created the BlackBerry MDS Connection Service or BlackBerry Collaboration Service pools for.
3. Click **Turn on automatic connections failover**.

In the System status section, the value of the BlackBerry Enterprise Server connection failover mode field changes to True.

After you finish: To turn off automatic failover, click **Turn off automatic connections failover**.

Related information

Fail over the BlackBerry MDS Connection Service or BlackBerry Collaboration Service manually, 120

Create a BlackBerry Collaboration Service pool for high availability

To configure BlackBerry Collaboration Service high availability, you can create a BlackBerry Collaboration Service pool for each BlackBerry Enterprise Server by associating multiple BlackBerry Collaboration Service instances with the BlackBerry Enterprise Server. By default, the BlackBerry Collaboration Service instance at the top of the pool list is the instance that the BlackBerry Enterprise Server assigns the active connection to. If the instance with the active connection stops responding, the BlackBerry Collaboration Service tries to connect to the next instance in the pool list.

For more information, see the *BlackBerry Enterprise Server Planning Guide*.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **BlackBerry Enterprise Server**.
2. If you configured BlackBerry Enterprise Server pairs, expand the appropriate pair name.
3. Click the name of the BlackBerry Enterprise Server instance that you want to assign the BlackBerry Collaboration Service pool to.
4. Click **Edit instance**.
5. Click one of the following tabs, depending on which instant messaging server that you installed in your organization's environment:
   - **Supported IBM Lotus Domino instances**
   - **Supported Novell GroupWise Messenger instances**
   - **Supported Microsoft Office Live Communications Server 2005 instances**
   - **Supported Microsoft Office Communications Server 2007 instances**
   - **Supported Microsoft Office Communications Server 2007 R2 instances**
   - **Supported Microsoft Lync Server 2010 instances**
6. In the list of current instances, add the BlackBerry Collaboration Service instances to the pool.
7. Click **Save all**.
8. Repeat steps 3 to 7 for each BlackBerry Enterprise Server instance in your organization's environment that you want to configure to use a BlackBerry Collaboration Service pool.

Related information

Remove a BlackBerry Collaboration Service instance from a pool, 123

Create a BlackBerry Attachment Service pool for high availability

During the BlackBerry Attachment Service installation process, the setup application writes data about the BlackBerry Attachment Service instance to the BlackBerry Configuration Database. You can create a BlackBerry Attachment Service pool for each BlackBerry Enterprise Server by associating multiple BlackBerry Attachment Service instances with each BlackBerry Enterprise Server. Within each pool, you can create primary and secondary groups.

For more information, see the *BlackBerry Enterprise Server Planning Guide*.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Attachment** > **Connector**.
2. Click the BlackBerry Attachment Connector that you installed with the BlackBerry Enterprise Server that you want to create the BlackBerry Attachment Service pool for. By default, the name of the BlackBerry Attachment Connector is <*computername*>_EMAIL_AC_13.
3. Click **Edit instance**.
4. On the **Supported Attachment Server Instances** tab, in the **Name** drop-down list, click the instance that you want to add.
5. In the **Results Query Period(s)** field, type the number of seconds that you want the BlackBerry Enterprise Server to wait for a response before it sends the request to another BlackBerry Attachment Service instance.
6. In the **Dedicated Server** drop-down list, click **yes** if you want the BlackBerry Attachment Service instance to process only specific content types for the BlackBerry Enterprise Server.
7. In the **Pool** drop-down list, complete one of the following actions:
   - To include the BlackBerry Attachment Service instance in the primary group of instances within a pool, click **Primary**.
   - To include the BlackBerry Attachment Service instance in the secondary group, click **Secondary**.
8. Complete the following actions:
   - To turn on support for an attachment file format, in the **Extensions** section, type the file extension of the format. Click the **Add** icon that is located beside the extension that you typed.
   - To turn off support for an attachment file format, in the **Extensions** section, click the **Delete** icon that is located beside the file extension.
9. Click the **Add** icon.
10. Repeat steps 5 to 9 for each BlackBerry Attachment Service instance that you want to add to the pool.

11. Click **Save all**.
12. Repeat steps 2 to 11 for each BlackBerry Enterprise Server instance that you want to use a BlackBerry Attachment Service pool.

The BlackBerry Administration Service writes the data about the BlackBerry Attachment Service pool to the BlackBerry Configuration Database. The BlackBerry Messaging Agent caches the pool data and uses the data to determine which BlackBerry Attachment Service instance can process a request.

You cannot determine the BlackBerry Attachment Connector that the BlackBerry Enterprise Server or the BlackBerry MDS Connection Service uses

If you install a BlackBerry Enterprise Server, the setup application also installs two BlackBerry Attachment Connector instances automatically. One of the BlackBerry Attachment Connector instances connects the BlackBerry Enterprise Server to the BlackBerry Attachment Service. The other instance connects the BlackBerry MDS Connection Service to the BlackBerry Attachment Service. During the installation process, the setup application gives both BlackBerry Attachment Connector instances a name that includes the computer name (for example, <*computer_name*>_AC).

The BlackBerry Administration Service displays the names of both the BlackBerry Attachment Connector instances. By default, you cannot determine easily which instance connects to the BlackBerry Enterprise Server or the BlackBerry MDS Connection Service, so you can change the display names of both the BlackBerry Attachment Connector instances to make them easier to identify.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Attachment** > **Connector**.
2. Click one of the BlackBerry Attachment Connector instances.
3. On the **Instance information** tab, locate either the **MDS Connection Service Instance name** section or the **Email (Exchange) Instance name** section. Consider the following naming conventions:
   - If you locate the section that is named **MDS Connection Service Instance name**, the BlackBerry MDS Connection Service connects to this BlackBerry Attachment Connector instance.
   - If you locate the section that is named **Email (Exchange) Instance name**, the BlackBerry Enterprise Server connects to this BlackBerry Attachment Connector instance.
4. Click **Edit instance**.
5. Perform one of the following actions:
   - If the BlackBerry MDS Connection Service connects to the BlackBerry Attachment Connector instance, in the **Instance information** section, in the **Friendly description** field, type a unique name (for example, <*server_name*>_AC_MDSCS).

- If the BlackBerry Enterprise Server uses the BlackBerry Attachment Connector instance, in the **Instance information** section, in the **Friendly description** field, type a unique name.

6. Click **Save all**.

The BlackBerry Administration Service updates the list of BlackBerry Attachment Connector instances automatically to use the names that you typed.

Create a BlackBerry Router pool for high availability

To configure BlackBerry Router high availability, you can create a BlackBerry Router pool for each BlackBerry Enterprise Server by assigning multiple BlackBerry Router instances to the BlackBerry Enterprise Server. The BlackBerry Enterprise Server determines which BlackBerry Router instance to connect to by trying to connect to the first BlackBerry Router instance in the pool list. If the BlackBerry Enterprise Server cannot connect to the first BlackBerry Router instance in the list, it tries to connect to each BlackBerry Router in sequence until a connection succeeds.

For more information, see the *BlackBerry Enterprise Server Planning Guide*.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, click **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **BlackBerry Enterprise Server**.
2. Click the name of the BlackBerry Enterprise Server or the name of the BlackBerry Enterprise Server pair that you want to assign the BlackBerry Router pool to.
3. Click **Edit instance**.
4. In the **SRP Address** section, type the FQDN of the computer that hosts the BlackBerry Router instance.
5. If the BlackBerry Router instance uses a port number other than port number 3101, in the **Port override** field, type the port number.
6. Click the **Add** icon.
7. Repeat steps 4 to 6 for each instance that you want to add to the pool.
8. Click **Save all**.
9. Restart the BlackBerry Enterprise Server using one of the following methods:
   - If you are changing a BlackBerry Enterprise Server instance, on the **Instance** tab, click **Restart instance**.
   - If you are changing a BlackBerry Enterprise Server pair, click on one of the instances. On the **Instance** tab, click **Restart instance**. Repeat this step for the other instance.
   - In the Windows Services, restart the BlackBerry Dispatcher.

10. Repeat steps 2 to 9 for each BlackBerry Enterprise Server instance in your organization's environment that you want to have use a BlackBerry Router pool.

Related information

Remove a BlackBerry Router instance from a pool, 124

Restarting BlackBerry Enterprise Server components, 392

Permit a BlackBerry Enterprise Server to connect to a remote BlackBerry Router

If you installed a BlackBerry Router on a computer that is separate from the computer that hosts a BlackBerry Enterprise Server, you must permit the BlackBerry Dispatcher that you installed with the BlackBerry Enterprise Server to connect to the BlackBerry Router. The BlackBerry Router that you installed on a separate computer can send data packets from the BlackBerry Enterprise Server to BlackBerry devices.

1. On the computer that hosts the BlackBerry Router, click **Start** > **Run**.
2. Type **regedit**.
3. Click **OK**.
4. Perform one of the following actions:
   - If you are running a 32-bit version of Windows, navigate to \\HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerryRouter.
   - If you are running a 64-bit version of Windows, navigate to \\HKEY_LOCAL_MACHINE\SOFTWARE \WOW6432Node \Research In Motion\BlackBerryRouter.
5. Verify the value of **AllowRemoteServices** is **1**.
6. If you want to change the port number that the BlackBerry Router uses to open connections to the BlackBerry Dispatcher, change the value of **ServicePort** to the port number that the BlackBerry Router should use, for example, port number 80. By default, the port number is 3101.
7. In the Windows Services, restart the BlackBerry Router service.

Creating a BlackBerry Administration Service pool that includes the BlackBerry Web Desktop Manager using DNS round robin

When you install the BlackBerry Administration Service, BlackBerry Web Desktop Manager, or both, the setup application installs the BlackBerry Administration Service services automatically. The BlackBerry Administration Service and BlackBerry Web Desktop Manager require the BlackBerry Administration Service services to run.

If you create a BlackBerry Administration Service pool using DNS round robin, you can install the BlackBerry Administration Service and BlackBerry Web Desktop Manager on each computer in the pool or you can install the BlackBerry Administration Service or BlackBerry Web Desktop Manager on some of the computers in the pool. If you install the BlackBerry Administration Service and BlackBerry Web Desktop Manager on each computer in the pool, you can use the pool name that you specified during the installation process in the URLs for the BlackBerry Administration Service and BlackBerry Web Desktop Manager (for example, https://<*pool_name*>/webconsole/login or https://<*pool_name*>/webdesktop/login).

If you do not install both components on each computer in the pool and you try to access one of the URLs using the pool name, the web browser might display an HTTP 404 error message. The HTTP 404 error message occurs when the web browser tries to connect to a computer in the pool that you did not install the component on that you are trying to access. For example, you can install the BlackBerry Administration Service on two of the computers in the pool and the BlackBerry Web Desktop Manager on two other computers in the pool.

To make sure that the web browser does not display HTTP 404 error messages, you can choose one of the following options:

- You can create separate pools within the BlackBerry Administration Service pool for the BlackBerry Administration Service and the BlackBerry Web Desktop Manager. You can provide your organization's administrators and BlackBerry device users with URLs that include the specific pool names.
- You can provide administrators and users in your organization's environment with URLs that include the FQDNs of the computers that you installed the BlackBerry Administration Service or BlackBerry Web Desktop Manager on (for example, https://<*FQDN_of_computer*>/webconsole/login or https://<*FQDN_of_computer*>/webdesktop/login).

Configure the BlackBerry Administration Service instances in a pool to communicate across network subnets

The instances in the BlackBerry Administration Service pool use multicast UDP to communicate with each other. If the BlackBerry Administration Service instances are located in different network subnets and your organization's network configuration does not permit multicast UDP across the network subnets, you must configure the BlackBerry Administration Service instances to use TCP to communicate with each other. For example, if your organization uses a UDP peer-to-peer firewall filter, you must configure the BlackBerry Administration Service instances to use TCP to communicate across the network subnets.

1. Make sure that no BlackBerry Administration Service instance is in the process of restarting.
2. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **BlackBerry Administration Service**.
3. Click **Edit component**.
4. In the **BlackBerry Administration Service pool** drop-down list, click **TCP with TCP PING**.
5. Click **Save all**.
6. Restart the BlackBerry Administration Service instances.

Related information

Restarting BlackBerry Enterprise Server components, 392

Changing the name of the BlackBerry Administration Service pool

When you install the first BlackBerry Administration Service instance in a BlackBerry Domain, the default name of the BlackBerry Administration Service pool is the FQDN of the computer that you perform the installation on. If you want to configure high availability using DNS round robin after the installation process completes, you must change the name of the BlackBerry Administration Service pool to the name of a record in the DNS server that represents the BlackBerry Administration Service instances in the pool. You must also change the name of the BlackBerry Administration Service pool if you have changed the name of the corresponding DNS record in the DNS server. You can only configure one BlackBerry Administration Service pool in a BlackBerry Domain.

When you change the name of the BlackBerry Administration Service pool, you must synchronize the BlackBerry Monitoring Service with the name of the BlackBerry Administration Service pool in the BlackBerry Configuration Database.

Change the name of the BlackBerry Administration Service pool

Before you begin: If you want to configure high availability for the BlackBerry Administration Service by creating a BlackBerry Administration Service pool using DNS round robin, create the DNS record that represents the BlackBerry Administration Service instances in the pool.

1. On a computer that hosts a BlackBerry Administration Service instance, in the BlackBerry Configuration Panel, on the **Administration Service - High Availability** tab, in the **Pool name** field, type a new name for the pool.
2. Click **OK**.
3. On the computer that hosts a BlackBerry Monitoring Service instance, in the BlackBerry Configuration Panel, on the **Administration Service - High Availability** tab, click the **Synchronize** button.
4. Click **OK**.
5. On the computer that hosts a BlackBerry Administration Service instance, in the Windows Services, restart the BlackBerry Administration Service services.
6. If the BlackBerry Administration Service instance uses a self-signed certificate, on the computers that host the other BlackBerry Administration Service instances, in the Windows Services, restart the BlackBerry Administration Service services.
7. On the computer that hosts a BlackBerry Monitoring Service instance, in the Windows Services, restart the BlackBerry Monitoring Service services.

Related information

Restarting BlackBerry Enterprise Server components, 392

Fail over the BlackBerry MDS Connection Service or BlackBerry Collaboration Service manually

You can fail over the BlackBerry MDS Connection Service or BlackBerry Collaboration Service when you want to perform maintenance on the instance with the active connection to the BlackBerry Enterprise Server or when a disaster recovery scenario occurs.

Before you begin: Verify that the standby BlackBerry MDS Connection Service or BlackBerry Collaboration Service is running.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **BlackBerry Enterprise Server**.
2. If you configured BlackBerry Enterprise Server pairs, expand the pair name.
3. Click the name of the BlackBerry Enterprise Server instance that you assigned the BlackBerry MDS Connection Service pool or BlackBerry Collaboration Service pool to.
4. Perform one of the following actions:
    - If you want to fail over the BlackBerry Collaboration Service and your organization's environment includes IBM Lotus Sametime, click the **Supported IBM Lotus Sametime instances** tab.
    - If you want to fail over the BlackBerry Collaboration Service and your organization's environment includes Novell GroupWise Messenger, click the **Supported Novell GroupWise Messenger instances** tab.
    - If you want to fail over the BlackBerry Collaboration Service and your organization's environment includes Microsoft Office Live Communications Server 2005, click the **Supported Microsoft Office Live Communications Server 2005 instances** tab.
    - If you want to fail over the BlackBerry Collaboration Service and your organization's environment includes Microsoft Office Communications Server 2007, click the **Supported Microsoft Office Communications Server 2007 instances** tab.
    - If you want to fail over the BlackBerry MDS Connection Service, click the **Supported MDS Connection Service instances** tab.
5. Click **Manual Failover**.
6. Click the instance that you want to assign the active connection to.
7. Click **Yes - Failover to standby instance**.

The Availability state for the instances changes automatically.

Monitoring the high availability status or job deployment status using the BlackBerry Administration Service

When you navigate to a BlackBerry Administration Service page that displays the high availability status or job deployment status, the BlackBerry Administration Service displays the high availability status of the BlackBerry Enterprise Server, BlackBerry Collaboration Service, or BlackBerry MDS Connection Service and the job deployment status that is stored in the BlackBerry Configuration Database. You can configure the BlackBerry Administration Service to refresh the high availability status or job deployment status every 30 seconds for the amount of time that you display the page in the web browser.

When you navigate to another page in the BlackBerry Administration Service, the BlackBerry Administration Service turns off the refresh option, and you must turn it on again manually when you return to the page that displays the status.

If more than one administrator logs in to the BlackBerry Administration Service, each administrator must turn on the refresh option manually so that the BlackBerry Administration Service refreshes the high availability status or job deployment status in the web browser for the administrator.

Monitor the high availability status or job deployment status using the BlackBerry Administration Service

1. In the BlackBerry Administration Service, navigate to one of the following locations:
   - To monitor the high availability status for a BlackBerry Enterprise Server pair, navigate to **Servers and components** > **High availability** > **Highly Available BlackBerry Enterprise Servers** > <***BES_pair***> .
   - To monitor the high availability status for all BlackBerry Enterprise Server pairs, navigate to **Servers and components** > **High availability** > **High availability summary**.
   - To monitor job deployment status, navigate to **Devices** > **Deployment jobs** > **View reconciliation event status**.
2. Click **Refresh page automatically**.

Remove a BlackBerry MDS Connection Service instance from a pool

You can remove a BlackBerry MDS Connection Service instance from a pool if your organization no longer requires it or to troubleshoot an issue.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **BlackBerry Enterprise Server**.
2. If you configured BlackBerry Enterprise Server pairs, expand the pair name.
3. Click the name of the BlackBerry Enterprise Server instance that uses the BlackBerry MDS Connection Service pool.
4. Click **Edit instance**.
5. On the **Supported MDS Connection Service instances** tab, remove the BlackBerry MDS Connection Service instance from the list of current instances.
6. Click **Save all**.

Remove a BlackBerry Collaboration Service instance from a pool

You can remove a BlackBerry Collaboration Service instance from a pool if your organization no longer requires it or to troubleshoot an issue.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **BlackBerry Enterprise Server**.
2. If you configured BlackBerry Enterprise Server pairs, expand the pair name.
3. Click the name of the BlackBerry Enterprise Server instance that uses the BlackBerry Collaboration Service pool.
4. Click **Edit instance**.
5. Click one of the following tabs, depending on the instant messaging server that you installed in your organization's environment:
   - **Supported IBM Lotus Sametime instances**
   - **Supported Novell GroupWise Messenger instances**
   - **Supported Microsoft Office Live Communications Server 2005 instances**
   - **Supported Microsoft Office Communications Server 2007 instances**
   - **Supported Microsoft Office Communications Server 2007 R2 instances**
   - **Supported Microsoft Lync Server 2010 instances**
6. Remove the BlackBerry Collaboration Service instance from the list of current instances.
7. Click **Save All**.

Remove a BlackBerry Attachment Service instance from a pool

You can remove a BlackBerry Attachment Service instance from a pool if your organization no longer requires it or to troubleshoot an issue.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Attachment** > **Connector**.
2. Click the BlackBerry Attachment Connector that is installed on the BlackBerry Enterprise Server that you want to remove the BlackBerry Attachment Service instance from. By default, the name of the BlackBerry Attachment Connector is <*computername*>_AC_EMAIL_13.
3. Click **Edit instance**.
4. Click the **Supported Attachment Server Instances** tab.
5. Click the **Delete** icon for the BlackBerry Attachment Service instance that you want to remove.
6. Click **Save all**.

Remove a BlackBerry Router instance from a pool

You can remove a BlackBerry Router instance from a pool if it is no longer required or to troubleshoot an issue.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **BlackBerry Enterprise Server**.
2. Click the name of the BlackBerry Enterprise Server instance or the name of the BlackBerry Enterprise Server pair that you want to remove the BlackBerry Router instance from.
3. Click **Edit instance** or **Edit host instance**.
4. In the **SRP Addresses** section, click the **Delete** icon for the BlackBerry Router instance that you want to remove.
5. Click **Save all**.

Configuring BlackBerry Configuration Database high availability

11

You can configure BlackBerry Configuration Database high availability by configuring database mirroring. Database mirroring requires that you configure a principal BlackBerry Configuration Database instance and a mirror BlackBerry Configuration Database. The BlackBerry Enterprise Server and BlackBerry Enterprise Server components can connect to the principal BlackBerry Configuration Database, and, if the principal BlackBerry Configuration Database stops responding, they can connect to a mirror BlackBerry Configuration Database automatically.

If your organization's environment does not support database mirroring, you can configure transactional replication. When you configure transactional replication and the BlackBerry Configuration Database stops responding, you must connect the BlackBerry Enterprise Server and BlackBerry Enterprise Server components to the replicated BlackBerry Configuration Database manually.

Prerequisites: Configuring database mirroring or database replication of the BlackBerry Configuration Database

- Install the same version and build of Microsoft SQL Server for the mirror or replicated database server that you installed for the principal database server.
- Configure the database servers to permit access from remote computers.
- Verify that the Microsoft SQL Server Agent uses a domain user account with the local administrative permissions set to the same permissions as the Windows account that runs the BlackBerry Enterprise Server services.
- Verify that the domain user account has permissons on both database servers so that each Microsoft SQL Server Agent can access the shared replication folder.
- Configure the database server that will host the mirror or replicated BlackBerry Configuration Database with the same permissions that you configured on the database server that hosts the prinicipal BlackBerry Configuration Database.
- Verify that the DNS server is running.

- If you turned on the automatic failover option for the BlackBerry Enterprise Server, use the BlackBerry Administration Service to change the failover type to Manual until you finish configuring database mirroring or database replication.
- If you are configuring database mirroring, configure the database servers as follows:
  - Only use static port number 1433.
  - Verify that the SQL Server Browser is running.
  - Do not use named instances.
- If you are configuring database mirroring, turn off the Named Pipes option in the Microsoft SQL Server Native Client on the computers that hosts the BlackBerry Enterprise Server instances.

Configuring database mirroring

You can use Microsoft SQL Server 2005 or 2008 database mirroring to configure the BlackBerry Configuration Database for high availability.

The BlackBerry Configuration Database only supports high safety with automatic failover (synchronous) operating mode for database mirroring.

For more information, visit http://msdn2.microsoft.com/en-us/library/ms175059(SQL.90).aspx.

Stop the BlackBerry Enterprise Server instances

To maintain database integrity, you must prevent all services that use the BlackBerry Configuration Database from connecting to the databases while you configure replication.

1. On the computers that host the BlackBerry Enterprise Server components, in the Windows Services, stop all of the BlackBerry Enterprise Server services in the following order:
   - BlackBerry Administration Service services
   - BlackBerry Mail Store Service
   - BlackBerry Instant Messaging Connector
   - BlackBerry MDS Connection Service
   - BlackBerry Dispatcher
   - BlackBerry Attachment Service
   - BlackBerry Controller
   - all of the remaining BlackBerry Enterprise Server services that connect to the BlackBerry Configuration Database

2. Repeat step 1 for each BlackBerry Enterprise Server component that connects to the BlackBerry Configuration Database.

Configure database mirroring for the BlackBerry Configuration Database

For more information about database mirroring, visit http://msdn2.microsoft.com/en-us/library/ms175059(SQL.90).aspx.

1. In the Microsoft SQL Server Management Studio, change the **Recovery Model** property for the principal database to **Full**.
2. Change the **Backup type** option to **Full** and back up the principal database.
3. Copy the backup files to the database server that you want to have host the mirror database.
4. On the database server that will host the mirror database, restore the database. If you did not perform a full backup, specify the **NO RECOVERY** option.
5. On the principal database, in the **Database Properties** window, on the **Mirroring** page, run the **Configure Security** wizard.
6. Start the mirroring process.
7. To verify that failover works correctly, fail over to the mirror database and back to the principal database manually.

After you finish: To permit the mirror BlackBerry Configuration Database to write BlackBerry Enterprise Server event messages, install the BlackBerry database notification system on the database server that hosts the mirror BlackBerry Configuration Database. For more information, see the *BlackBerry Enterprise Server Installation Guide*.

Start the BlackBerry Enterprise Server instances

After you configure the database, permit all BlackBerry Enterprise Server instances to connect to the principal BlackBerry Configuration Database.

1. On the computers that host the BlackBerry Enterprise Server components, in the Windows Services, start all of the BlackBerry Enterprise Server services in the following order:
   - BlackBerry Controller
   - BlackBerry Router
   - BlackBerry Attachment Service
   - BlackBerry Dispatcher
   - BlackBerry MDS Connection Service
   - BlackBerry Instant Messaging Connector

- BlackBerry Alert
- BlackBerry Mail Store Service
- BlackBerry User Administration Service
- all of the remaining BlackBerry Enterprise Server services

2. Repeat step 1 for each BlackBerry Enterprise Server component that connects to the BlackBerry Configuration Database.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configure the BlackBerry Enterprise Solution to support database mirroring

When you configure the BlackBerry Enterprise Solution to support database mirroring, the BlackBerry Administration Service adds a registry key to all of the computers that host BlackBerry Enterprise Server components in the BlackBerry Domain and the registry key includes the name of the Microsoft SQL Server that hosts the mirror database. The BlackBerry Administration Service also adds the name of the Microsoft SQL Server that hosts the mirror database to the BlackBerry Configuration Database.

CAUTION: If you click **Save all** more than once but you do not restart the BlackBerry Enterprise Server services or the computers that host the BlackBerry Enterprise Server components that the BlackBerry Administration Service specifies as **Updated**, you should restart the BlackBerry Enterprise Server services or restart the computers for all of the BlackBerry Enterprise Server components.

Before you begin: The database server that hosts the mirror database must be running.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, go to **BlackBerry Solution Topology** > **BlackBerry Domain**.
2. Click **Edit domain**.
3. In the **Database mirroring turned on** drop-down list, click **Yes**.
4. In the **Mirroring database host** field, type the name of the mirror database server.
5. Click **Save all**.
6. On the computers that host the BlackBerry Enterprise Server components that are specified as **Updated** in the **Server responses to mirroring data update** table, restart the BlackBerry Enterprise Server services or restart the computers that host the components.
7. On the computers that host the BlackBerry Enterprise Server components that are specified as **No response. Please save the data again to attempt to update this server**, verify that the computers are running and connected to the network and then resend the database mirroring parameters to the BlackBerry Enterprise Server components.

Related information

Resend the database mirroring parameters to BlackBerry Enterprise Server components, 129

Resend the database mirroring parameters to BlackBerry Enterprise Server components

If the computers that host BlackBerry Enterprise Server components were not running or connected to the network when you configured the BlackBerry Enterprise Solution to support database mirroring, or if you do not know if all of the components were configured to support database mirroring, you should resend the database mirroring parameters to the components. When you resend the database mirroring parameters, the BlackBerry Administration Service adds a registry key to the computers that host the components. The registry key includes the name of the Microsoft SQL Server that hosts the mirror database.

CAUTION: If you resend the database mirroring parameters more than once but you do not restart the BlackBerry Enterprise Server services or the computers that host the BlackBerry Enterprise Server components that the BlackBerry Administration Service specifies as **Updated**, you should restart the BlackBerry Enterprise Server services or restart the computers for all of the BlackBerry Enterprise Server components.

Before you begin: The database server that hosts the mirror database must be running.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, go to **BlackBerry Solution Topology** > **BlackBerry Domain**.
2. Click **Resend database mirroring parameters**.
3. On the computers that host the BlackBerry Enterprise Server components that are specified as **Updated** in the **Server responses to mirroring data update** table, restart the BlackBerry Enterprise Server services or restart the computers that host the components.
4. On the computers that host the BlackBerry Enterprise Server components that are specified as **No response. Please save the data again to attempt to update this server**, verify that the computers are running and connected to the network and then resend the database mirroring parameters to the BlackBerry Enterprise Server components.

Configuring the BlackBerry Configuration Database for one-way transactional replication in an environment that includes Microsoft SQL Server 2005 or 2008

Stop the BlackBerry Enterprise Server instances

To maintain database integrity, you must prevent all services that use the BlackBerry Configuration Database from connecting to the databases while you configure replication.

1. On the computers that host the BlackBerry Enterprise Server components, in the Windows Services, stop all of the BlackBerry Enterprise Server services in the following order:
   - BlackBerry Administration Service services
   - BlackBerry Mail Store Service
   - BlackBerry Instant Messaging Connector
   - BlackBerry MDS Connection Service
   - BlackBerry Dispatcher
   - BlackBerry Attachment Service
   - BlackBerry Controller
   - all of the remaining BlackBerry Enterprise Server services that connect to the BlackBerry Configuration Database
2. Repeat step 1 for each BlackBerry Enterprise Server component that connects to the BlackBerry Configuration Database.

Create the replicated BlackBerry Configuration Database from a backup

Before you begin: Back up the BlackBerry Configuration Database with the Backup type option set to Full.

1. Copy the backup file from the database server that hosts the BlackBerry Configuration Database to the database server that will host the replicated BlackBerry Configuration Database.
2. In the Microsoft SQL Server Management Studio, in the left pane, navigate to the database server that will host the replicated BlackBerry Configuration Database.
3. Right-click **Database**. Click **Restore Database**.
4. Select **From device**.
5. Navigate to the backup file that you copied from the database server that hosts the BlackBerry Configuration Database.
6. Click **OK**.
7. In the **To database** drop-down list, select the BlackBerry Configuration Database.
8. In the list of backup sets to restore, select the backup file.
9. Click **Options**.
10. Select **Overwrite the existing database**.
11. Click **OK**.

Permit access to the BlackBerry Configuration Database instances

1. In the Microsoft SQL Server Management Studio, connect to the database server that hosts the BlackBerry Configuration Database.
2. Right-click the BlackBerry Configuration Database. Click **Properties**.
3. Click **Options**.
4. In the **State** section, in the **Restrict Access** drop-down list, select **Multiple**.
5. Click **OK**.
6. Repeat steps 1 to 5 for the replicated BlackBerry Configuration Database.

Configure the publication for the BlackBerry Configuration Database

1. In the Microsoft SQL Server Management Studio, in the left pane, navigate to the database server that hosts the BlackBerry Configuration Database.
2. Click **Replication**.

3. Right-click **Local Publications**. Click **New Publication**.
4. If the **Welcome** dialog box appears, click **Next**.
5. If this is the first time that you are configuring a publication on the database server, perform the following actions:
   - Select *<database_server>* **will act as its own Distributor**. Click **Next**.
   - In the **Snapshot folder** field, type the network location of the snapshot folder. Click **Next**.
6. In the list of databases, select the BlackBerry Configuration Database name. Click **Next**.
7. Click **Transactional publication**. Click **Next**.
8. In the **Objects to publish** list, select **Tables, Stored Procedures, Views, and User Defined Functions**.
9. If you installed the BlackBerry database notification system on the computer, expand **Tables** and clear the **ServiceConfig** table and the **ServiceTable** table. Click **Next**.
10. If the **Article Issues** dialog box appears, click **Next**.
11. If the **Filter Table Rows** dialog box appears, click **Next**.
12. Select **Schedule the Snapshot Agent to run at the following times**.
13. Accept or change the default schedule. Click **Next**.
14. On the **Snapshot Agent Security** page, click **Security Settings**.
15. Select **Run under the following Windows account**.
16. Type the user name and password of a domain account that has local administrative permissions.
17. Select **By impersonating the process account**.
18. Click **OK**. Click **Next**.
19. Select **Create the publication**. Click **Next**.
20. In the **Publication name** field, type a name for the publication.
21. Click **Finish**.

After you finish: Verify that you can access the shared snapshot folder from both database servers.

Increase the maximum data size for transactional replication

When you set up transactional replication, you must increase the default value for the maximum number of bytes of data that the BlackBerry Enterprise Servercan write to a replicated database column in one transaction.

1. In the Microsoft SQL Server Management Studio, connect to the database server that hosts the BlackBerry Configuration Database.

2. Right-click the server. Click **Properties**.
3. Click **Advanced**.
4. In the **Miscellaneous** section, set the **Max Text Replication Size** to the maximum, **2147483647**.
5. Click **OK**.

Prepare the database server that hosts the replicated BlackBerry Configuration Database and configure the subscription

1. In the Microsoft SQL Server Management Studio, in the left pane, connect to the database server that hosts the replicated BlackBerry Configuration Database.
2. Navigate to the database server that hosts the replicated BlackBerry Configuration Database.
3. Click **Replication**.
4. Right-click **Local Subscriptions**. Click **New Subscription**.
5. In the list of publishers, select the name of the database server that hosts the BlackBerry Configuration Database.
6. In the list of databases and publications, select the publication for the BlackBerry Configuration Database. Click **Next**.
7. Select **Run each agent at its Subscriber (pull subscriptions)**. Click **Next**.
8. In the **Subscriber** column, select the database server that hosts the replicated BlackBerry Configuration Database.
9. In the **Subscription Database** drop-down list, select the replicated BlackBerry Configuration Database. Click **Next**.
10. Change the distribution agent security so that you can access the Snapshot Agent using a Windows account with administrative permissions on the domain.
11. Select **By impersonating the process account**.
12. Click **OK**. Click **Next**.
13. In the **Agent Schedule** drop-down list, select **Run continuously**. Click **Next**.
14. In the **Subscription properties**, clear **Initialize**. Click **Next**.
15. Select **Create the Subscriptions**. Click **Next**.
16. Click **Finish**.

Start the BlackBerry Enterprise Server instances

After you configure the database, permit all BlackBerry Enterprise Server instances to connect to the principal BlackBerry Configuration Database.

1. On the computers that host the BlackBerry Enterprise Server components, in the Windows Services, start all of the BlackBerry Enterprise Server services in the following order:
    - BlackBerry Controller
    - BlackBerry Router
    - BlackBerry Attachment Service
    - BlackBerry Dispatcher
    - BlackBerry MDS Connection Service
    - BlackBerry Instant Messaging Connector
    - BlackBerry Alert
    - BlackBerry Mail Store Service
    - BlackBerry User Administration Service
    - all of the remaining BlackBerry Enterprise Server services
2. Repeat step 1 for each BlackBerry Enterprise Server component that connects to the BlackBerry Configuration Database.

Related information

Restarting BlackBerry Enterprise Server components, 392

Reacting if the BlackBerry Configuration Database that you configured for transactional replication stops responding

If a BlackBerry Configuration Database that you configured for one-way transactional replication stops responding, you must configure all BlackBerry Enterprise Server instances and BlackBerry Enterprise Server components that connect to the BlackBerry Configuration Database to connect to a replicated BlackBerry Configuration Database on another database server.

To configure the BlackBerry Enterprise Server instances and components, you delete the pull subscription from the replicated database server, run a SQL query to update the numbering of the identity values in the replicated BlackBerry Configuration Database, and run the BlackBerry Enterprise Server setup application to permit each BlackBerry Enterprise Server instance and component to connect to the replicated BlackBerry Configuration Database.

Return to the BlackBerry Configuration Database when you configured transactional replication

When the BlackBerry Configuration Database becomes available again after it has stopped responding, you can update the BlackBerry Enterprise Server and BlackBerry Enterprise Server components so that they use the BlackBerry Configuration Database instead of the replicated BlackBerry Configuration Database.

1. Back up the replicated BlackBerry Configuration Database.
2. To avoid data corruption, prevent each BlackBerry Enterprise Server instance from connecting to the replicated BlackBerry Configuration Database.
3. On the database server that hosts the BlackBerry Configuration Database, replace the BlackBerry Configuration Database with a restored version of the replicated BlackBerry Configuration Database.
4. Run the setup application to permit each BlackBerry Enterprise Server instance and BlackBerry Enterprise Server component to connect to the BlackBerry Configuration Database.

Configuring a new mirror BlackBerry Configuration Database

If the principal BlackBerry Configuration Database stops responding and the BlackBerry Enterprise Server fails over automatically to the mirror BlackBerry Configuration Database, the mirror BlackBerry Configuration Database becomes the new principal BlackBerry Configuration Database.

If you configure a new mirror BlackBerry Configuration Database, you must resend the database mirroring parameters to the BlackBerry Enterprise Server components so that they can use the new mirror BlackBerry Configuration Database.

Related information

Resend the database mirroring parameters to BlackBerry Enterprise Server components, 129

Sending software and BlackBerry Java Applications to BlackBerry devices

12

Managing BlackBerry Java Applications and BlackBerry Device Software

You can use the BlackBerry Administration Service to install and manage the BlackBerry Device Software and BlackBerry Java Applications on BlackBerry devices.

To send BlackBerry Java Applications to devices, you must first add the applications to the application repository. You can use the application repository to store and manage all versions of the BlackBerry Java Applications that you want to install on, update on, or remove from devices.

In the BlackBerry Administration Service, you create software configurations to specify the versions of the BlackBerry Device Software and BlackBerry Java Applications that you want to install on, update on, or remove from devices. You also use software configurations to specify which applications are required, optional, or not permitted. When you create a software configuration, you must also specify whether users can install applications that are not listed in the software configuration.

When you add a BlackBerry Java Application to a software configuration, you must assign an application control policy to the application to specify what resources the application can access. You can use default application control policies or you can create and use custom application control policies. If you permit users to install unlisted applications, you must create an application control policy for unlisted applications that specifies what resources the applications can access.

When you assign a software configuration to a group or individual user accounts, the BlackBerry Administration Service creates a deployment job to install the BlackBerry Device Software and BlackBerry Java Applications on devices and to apply application control policies to the devices. A deployment job consists of a number of tasks. Each task manages the delivery of a specific object (for example, a BlackBerry Java Application or an application control policy) by communicating with the appropriate BlackBerry Enterprise Server components.

If you assign more than one software configuration to a user account, all of the settings in the multiple software configurations are applied to the user's device. The BlackBerry Enterprise Server resolves conflicting settings using predefined reconciliation rules and prioritized rankings that you can specify using the BlackBerry Administration Service.

After you install the BlackBerry Device Software and BlackBerry Java Applications on devices, you can view details about how the BlackBerry Administration Service resolved software configuration conflicts.

For more information about installing and managing the BlackBerry Device Software on devices, visit www.blackberry.com/go/serverdocs to see the *BlackBerry Device Software Update Guide*.

Developing BlackBerry Java Applications for BlackBerry devices

Application developers can use the BlackBerry Java Development Environment or the for Eclipse to create and test BlackBerry Java Applications for BlackBerry devices, and to package BlackBerry Java Applications to install them on BlackBerry devices using a user's computer or over the wireless network. Application developers can use the BlackBerry JDE or the BlackBerry Java Plug-in for Eclipse to generate .cod files that contain the compiled application code for a BlackBerry Java Application. BlackBerry devices execute .cod files to run BlackBerry Java Applications. The BlackBerry JDE and the BlackBerry Java Plug-in for Eclipse also include tools to generate .jad files or .alx descriptor files that provide information about a BlackBerry Java Application that is used when the application is compiled.

MIDlets are Java applications that conform to the MIDP standard and can run on any mobile device that runs Java applications. Most MIDlets are distributed as .jar files. The BlackBerry JDE and the BlackBerry Java Plug-in for Eclipse include tools that you can use to convert existing MIDlets that are in .jad and .jar file formats to .cod file formats for use on BlackBerry devices.

For more information about developing and customizing BlackBerry Java Applications, visit www.blackberry.com/developers.

Preparing to distribute BlackBerry Java Applications

To send a BlackBerry Java Application to BlackBerry devices, the application developer must create a .zip file that contains the necessary application files and an .alx file that contains information about the application. If a directory structure is described in the .alx file, that directory structure must be represented in the .zip file.

For more information about creating BlackBerry Java Applications and .alx files, visit www.blackberry.com/developers to see the *BlackBerry Java Development Environment Development Guide*.

Before you distribute BlackBerry Java Applications, you must specify a shared network folder for BlackBerry Java Applications using the BlackBerry Administration Service. This shared network folder must not be the same network share location that is used for BlackBerry Device Software, and it must not be located in <*drive*>:\Program Files\Common Files \Research In Motion . The BlackBerry Administration Service accesses the shared network folder to install BlackBerry Java

Applications on BlackBerry devices. Do not add application files to the shared network folder or make changes to the files that the BlackBerry Administration Service stores in the shared network folder.

To make a BlackBerry Java Application available for installation on BlackBerry devices, you must add the application to the BlackBerry Administration Service application repository. After you add an application to the application repository, you can add the application to a software configuration, specify whether the application is required, optional, or not permitted on BlackBerry devices, and assign an application control policy to the application to control the access permissions for the application. You assign software configurations to user accounts to install or upgrade BlackBerry Java Applications on BlackBerry devices, or to remove BlackBerry Java Applications from BlackBerry devices.

Specify a shared network folder for BlackBerry Java Applications

Before you begin: Create a shared network folder on the network that hosts the BlackBerry Enterprise Server. This shared network folder must not be the same network share location that is used for BlackBerry Device Software, and it must not be located in <*drive*>:\Program Files\Common Files\Research In Motion .

The administration accounts that you use for the BlackBerry Administration Service must have write permissions for the shared network folder. The administration accounts that run the BlackBerry Administration Service Application Server service must have write permissions for the shared network folder. BlackBerry devices and the computers that host the BlackBerry Enterprise Server instances must have access to the shared network folder.

You must specify a shared network folder for BlackBerry Java Applications using the BlackBerry Administration Service before you add any BlackBerry Java Applications to the application repository. The BlackBerry Administration Service must access the shared network folder to install BlackBerry Java Applications on BlackBerry devices. Do not add application files to the shared network folder or make changes to the files that the BlackBerry Administration Service stores in the shared network folder.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service**.
3. Click **Edit component**.
4. In the **Software management** section, in the **BlackBerry Administration Service application shared network drive** field, type the path of the shared network folder using the following format: \\<*computer_name*>\<*shared_folder*>.

   The shared network path must be typed in UNC format (for example, \\ComputerName\Applications\Testing).

5. Click **Save all**.

Add a BlackBerry Java Application to the application repository

To send a BlackBerry Java Application to BlackBerry devices, you must first add the BlackBerry Java Application bundle to the application repository. To send an updated version of a BlackBerry Java Application to BlackBerry devices, you must first add the updated bundle to the application repository.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software** > **Applications**.
2. Click **Add or update applications**.
3. In the **Application location** section, click **Browse**. Navigate to the BlackBerry Java Application bundle that you want to add to, or update in, the application repository.
4. Click **Next**.
5. Click **Add application**.

Add a collaboration client to the application repository

To send a collaboration client to BlackBerry devices, you must first add the collaboration client bundle to the application repository. To send an updated version of a collaboration client to BlackBerry devices, you must first add the updated bundle to the application repository.

Before you begin: To download the .zip file for the latest version of the collaboration client, visit www.blackberry.com/support/downloads. For information about collaboration clients and whether they are compatible with specific versions of the BlackBerry Enterprise Server, visit na.blackberry.com/eng/support/downloads/im_server_compatibility.jsp.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software** > **Applications**.
2. Click **Add or update applications**.
3. In the **Application location** section, navigate to the collaboration client bundle that you want to add to, or update in, the application repository.
4. Click **Next**.
5. Click **Publish application**.

Specify keywords for a BlackBerry Java Application

You can specify keywords for a BlackBerry Java Application. You can use the keywords to search for the application in the application repository.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software** > **Applications**.
2. Click **Manage applications**.
3. Search for an application.
4. In the search results, click the name of an application.
5. Click **Edit application**.
6. In the **Application keywords** field, type a keyword.
7. Click the **Add** icon.
8. Repeat steps 6 and 7 for each keyword that you want to add.
9. Click **Save all**.

Configuring application control policies

When you add a BlackBerry Java Application to a software configuration so that you can install the application on BlackBerry devices, you must specify an application control policy that you want to apply to the BlackBerry Java Application. Application control policies control the data and APIs that BlackBerry Java Applications can access on BlackBerry devices, and the external data sources and network connections that BlackBerry Java Applications can access.

The BlackBerry Administration Service includes a standard application control policy for BlackBerry Java Applications that you classify as required, optional, or not permitted. You can change the default settings of the standard application control policies or create custom application control policies for a BlackBerry Java Application.

For more information about configuring settings for application control policy rules, visit www.blackberry.com/go/serverdocs to see the *BlackBerry Enterprise Server Policy Reference Guide*.

Standard application control policies

The BlackBerry Enterprise Server includes the following standard application control policies.

Application control policy	Description
Standard Required	When you apply the application control policy to a BlackBerry Java Application, rule settings require that the BlackBerry Java Application be installed and permitted to run on BlackBerry devices. BlackBerry devices install the application automatically.
Standard Optional	When you apply the application control policy to a BlackBerry Java Application, rule settings make the BlackBerry Java Application optional on the BlackBerry device. Users can install and run the BlackBerry Java Application on their BlackBerry devices.
Standard Disallowed	When you apply the application control policy to a BlackBerry Java Application, rule settings prevent users from installing the BlackBerry Java Application on BlackBerry devices. Users cannot install and run the BlackBerry Java Application on their BlackBerry devices.

Change a standard application control policy

When you add a BlackBerry Java Application to a software configuration, you must assign an application control policy to the BlackBerry Java Application. Based on the requirements of your organization's environment, you can change the default settings for the standard application control policies.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software** > **Applications**.
2. Click **Manage default application control policies**.
3. Click the standard application control policy that you want to change.
4. Click **Edit application control policy**.
5. On the **Access settings** tab, in the **Settings** section, change the settings for the standard application control policy.
6. Click **Save all**.

Create custom application control policies for a BlackBerry Java Application

After you add a BlackBerry Java Application to the application repository, you can configure the application to use the standard application control policies, or you can create custom application control policies for the application. If you want a BlackBerry Java Application to use custom application control policies, you must create the custom application control policies before you add the application to a software configuration. When you add the application to a software configuration, you can select which custom application control policy you want to apply to the application.

If you add the BlackBerry Java Application to multiple software configurations and you assign different custom application control policies to the BlackBerry Java Application in the different software configurations, you must set the priority for the custom application control policies. This priority determines which custom application control policy the BlackBerry Policy Service applies if you assign multiple software configurations to a user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software** > **Applications**.
2. Click **Manage applications**.
3. Search for a BlackBerry Java Application.
4. In the search results, click a BlackBerry Java Application.
5. In the **Application versions** section, click the version of the application that you want to create a custom application control policy for.
6. Click **Edit application**.
7. On the **Application control policies** tab, in the **Settings** section, select the **Use custom application control policies** option.
8. Perform any of the following tasks:

Task	Steps
Create an application control policy for required BlackBerry Java Applications.	1. In the **Required application name** field, type a name for the application control policy. 2. In the **Settings** section, configure the settings for the application control policy. 3. Click the **Add** icon. 4. Repeat steps a to c for each application control policy that you want to create.
Create an application control policy for optional BlackBerry Java Applications.	1. In the **Optional application name** field, type a name for the application control policy. 2. In the **Settings** section, configure the settings for the application control policy. 3. Click the **Add** icon. 4. Repeat steps a to c for each application control policy that you want to create.
Create an application control policy for BlackBerry Java Applications that are not permitted.	1. In the **Disallowed application name** field, type a name for the application control policy. 2. Click the **Add** icon.

9. If necessary, in each section, click the up and down arrows to set the priority for the application control policies.

10. Click **Save all**.

IT policy rules take precedence on smartphones

IT policy rule settings override application control policy rule settings. For example, if you change the Allow Internal Connections IT policy rule to No for BlackBerry smartphones, and if the smartphones have an application control policy set that allows a specific application to make internal connections, the application cannot make internal connections.

The smartphone revokes an application control policy and resets if the permissions of the application it is applied to become more restrictive. Smartphones permit users to make application permissions more restrictive, but not less restrictive, than the permissions that you specify.

Application control policies for unlisted applications

When you create a software configuration and assign it to user accounts so that you can send BlackBerry Device Software, BlackBerry Java Applications, and standard application settings to BlackBerry devices, you must configure whether the software configuration permits users to install and use applications that are not included in the software configuration (also known as unlisted applications). When you configure whether unlisted applications are permitted and optional or not permitted on BlackBerry devices, you must assign an application control policy for unlisted applications to the software configuration.

An application control policy for unlisted applications determines what unlisted applications are permitted on BlackBerry devices and what data the unlisted applications can access on BlackBerry devices. The BlackBerry Administration Service has two standard application control policies for unlisted applications: one for unlisted applications that are optional, and one for unlisted applications that are not permitted. You can change the default settings of the standard application control policy for unlisted applications that are optional, or you can create custom application control policies for unlisted applications that are optional.

For more information about the rule settings in application control policies for unlisted applications, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Change the standard application control policy for unlisted applications that are optional

For more information about the rule settings in application control policies for unlisted applications, see the *BlackBerry Enterprise Server Policy Reference Guide*.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software**.

2. Click **Manage application control policies for unlisted applications**.
3. Click the **Standard Unlisted Optional** application control policy.
4. Click **Edit application control policy**.
5. On the **Access settings** tab, in the **Settings** section, configure the settings for the application control policy.
6. Click **Save all**.

Create an application control policy for unlisted applications

The BlackBerry Administration Service includes two default application control policies for unlisted applications: one for unlisted applications that you permit on BlackBerry devices, and one for unlisted applications that you do not permit on BlackBerry devices. You can also create custom application control policies for unlisted applications that are optional.

For more information about the rule settings in application control policies for unlisted applications, see the *BlackBerry Enterprise Server Policy Reference Guide*.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software**.
2. Click **Create an application control policy for unlisted applications**.
3. In the **Application control policy information** section, in the **Name** field, type a name for the application control policy for unlisted applications.
4. Click **Save**.
5. On the **BlackBerry solution management** menu, click **Manage application control policies for unlisted applications**.
6. Click the application control policy that you created.
7. Click **Edit application control policy**.
8. On the **Access settings** tab, in the **Settings** section, configure the settings for the application control policy.
9. Click **Save all**.

Configure the priority of application control policies for unlisted applications

You can assign multiple software configurations to user accounts. You can assign different application control policies for unlisted applications to different software configurations. You must configure the priority of the different application control policies for unlisted applications so that the BlackBerry Policy Service can determine which application control policies to apply to user accounts when you assign multiple software configurations to user accounts.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software**.
2. Click **Manage application control policies for unlisted applications**.
3. Click **Set priority of application control policies for unlisted applications**.
4. Click the up and down arrows to set the priority of application control policies for unlisted applications.
5. Click **Save**.

Creating software configurations

You can use software configurations to perform the following actions on BlackBerry devices:

- install, upgrade, or remove BlackBerry Java Applications and the BlackBerry collaboration client over the wireless network or using the BlackBerry Web Desktop Manager
- assign application control policies to BlackBerry Java Applications to control application permissions and the data that the applications can access
- specify that a BlackBerry Java Application is not permitted
- specify whether BlackBerry Java Applications that you do not include in the software configuration are permitted or not permitted
- configure the access permissions for BlackBerry Java Applications that you do not include in the software configuration
- install or upgrade the BlackBerry Device Software over the wireless network or using the BlackBerry Web Desktop Manager
- specify standard application settings

You can assign a software configuration to a group, multiple user accounts, or a single user account. After you assign a software configuration, you can change the settings in the software configuration to manage the BlackBerry Java Applications, BlackBerry Device Software, and standard application settings on 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 BlackBerry devices.

If you assign multiple software configurations to a user account, the settings in each software configuration are applied to the BlackBerry device. The BlackBerry Administration Service uses a set of rules to resolve conflicting settings in the multiple software configurations.

The *BlackBerry Enterprise Server Administration Guide* contains information about creating software configurations to manage BlackBerry Java Applications on BlackBerry devices. For more information about using software configurations to manage BlackBerry Device Software on BlackBerry devices, visit www.blackberry.com/go/serverdocs to see the *BlackBerry Device Software Upgrade Guide*.

Related information

Reconciliation rules for conflicting settings in software configurations, 161

Create a software configuration

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software**.
2. Click **Create a software configuration**.
3. In the **Configuration information** section, in the **Name** field, type a name for the software configuration.
4. In the **Disposition for unlisted applications** drop-down list, perform one of the following actions:
   - To permit users to install applications that are not included in the software configuration on their BlackBerry devices, click **Optional**.
   - To prevent users from installing applications that are not included in the software configuration on their BlackBerry devices, click **Disallowed**.
5. In the **Application control policy for unlisted applications** drop-down list, click the application control policy for unlisted applications that you want to assign to the software configuration.
6. Click **Save**.

After you finish: Add BlackBerry Device Software configurations and BlackBerry Java Applications to the software configuration.

Add a BlackBerry Java Application to a software configuration

You must add a BlackBerry Java Application to a software configuration and assign the software configuration to user accounts to install the BlackBerry Java Application on BlackBerry devices over the wireless network. To upgrade an application, you must add the new version of the application to the appropriate software configuration. The BlackBerry Enterprise Server upgrades the application that is on BlackBerry devices to the new version.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software**.
2. Click **Manage software configurations**.
3. Click the software configuration that you want to add a BlackBerry Java Application to.
4. Click **Edit software configuration**.
5. On the **Applications** tab, click **Add applications to software configuration**.
6. Search for the BlackBerry Java Applications that you want to add to the software configuration.
7. In the search results, select a BlackBerry Java Application that you want to add to the software configuration.
8. In the **Disposition** drop-down list for the BlackBerry Java Application, perform one of the following actions:

- To install the BlackBerry Java Application automatically on BlackBerry devices, and to prevent users from removing the application, click **Required**.
- To permit users to install and remove the BlackBerry Java Application, click **Optional**.
- To prevent users from installing a BlackBerry Java Application on BlackBerry devices, click **Disallowed**.

9. In the **Application data** section, in the **Application control policy** drop-down list, click an application control policy to apply to the BlackBerry Java Application.
10. If necessary, in the **Deployment** drop-down list, perform one of the following actions:
    - To install the application on BlackBerry devices over the wireless network, click **Wireless**.
    - To install the application on BlackBerry devices using a USB connection to the user's computer and the BlackBerry Web Desktop Manager, click **Wired**.
11. Repeat steps 6 to 10 for each BlackBerry Java Application that you want to add to the software configuration.
12. Click **Add to software configuration**.
13. Click **Save all**.

Assign a software configuration to a group

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. Click a group.
4. Click **Edit group**.
5. On the **Software configuration** tab, in the **Available software configurations** list, click a software configuration.
6. Click **Add**.
7. Repeat steps 5 and 6 for each software configuration that you want to assign.
8. Click **Save all**.

Related information

Create a group to manage similar user accounts, 84
View the status of a job, 150
Managing the default distribution settings for jobs, 292
Managing the distribution settings for a specific job, 298
Managing software configurations, 306

Assign a software configuration to multiple user accounts

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for one or more user accounts.
4. Select one or more user accounts.
5. In the **Add to user configuration** list, click **Add software configuration**.
6. In the **Available software configurations** list, click the software configuration that you want to assign to the user accounts.
7. Click **Add**.
8. Repeat steps 6 and 7 for each software configuration that you want to assign to the user accounts.
9. Click **Save**.

Related information

View the status of a job, 150
Managing the default distribution settings for jobs, 292
Managing the distribution settings for a specific job, 298
Managing software configurations, 306

Assign a software configuration to a user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. On the **Software configuration** tab, in the **Available software configurations** list, click the appropriate software configuration.
7. Click **Add**.
8. Repeat steps 6 and 7 for each software configuration that you want to assign.
9. Click **Save all**.

When you assign a software configuration to a user account, the BlackBerry Administration Service creates a job to deliver the resulting object to the BlackBerry device.

Related information

View the status of a job, 150
Managing the default distribution settings for jobs, 292
Managing the distribution settings for a specific job, 298
Managing software configurations, 306

Install BlackBerry Java Applications on a BlackBerry device at a central computer

If you do not want to install BlackBerry Java Applications on a BlackBerry device over the wireless network, and you do not want the user to install the BlackBerry Java Applications using the BlackBerry Web Desktop Manager or BlackBerry Desktop Software, you can install the BlackBerry Java Applications on a BlackBerry device by connecting the BlackBerry device to a central computer that can access the BlackBerry Administration Service.

Before you begin:

- Assign a software configuration with the necessary BlackBerry Java Applications to the appropriate user account.
- To permit the BlackBerry Administration Service to connect to a BlackBerry device that is attached to the computer that hosts the BlackBerry Administration Service by a USB connection, add the web address of the BlackBerry Administration Service to the list of trusted web sites in the web browser. Log in to the BlackBerry Administration Service again.
- Verify that the central computer can access the BlackBerry Administration Service.
- Connect the BlackBerry device that is associated with the user account to the central computer.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Attached devices**.
2. Click **Device software**.
3. Click **Automatic installation of applications on the BlackBerry device**.
4. Complete the instructions on the screen.

View the status of a job

After you assign a software configuration to user accounts or change an existing software configuration that you assigned to user accounts, the BlackBerry Administration Service creates a job to deliver BlackBerry Device Software, BlackBerry Java applications, or application settings to BlackBerry devices. If you assign an IT policy to user accounts or change an existing IT policy, a job sends the IT policy changes to BlackBerry devices. You can view the status of a job to determine if it is ready to run, currently running, completed, or completed with task failures.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Manage deployment jobs**.
3. Search for a job.
4. In the search results, in the **Status** column, view the status of the job.
5. To view more information about a job or to change a job, click the ID of the job.

Related information

Stopping a job that is running, 158

View the status of a task

Each deployment job consists of multiple tasks. Each task delivers a specific object or setting to a BlackBerry device that carries out an action, for example, updating BlackBerry Device Software, installing or removing a BlackBerry Java Application, or applying updated IT policy settings or application settings. You can view the status of tasks. If a BlackBerry Enterprise Server does not complete a task, you can view error messages that help you troubleshoot the task failure.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Manage deployment job tasks**.
3. Search for a task.
4. In the search results, in the **Status** column, view the status of the task.
5. To view more information about a task, click **More**.

Error messages: BlackBerry Java Application tasks

To troubleshoot errors that display for a task when you send a BlackBerry Java Application to a BlackBerry device, or update a BlackBerry Java Application on a BlackBerry device, you can try to determine the cause by collecting the following information:

- BlackBerry Policy Service log files from the day the issue was reported (log level 4 recommended)

- BlackBerry Dispatcher log files from the day the issue was reported (log level 4 recommended)
- BlackBerry Administration Service log files from the day the issue was reported (log level 4 recommended)
- BlackBerry device information (for example, the BlackBerry device model, BlackBerry Device Software version, wireless service provider, IT policy assigned to the BlackBerry device, service books on the BlackBerry device, and so on)
- event log of the BlackBerry device from the day the issue was reported

If the preceding information does not help you to address the issue, you can collect the following information:

- BlackBerry Policy Service log files from the day the issue was reported (log level 6 recommended)
- system event logs
- copy of the BlackBerry Configuration Database
- SQL trace of the BlackBerry Policy Service that communicates with the BlackBerry Configuration Database

For information about changing the log level for a BlackBerry Enterprise Server component, visit www.blackberry.com/support to read article KB04342. For information about obtaining the event log for a BlackBerry device, visit www.blackberry.com/support to read article KB05349.

If the recommended administrative action for an error message does not resolve the issue, contact RIM Technical Support.

Sequence Processing Stopped due to error processing SEND_APC_APP command

The BlackBerry Policy Service sends application data to a BlackBerry device as a group of application modules. If the BlackBerry Policy Service does not deliver one of the application modules to the BlackBerry device, the remaining application modules are not delivered to the BlackBerry device.

You can try to resend the BlackBerry Java Application to the BlackBerry device.

SendApp failed due to error getting application data, processing stopped

An error occurred when the BlackBerry Policy Service tried to retrieve the data that it required to install the BlackBerry Java Application.

You can verify that the BlackBerry Policy Service can access the network share that you use to store the application files.

QueueModule failed, processing stopped

An error occurred when the BlackBerry Policy Service tried to process the application modules and send the application modules to the BlackBerry device.

You can verify that the BlackBerry Policy Service can access the network share that stores the application files.

Device timed out waiting for module

The BlackBerry device reported a timeout failure while waiting for the application modules.

You can resend the BlackBerry Java Application to the BlackBerry device. If the second attempt to install the BlackBerry Java Application is not successful, in the log files that you collected, locate the user account that experienced the issue. Trace the installation activity.

Device reported insufficient memory to install module

The BlackBerry device does not have enough application memory available to install the application modules.

You can instruct the user to make more application memory available on the BlackBerry device. Resend the BlackBerry Java Application.

Device reported insufficient privileges to install module

The BlackBerry device does not have the necessary permissions to install the BlackBerry Java Application.

You can verify that the BlackBerry device is configured with the necessary permissions to install a BlackBerry Java Application. Resend the BlackBerry Java Application.

Device reported invalid version in packet, supported version is %s

The BlackBerry Java Application is not compatible with the BlackBerry Device Software version that is running on the BlackBerry device.

You can verify that the BlackBerry Java Application is compatible with the BlackBerry Device Software version that is running on the BlackBerry device.

Device reported Data Format Error in packet while installing module

An error occurred in the BlackBerry Policy Service that prevented the BlackBerry device from installing the BlackBerry Java Application.

In the log files that you collected, locate the user account that experienced the issue. Trace the installation activity.

Device reported a %s error while installing module

Device reported a general failure installing the module

Device reported a security violation while installing the application

Device reported insufficient app data while installing module

Device reported insufficient body data while installing module

Device reported invalid app data length while installing module

Device reported invalid command while installing module

Device reported invalid module hash while installing module

Device reported that the module save failed

Device reported that there was an incomplete module

The BlackBerry device identified a formatting error in the application data before or during the installation process.

You can verify that the application files are formatted properly and try to send the BlackBerry Java Application to the BlackBerry device again. If your second try at the installation is not successful, in the log files that you collected, locate the user account that experienced the issue. Trace the installation activity.

Incomplete ACK data for APPD request

The BlackBerry Policy Service did not receive an acknowledgment message from a BlackBerry device that indicates that the BlackBerry Java Application was installed.

You can verify that the BlackBerry device is turned on and is located in a wireless coverage area. Resend the BlackBerry Java Application.

For the command: %s Device reported a general failure

For the command: %s Device reported non command handler for request

For the command: %s Device reported security violation

For the command: %s Device reported unable to decrypt

For the command: %s Device reported key mismatch

For the command: %s Device reported unsupported command version

For the command: %s Device reported code base error

For the command: %s Device reported a general failure installing the module

The BlackBerry device cannot execute the command to install or update the BlackBerry Java Application.

In the log files that you collected, locate the user account that experienced the issue. Trace the installation activity.

Error messages: BlackBerry Device Software tasks

To troubleshoot errors that display for a task when you are updating BlackBerry Device Software on a BlackBerry device, you can try to determine the cause by collecting the following information:

- BlackBerry Policy Service log files from the day the issue was reported (log level 4 recommended)
- BlackBerry Dispatcher log files from the day the issue was reported (log level 4 recommended)
- BlackBerry Administration Service log files from the day the issue was reported (log level 4 recommended)
- BlackBerry device information (for example, the BlackBerry device model, BlackBerry Device Software version, wireless service provider, IT policy assigned to the BlackBerry device, service books on the BlackBerry device, and so on)
- event log of the BlackBerry device from the day the issue was reported
- error report from the update application; instruct users to view the details of the errors reported by the update application and to send error reports to an administrative email address that you must specify

If the preceding information does not address the issue, you can collect the following information:

- BlackBerry Policy Service log files from the day the issue was reported (log level 6 recommended)
- system event logs
- copy of the BlackBerry Configuration Database
- SQL trace of the BlackBerry Policy Service that communicates with the BlackBerry Configuration Database

For information about changing the log level for a BlackBerry Enterprise Server component, visit www.blackberry.com/support to read article KB04342. For information about obtaining the event log for a BlackBerry device, visit www.blackberry.com/support to read article KB05349.

If the recommended administrative action for an error message does not resolve the issue, contact RIM Technical Support.

Available upgrade rejected

You can determine the reason for the error message and determine the status code that is associated with the error by viewing the event log of the BlackBerry device.

- **0x01 not supported by device**: The BlackBerry device model or the current version of the BlackBerry Device Software on the BlackBerry device does not support the BlackBerry Device Software update.

  You can verify that the BlackBerry device model and the current BlackBerry Device Software version support the BlackBerry Device Software update.

- **0x02 not consistent with device version or vendorid**: The BlackBerry device model, the current version of the BlackBerry Device Software on the device, or the vendor ID that is associated with the BlackBerry device does not support the BlackBerry Device Software update.

  You can verify that the BlackBerry device model, the current BlackBerry Device Software version, and the vendor ID that are associated with the BlackBerry device support the BlackBerry Device Software update.

- **0x03 disallowed by IT policy**: An IT policy rule in an IT policy that you assigned to the user account does not permit BlackBerry Device Software updates over the wireless network.

  You can verify that the IT policy rule settings in the IT policy that you assigned to the user account permits BlackBerry Device Software updates over the wireless network.

- **0x05 duplicate**: A previous request to install the same BlackBerry Device Software version has already been sent to the BlackBerry device.

- **0x07 bad request**: An error occured when the BlackBerry Infrastructure processed the request to update the BlackBerry Device Software on the BlackBerry device.

  You can try to send the BlackBerry Device Software update again.

- **0x08 insufficient storage**: The BlackBerry device does not have enough memory available to update the BlackBerry Device Software.

  You can manage the BlackBerry device so that it has enough memory available to update the BlackBerry Device Software (for example, remove applications from the BlackBerry device that are no longer required).

- **0x09 reset required**: The user must reset the BlackBerry device to clear a code module condition.

  You can instruct the user to reset the BlackBerry device and you can send the BlackBerry Device Software update again.

- **0X10 service book flag disabled**: A service book on the BlackBerry device does not permit you to send BlackBerry Device Software updates over the wireless network.

You can verify that the service books on the BlackBerry device permit BlackBerry Device Software updates over the wireless network.

Available upgrade deferred by user

- **0x01 prior upgrade in progress**: The BlackBerry Device Software update did not complete because a previous BlackBerry Device Software update was in progress.

  If the previous BlackBerry Device Software update did not install the correct BlackBerry Device Software version, you can wait until the update completes and then you can send the BlackBerry Device Software update again.

Upgrade prompt deferred

- **0x02 reset required** The user must reset the BlackBerry device to clear a code module condition.

  You can instruct the user to reset the BlackBerry device. The update application tries to perform the update for up to 72 hours. After 72 hours, the update application performs the update and the user no longer has the option to defer the update.

Upgrade rejected

An error or inconsistency exists in the BlackBerry Device Software files that are available from the BlackBerry Infrastructure.

Upgrade failed, rollback complete

After the update application downloaded and applied the current BlackBerry Device Software patch files to the BlackBerry device, an error occurred when the update application tried to restart the BlackBerry device. As a result, the update application reapplied the previous BlackBerry Device Software files to the BlackBerry device and cancelled the BlackBerry Device Software update.

Available upgrade deleted by administrator

When a BlackBerry Device Software update request either completes or does not complete, this status message displays when the BlackBerry Infrastructure deletes the update request.

Mandatory upgrade failed

After the update application downloaded and applied the current BlackBerry Device Software files to the BlackBerry device, an error occured when the update application tried to restart the BlackBerry device. As a result, the update application reapplied the previous BlackBerry Device Software files to the BlackBerry device, and cancelled the update.

BlackBerry Administration Service error

An error occurred when the BlackBerry Administration Service processed the request to update the BlackBerry Device Software on a BlackBerry device.

Related information

Restarting BlackBerry Enterprise Server components, 392

Error messages: Standard application settings tasks

To troubleshoot errors that display for a task when you change the standard application settings on a BlackBerry device, you can try to determine the cause by collecting the following information:

- BlackBerry Synchronization Service log files from the day the issue was reported (log level 4 recommended)
- BlackBerry Dispatcher log files from the day the issue was reported (log level 4 recommended)
- BlackBerry Administration Service log files from the day the issue was reported (log level 4 recommended)
- BlackBerry device information (for example, the BlackBerry device model, BlackBerry Device Software version, wireless service provider, IT policy assigned to the BlackBerry device, service books on the BlackBerry device, and so on)
- event log of the BlackBerry device from the day the issue was reported

If the preceding information does not address the issue, you can collect the following information:

- BlackBerry Synchronization Service log files from the day the issue was reported (log level 6 recommended)
- system event logs
- copy of the BlackBerry Configuration Database
- SQL trace of the BlackBerry Synchronization Service that communicates with the BlackBerry Configuration Database

For information about changing the log level for a BlackBerry Enterprise Server component, visit www.blackberry.com/support to read article KB04342. For information about obtaining the event log of a BlackBerry device, visit www.blackberry.com/support to read article KB05349.

If the recommended administrative action for an error message does not resolve the issue, contact RIM Technical Support.

Restore failed -- error getting value

The BlackBerry Synchronization Service cannot read the value of the standard application settings because the BlackBerry Configuration Database is unavailable.

Verify that the BlackBerry Synchronization Service can access the BlackBerry Configuration Database. If necessary, restart the BlackBerry Configuration Database.

Failed to set properties for item

The BlackBerry Synchronization Service cannot specify the value of the standard application settings because the BlackBerry Configuration Database is unavailable.

Verify that the BlackBerry Synchronization Service can access the BlackBerry Configuration Database. If necessary, restart the BlackBerry Configuration Database.

Failed to backup data to database

The BlackBerry Synchronization Service cannot apply the value of the standard application settings because the BlackBerry Configuration Database is unavailable.

Verify that the BlackBerry Synchronization Service can access the BlackBerry Configuration Database. If necessary, restart the BlackBerry Configuration Database.

Failed to delete item

The BlackBerry Synchronization Service cannot delete the value of the standard application settings because the BlackBerry Configuration Database is unavailable.

Verify that the BlackBerry Synchronization Service can access the BlackBerry Configuration Database. If necessary, restart the BlackBerry Configuration Database.

Failed to create an instance of the XML DOM document

The BlackBerry Synchronization Service cannot create XML data for the standard application settings.

Failed to load XML document

The BlackBerry Synchronization Service cannot load XML data for the standard application settings.

Invalid GUID

The BlackBerry Synchronization Service received an invalid globally unique identifier from the BlackBerry device.

Invalid/unknown command

The BlackBerry Synchronization Service received an invalid command from the BlackBerry device.

Related information
Restarting BlackBerry Enterprise Server components, 392

Error messages: IT policy tasks

To troubleshoot errors that display for a task when you send an IT policy to a BlackBerry device or update an IT policy on a BlackBerry device, you can try to determine the cause by collecting the following information:

- BlackBerry Policy Service log files from the day the issue was reported (log level 4 recommended)
- BlackBerry Dispatcher log files from the day the issue was reported (log level 4 recommended)
- BlackBerry Administration Service log files from the day the issue was reported (log level 4 recommended)
- BlackBerry device information (for example, the BlackBerry device model, BlackBerry Device Software version, wireless service provider, IT policy assigned to the BlackBerry device, service books on the BlackBerry device, and so on)
- event log of the BlackBerry device from the day the issue was reported

If the preceding information does not help you to address the issue, you can collect the following information:

- BlackBerry Policy Service log files from the day the issue was reported (log level 6 recommended)
- system event logs
- copy of the BlackBerry Configuration Database
- SQL trace of the BlackBerry Policy Service that communicates with the BlackBerry Configuration Database

For information about changing the log level for a BlackBerry Enterprise Server component, visit www.blackberry.com/support to read article KB04342. For information about obtaining the event log for a BlackBerry device, visit www.blackberry.com/support to read article KB05349.

If the recommended administrative action for an error message does not resolve the issue, contact Research In Motion Technical Support.

Reject Security Violation

Reject Authentication Failed

Data might not have been permanently deleted from the BlackBerry device before you assigned the BlackBerry device to a new user account and activated the BlackBerry device again.

You can permanently delete the data on the BlackBerry device and activate the BlackBerry device again.

Invalid password

Set Password Failed

You sent the Specify new device password and lock device IT administration command to a BlackBerry device and the password might not have satisfied the password criteria that the BlackBerry device user configured on the BlackBerry device.

You can resend the Specify new device password and lock device IT administration command to the BlackBerry device and specify a password that satisfies the password criteria that you configured using IT policy rules.

Sequence Processing Stopped due to error processing SET_IT_POLICY_COMMAND command

The BlackBerry Policy Service can send the IT policy data to a BlackBerry device in a group of commands. If the IT policy command is not delivered to the BlackBerry device, the remaining commands in the group are not delivered to the BlackBerry device.

You can try to resend the IT policy to the BlackBerry device. You can also try to resend the service books to the BlackBerry device.

Stopping a job that is running

After you assign a software configuration to user accounts or change an existing software configuration that you already assigned to user accounts, the BlackBerry Administration Service creates a job to deliver BlackBerry Device Software, BlackBerry Java Applications, or application settings to BlackBerry devices. If you assign an IT policy to user accounts or change an existing IT policy, a job sends the IT policy changes to BlackBerry devices. If you want to make changes to a job that is running, you can stop a job.

When you stop a job, the BlackBerry Enterprise Server does not process the remaining tasks in the job, and the BlackBerry Administration Service changes the scheduled start time for the job to the following day. The job returns to a ready to run status. You can make changes to the start time, priority, and distribution settings of the job. If you do not change the start time for the job, the BlackBerry Enterprise Server delivers the job on the following day using the default job schedule settings. When the job starts again, the BlackBerry Enterprise Server processes the remaining tasks in the job.

If you want to delete a job, change the start date of the job to a date that exceeds the job failure period that you configured in the job schedule settings. The default job failure period is 30 days.

Related information

Change default settings for a job schedule, 292
Specify the start time and priority for a job, 299

Stop a job that is running

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Manage deployment jobs**.
3. Search for the job that you want to stop.
4. In the search results, click the ID of the job that you want to stop.
   You can only stop jobs with a Running status.
5. Click **Stop Current Execution**.
6. Click **Yes - Stop Current Execution**.

Related information

View the status of a job, 150
Managing the default distribution settings for jobs, 292
Managing the distribution settings for a specific job, 298

View the users that have a BlackBerry Java Application installed on their BlackBerry devices

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software** > **Applications**.
2. Click **Manage applications**.
3. Search for an application.
4. In the search results, click the name of an application.
5. In the **Application versions** section, click a version of the application.

6. Click **View users with application**.
7. Search for users that are associated with BlackBerry devices that you installed the BlackBerry Java Application on.

View how the BlackBerry Administration Service resolved software configuration conflicts for a user account

You can assign multiple software configurations to a user account or group. The BlackBerry Administration Service uses specific rules to resolve conflicting settings in the multiple software configurations that you assign to a user account or group. After the BlackBerry Administration Service applies software configurations to a BlackBerry device, you can view how the BlackBerry Administration Service resolved any of the conflicting settings in the multiple software configurations.

Before you begin: Assign multiple software configurations to a user account or group.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. Click the name of a user account.
5. On the **Software configuration** tab, perform one of the following actions:
   - To view how the BlackBerry Administration Service resolved conflicts that involve BlackBerry Java Applications, click **View resolved applications**.
   - To view how the BlackBerry Administration Service resolved conflicts that involve BlackBerry Device Software, click **View Resolved BlackBerry Device Software bundles**.
   - To view how the BlackBerry Administration Service resolved conflicts that involve application control policies for unlisted applications, click **View Resolved Application Control Policy for Unlisted Applications**.
   - To view how the BlackBerry Administration Service resolved conflicts that involve the standard application settings in BlackBerry Device Software configurations, click **View Resolved BlackBerry Device Software application settings**.
6. View the appropriate information about how the BlackBerry Administration Service resolved the software configuration conflicts for the user account.

Reconciliation rules for conflicting settings in software configurations

If you assign multiple software configurations to user accounts or groups, the multiple software configurations might contain conflicting settings. For example, you might specify that a BlackBerry Java Application is required in a software configuration that you assign to a user account, but you might also specify that the same application is not permitted in a software configuration that you assign to a group that the user account belongs to. Conflicts can occur when you assign multiple BlackBerry Java Applications, application control policies, application control policies for unlisted applications, BlackBerry Device Software, and the standard application settings in BlackBerry Device Software configurations.

The BlackBerry Administration Service uses predefined reconciliation rules to resolve conflicting settings in multiple software configurations, and to determine which applications, software, and settings the BlackBerry Administration Service installs on or applies to a BlackBerry device. The BlackBerry Administration Service resolves conflicting settings as an asynchronous background activity. You can view the outcome of the reconciliation activities, reconciliation errors, and the applications, software, and settings that the BlackBerry Administration Service installed on or applied to a BlackBerry device.

The BlackBerry Administration Service might have to reconcile software configuration settings that conflict if you perform any of the following actions:

- activate a user account
- assign a new BlackBerry device or PIN to a user
- assign a user account to or remove a user account from a group
- add a group to or remove a group from another group
- add an application to or remove an application from a software configuration
- change the settings for an application in a software configuration
- change the settings for an application control policy
- change the ranking for application control policies
- install a new version of the BlackBerry Device Software on a BlackBerry device
- add a BlackBerry Device Software configuration to or remove a BlackBerry Device Software configuration from a software configuration
- change a BlackBerry Device Software configuration
- change the standard application settings in a BlackBerry Device Software configuration

Reconciliation rules: BlackBerry Java Applications

Scenario	Rule
Multiple software configurations are assigned to a user account or the groups the user belongs to. Multiple BlackBerry Java Applications are contained in each software configuration.	The BlackBerry Java Applications in each software configuration are installed on the BlackBerry device. If the BlackBerry Device Software does not support a specific BlackBerry Java Application, the application is not installed on the BlackBerry device.
Multiple software configurations that contain different versions of the same BlackBerry Java Application are assigned to a user account or the groups the user belongs to.	When different versions of an application exist in the software configurations that are assigned to a user account, the latest version of the application that is supported by the BlackBerry Device Software is installed on the BlackBerry device. For example, if a software configuration with version 1.0 of an application is assigned to a user account, and another software configuration with version 2.0 of the application is assigned to a user account, version 2.0 of the application is installed on the BlackBerry device. The version of a BlackBerry Java Application that is in a software configuration that is assigned to a user account takes precedence over the version of a BlackBerry Java Application that is in a software configuration that is assigned to a group. For example, if version 1.0 of an application is in a software configuration that is assigned to a user account, and version 2.0 of an application is in a software configuration that is assigned to a group that the user belongs to, version 1.0 of the application is installed on the BlackBerry device.
Multiple software configurations that contain the same BlackBerry Java Application are assigned to a user account or the groups the user belongs to. The disposition of the BlackBerry Java Application (required, optional, or disallowed) is different in each software configuration. The deployment method (wired or over the wireless network) for the application is different in each software configuration.	The disposition specified for an application in a software configuration that is assigned to a user account takes precedence over the disposition of the same application in any software configuration that is assigned to a group. If the application has different dispositions in multiple software configurations that are assigned at the same level (either to the user account or groups), the required disposition takes precedence over the optional disposition, and the optional disposition takes precedence over the disallowed disposition.

Scenario	Rule
	The BlackBerry Administration Service resolves the deployment method after resolving the disposition of an application. The deployment method specified for an application in a software configuration that is assigned to a user account takes precedence over the deployment method for the same application in any software configuration that is assigned to a group. The wireless setting takes precedence over the wired setting.
One or more software configurations that include BlackBerry Java Applications are assigned to a user account or the groups the user belongs to, but a limited amount of available memory remains on the BlackBerry device.	The BlackBerry Administration Service checks the amount of available memory on the BlackBerry device after resolving application conflicts (for example, resolving conflicting disposition and deployment settings) and before installing a BlackBerry Java Application. If there is not enough memory available on the BlackBerry device to support the application, the application is not installed. Depending on the amount of available memory, applications are installed in the following order: 1. Required applications that are configured for wireless deployment 2. Required applications that are configured for wired deployment 3. Optional applications that are configured for wireless deployment 4. Optional applications that are configured for wired deployment
A software configuration is assigned to a user account and it contains a BlackBerry Java Application that has a dependency on another BlackBerry Java Application.	If a BlackBerry Java Application in a software configuration has a dependency on another application, and the other application is not included in a software configuration that is assigned to the user account or a group that the user belongs to, the application is not installed on the BlackBerry device. If a BlackBerry Java Application in a software configuration has a dependency on another application, and the dependent application is included in a software configuration that is assigned to the user account or a group the user belongs to, the dependent application is installed first. If the dependent application is installed

Scenario	Rule
	successfully, the application with the dependency is then installed.
A software configuration is assigned to a user account and it contains a BlackBerry Java Application that has a dependency on another BlackBerry Java Application. The dependent application is not supported on the BlackBerry device.	If a dependent application is not supported by the BlackBerry device or was not installed successfully on the BlackBerry device, the application with the dependency is not installed on the user's BlackBerry device.
Multiple BlackBerry Java Applications have a circular dependency (for example, application A is dependent on application B, application B is dependent on application C, and application C is dependent on application A) and are included in the same application bundle. The application bundle is added to the application repository. The applications are added to a software configuration and assigned to a user account or a group the user belongs to.	If multiple BlackBerry Java Applications are included in the same application bundle and have a circular dependency, the applications are not installed on the BlackBerry device. If multiple applications have a circular dependency, they can only be installed if they exist in separate application bundles and are installed using wired deployment.

Reconciliation rules: BlackBerry Device Software

Scenario	Rule
A software configuration that contains BlackBerry Device Software is assigned to a user account. A software configuration that contains a different version of BlackBerry Device Software is assigned to a group that the user account belongs to.	The BlackBerry Device Software in a software configuration that is assigned to a user account takes precedence over the BlackBerry Device Software in a software configuration that is assigned to a group.
Multiple software configurations that contain different versions of BlackBerry Device Software are assigned to a user account.	The version of the BlackBerry Device Software that is supported by the BlackBerry device and by the wireless service provider, and that you ranked highest in the BlackBerry Administration Service, is installed on the BlackBerry device. The BlackBerry Enterprise Server does not install a version of the BlackBerry Device Software if that version is ranked lower than the version of the BlackBerry Device Software that is currently installed on the BlackBerry device.

Reconciliation rules: Standard application settings

Scenario	Rule
A software configuration with standard application settings is assigned to a user account. A software configuration with different standard application settings is assigned to a group that the user account belongs to.	The standard application settings in a software configuration that is assigned to a user account take precedence over the standard application settings in a software configuration that is assigned to a group.
A user account belongs to multiple groups. The calendar initial view setting is configured differently in each of the software configurations that are assigned to the groups.	The calendar initial view setting that is applied to the user's BlackBerry device is the lowest value that was specified in the multiple software configurations.
A user account belongs to multiple groups. The calendar keep appointments setting is configured differently in each of the software configurations that are assigned to the groups.	The calendar keep appointments setting that is applied to the user's BlackBerry device is the highest value that was specified in the multiple software configurations.
A user account belongs to multiple groups. The email confirm delete setting is set to Yes in one or more of the software configurations that are assigned to the groups. The setting is set to No in the remaining software configurations.	If the email confirm delete setting is set to Yes in a software configuration that is assigned to a group that the user account belongs to, the Yes setting is applied to the BlackBerry device.
A user account belongs to multiple groups. The email hide sent messages setting is set to Yes in one or more of the software configurations that are assigned to the groups. The setting is set to No in the remaining software configurations.	If the email hide sent messages setting is set to No in a software configuration that is assigned to a group that the user account belongs to, the No setting is applied to the BlackBerry device.
A user account belongs to multiple groups. The email save copy in sent folder setting is set to Yes in one or more of the software configurations that are assigned to the groups. The setting is set to No in the remaining software configurations.	If the email save copy in sent folder setting is set to Yes in a software configuration that is assigned to a group that the user account belongs to, the Yes setting is applied to the BlackBerry device.
A user account belongs to multiple groups. The address book sort by setting is configured differently in each of the software configurations that are assigned to the groups.	If the address book sort by setting is configured differently in the software configurations that are assigned to the groups that the user account belongs to, the first name setting takes precedence over the last name setting, and the last name setting takes precedence over the company name setting.
A user account belongs to multiple groups. The attributes settings for the various standard application settings are	The Locked and visible setting takes precedence over the Unlocked and visible setting. The Unlocked and visible

Scenario	Rule
configured differently in the software configurations that are assigned to the groups.	setting takes precedence over the Unlocked and hidden setting.
Standard application settings are configured in a software configuration and assigned to user accounts with BlackBerry devices that are running a BlackBerry Device Software version earlier than 5.0.	Standard application settings apply only to BlackBerry devices that are associated with BlackBerry Enterprise Server version 5.0 or later, and BlackBerry devices that are running BlackBerry Device Software version 5.0 or later.

Reconciliation rules: Application control policies

Scenario	Rule
A user is assigned multiple software configurations that each contain the same application. A different application control policy is assigned to the application in each software configuration.	An application control policy for an application in a software configuration that is assigned to a user account takes precedence over an application control policy for the same application in a software configuration that is assigned to a group. The required setting takes precedence over the optional setting. The optional setting takes precedence over the disallowed setting. If multiple software configurations contain the same application, and each software configuration is assigned a different custom application control policy with the same disposition (for example, two custom required application control policies), the application control policy that you ranked highest in the BlackBerry Administration Service is applied to the user's BlackBerry device.

Reconciliation rules: Application control policies for unlisted applications

Scenario	Rule
A software configuration with a default or custom application control policy for unlisted applications is assigned to a user account. A software configuration with a different application control policy for unlisted applications is assigned to a group that the user account belongs to.	The application control policy for unlisted applications in a software configuration that is assigned to a user account takes precedence over the application control policy for unlisted applications in a software configuration that is assigned to a group.

Scenario	Rule
A software configuration that defines unlisted applications as disallowed is assigned to a user account. A software configuration that defines unlisted applications as optional is also assigned to the user account.	If unlisted applications are defined as disallowed in a software configuration that is assigned to a user account, unlisted applications are not permitted on the BlackBerry device.
Multiple software configurations with different application control policies for unlisted applications are assigned to a user account.	The application control policy for unlisted applications that you ranked highest in the BlackBerry Administration Service is applied to the BlackBerry device.

Alternative methods for installing BlackBerry Java Applications on BlackBerry devices

Installing BlackBerry Java Applications on BlackBerry devices without using the BlackBerry Administration Service

You can install and update BlackBerry Java Applications on BlackBerry devices without using the BlackBerry Administration Service. You can use any of the following tools or software to install, update, and manage BlackBerry Java Applications on BlackBerry devices:

- BlackBerry Desktop Software
- BlackBerry Web Desktop Manager
- BlackBerry Application Web Loader on a web server
- standalone application loader tool
- web browser on BlackBerry devices

Developing BlackBerry Java Applications for BlackBerry devices

Application developers can use the BlackBerry Java Development Environment or the for Eclipse to create and test BlackBerry Java Applications for BlackBerry devices, and to package BlackBerry Java Applications to install them on

BlackBerry devices using a user's computer or over the wireless network. Application developers can use the BlackBerry JDE or the BlackBerry Java Plug-in for Eclipse to generate .cod files that contain the compiled application code for a BlackBerry Java Application. BlackBerry devices execute .cod files to run BlackBerry Java Applications. The BlackBerry JDE and the BlackBerry Java Plug-in for Eclipse also include tools to generate .jad files or .alx descriptor files that provide information about a BlackBerry Java Application that is used when the application is compiled.

MIDlets are Java applications that conform to the MIDP standard and can run on any mobile device that runs Java applications. Most MIDlets are distributed as .jar files. The BlackBerry JDE and the BlackBerry Java Plug-in for Eclipse include tools that you can use to convert existing MIDlets that are in .jad and .jar file formats to .cod file formats for use on BlackBerry devices.

For more information about developing and customizing BlackBerry Java Applications, visit www.blackberry.com/developers.

Methods you can use to install BlackBerry Java Applications on BlackBerry devices

If you do not want to use the BlackBerry Administration Service to install or update BlackBerry Java Applications on BlackBerry devices over the wireless network, you can use any of the following methods:

Method	Description
Install BlackBerry Java Applications using the BlackBerry Desktop Software	You can install a BlackBerry Java Application on a BlackBerry device by instructing the user to use the application loader tool that is part of the BlackBerry Desktop Software. An automated application installer installs the application files on the user's computer. The user uses the BlackBerry Desktop Manager to navigate to the application files and install the BlackBerry Java Application on a BlackBerry device that the user connects to the computer.
Install BlackBerry Java Applications using the BlackBerry Application Web Loader	You can install a BlackBerry Java Application on a BlackBerry device by instructing the user to browse to a specific web server that you configured to use the BlackBerry Application Web Loader. The user must connect the BlackBerry device to the computer.
Install BlackBerry Java Applications using the standalone application loader tool	You can install a BlackBerry Java Application on a BlackBerry device by installing the standalone application loader tool in a shared network folder, and providing users with a link to run the tool. The user must connect the BlackBerry device to the computer. This method requires that you install the BlackBerry Device Manager on the user's computer but does not require a full installation of the BlackBerry Desktop Software.

Method	Description
Install BlackBerry Java Applications using a web browser on BlackBerry devices	You can install a BlackBerry Java Application on a BlackBerry device by installing the files for the BlackBerry Java Application on a web server and instructing the user to browse to the appropriate web address on the BlackBerry device. Users can download the BlackBerry Java Application from an Internet web site using a web browser or from an intranet web site using the BlackBerry Browser. This method does not require the user to connect the BlackBerry device to the computer.

Installing BlackBerry Java Applications using the BlackBerry Desktop Software

Application developers can use the BlackBerry Java Development Environment or the for Eclipse to create an automated application installer. You can use the application installer to install the files for a BlackBerry Java Application (the .alx identifier file and the application's .cod files) on users' computers. You can then instruct users to use the application loader tool in the BlackBerry Desktop Software to install the BlackBerry Java Application on their BlackBerry devices. Users must connect their BlackBerry devices to their computers.

This method has the following advantages:

- You can control how the application files are distributed to users' computers.
- Users are responsible for completing the installation.
- If you installed the BlackBerry Desktop Software on users' computers, they can use it to install the BlackBerry Java Applications.

This method has the following disadvantages:

- You must install the BlackBerry Desktop Software on users' computers.
- The users must use the BlackBerry Desktop Software to install the BlackBerry Java Application.
- You cannot control when the users install the BlackBerry Java Application.
- Users must connect their BlackBerry devices to their computers.

Prerequisites: Installing BlackBerry Java Applications using the BlackBerry Desktop Software

BlackBerry device

- BlackBerry APIs and Java ME (standard on BlackBerry devices)

User's computer

- Windows 2000 or later, Windows XP, or Windows Vista
- BlackBerry Desktop Software version 4.0 or later
- Research In Motion USB drivers and a USB connection for the BlackBerry device

BlackBerry Java Application

- .alx files and .cod files: The .alx file is the application descriptor that provides information about the application and the location of the application's .cod files. A .cod file contains compiled and packaged application code. The application loader tool requires these files so that it can install the BlackBerry Java Application on BlackBerry devices.
- required modules: Some BlackBerry Java Applications require modules that are part of the BlackBerry Device Software. The required modules are listed in the .alx file in a <requires> tag. If the required modules do not exist on the BlackBerry device, you need to install the necessary BlackBerry Device Software on the BlackBerry device. For more information about application dependencies, visit www.blackberry.com/developers to read the *BlackBerry Java Development Environment Development Guide*.

Make the BlackBerry Java Application available to the BlackBerry Desktop Software

1. Obtain the application installer (.exe file) for the BlackBerry Java Application from the application developer, vendor, or wireless service provider.
2. Run the application installer on the user's computer to install the .alx identifier file and .cod file in an installation folder on the user's computer. You can also run the application installer to install the .alx identifier file and .cod file in a shared network folder that users can access from their computers.

Install the BlackBerry Java Application using the BlackBerry Desktop Software

For instructions for how to install a BlackBerry Java Application using the BlackBerry Desktop Software, visit www.blackberry.com/go/docs to find the required version of the *BlackBerry Desktop Software User Guide*.

Installing BlackBerry Java Applications using the BlackBerry Application Web Loader

You can configure the BlackBerry Application Web Loader, which uses Microsoft ActiveX, to install a BlackBerry Java Application on BlackBerry devices using a web server and Microsoft Internet Explorer on users' computers. You can add the BlackBerry Application Web Loader to a web server (for example, on your organization's intranet or a public web server), and instruct users to browse to the appropriate web address using Microsoft Internet Explorer. The BlackBerry Application Web Loader prompts users to install the BlackBerry Java Application, and installs the required .cod files for the application on BlackBerry devices. The users must connect their BlackBerry devices to their computers.

The BlackBerry Application Web Loader supports .cod files only. To install a MIDlet, convert the .jar file to a .cod file. For more information about how to compile .java and .jar file formats into the .cod file format, visit www.blackberry.com/developers to read the *BlackBerry Java Development Environment Development Guide*. For more information about the BlackBerry Application Web Loader and a sample development template, visit www.blackberry.com/go/docs to read the *BlackBerry Application Web Loader Developer Guide*.

This method has the following advantages:

- You do not have to install the BlackBerry Desktop Software on users' computers.
- The installation process is straightforward and requires Microsoft Internet Explorer, a common web browser.
- Users are responsible for completing the installation.

This method has the following disadvantages:

- You cannot control when the users install the BlackBerry Java Application.
- Users must connect their BlackBerry devices to their computers.

Prerequisites: Installing BlackBerry Java Applications using the BlackBerry Application Web Loader

BlackBerry device

- BlackBerry APIs and Java ME (standard on BlackBerry devices)

User's computer

- Windows 2000 or later, Windows XP, or Windows Vista

- Microsoft Internet Explorer version 5.0 or later
- Microsoft ActiveX version 8.0 or later
- BlackBerry Application Web Loader; if the BlackBerry Application Web Loader is not installed, the user is prompted to install it after the user browses to the specified web address
- Research In Motion USB drivers and a USB connection for the BlackBerry device

Web server

Configure the following MIME types on the web server to permit users to download and install BlackBerry Java Applications on BlackBerry devices:

- .cod files: application/vnd.rim.cod
- .jad files: text/vnd.sun.j2me.app-descriptor
- scripting language: Use a scripting language that is supported by Microsoft Internet Explorer and Microsoft ActiveX.
- AxLoader.cab file: Copy the AxLoader.cab file to the folder that the web page .html files are located in (or update the <object> element URL information in the .html file to the new location).

BlackBerry Java Application

- .jad files and .cod files: The .jad file is the application descriptor that provides information about the application and the location of .cod files. A .cod file contains compiled and packaged application code. The BlackBerry Application Web Loader requires these files to install the BlackBerry Java Application.
- The maximum .jad file size is 4096 bytes.
- The maximum number of .cod files supported by the BlackBerry Application Web Loader is 32.
- MIDlet support: The BlackBerry Application Web Loader supports CLDC applications that reference the BlackBerry API or MIDlets that have been converted to the .cod file format.

Enable the BlackBerry Application Web Loader on a web server

Before you begin:

- Obtain the .jad and .cod files for the BlackBerry Java Application from the application developer, vendor, or wireless service provider.
- Visit www.blackberry.com/developers to download the latest version of the BlackBerry Application Web Loader (AxLoader.cab).

1. Create a web page that you can use to install the BlackBerry Java Application on BlackBerry devices.
2. Copy the AxLoader.cab file to the folder where the web page’s .html files are located.
3. Copy the .jad and .cod files for the application on the web server that hosts the web page.

4. Reference a specific version of the BlackBerry Application Web Loader.

   For more information about referencing a specific version of the BlackBerry Application Web Loader, visit www.blackberry.com/go/docs to read the *BlackBerry Application Web Loader Developer Guide.*

5. Associate the BlackBerry Application Web Loader with the .jad file.
6. To load the .jad file, invoke loadJad(). Use a string parameter that represents one of the following:
   - If the .jad file is in the same location as the AxLoader.cab file, use the .jad file name.
   - If the .jad file is in a different location than the AxLoader.cab file, use the relative location address of the .jad file.
7. Send the web address to users.

The BlackBerry Application Web Loader requires the BlackBerry device password before it can install a BlackBerry Java Application. If a password is set, the AxLoaderPassword control is used to obtain the password. This control is included in the AxLoader.cab file. For more information about obtaining a BlackBerry device password, visit www.blackberry.com/go/docs to read the *BlackBerry Application Web Loader Developer Guide*.

Install the BlackBerry Java Application using the BlackBerry Application Web Loader

Send these instructions to users.

1. Connect the BlackBerry device to your computer.
2. Using Microsoft Internet Explorer version 5.0 or later, browse to <*web_address*>.
3. If the required version of the BlackBerry Application Web Loader is not installed on your computer, accept the installation prompt, and complete the instructions on the screen.
4. Complete the instructions on the screen to install the BlackBerry Java Application.

Installing BlackBerry Java Applications using the standalone application loader tool

The standalone application loader tool is included in the BlackBerry Enterprise Server installation files. You can make the standalone application loader tool available from a shared network folder and provide users with a link to run the tool and install the BlackBerry Java on their BlackBerry devices. The users must connect their BlackBerry devices to their computers to install the BlackBerry Java Application.

You must install the BlackBerry Device Manager on users' computers so that users can use this method to install BlackBerry Java Applications. The BlackBerry Device Manager manages the connection between the standalone application loader tool and the BlackBerry device. The BlackBerry Device Manager is included in the BlackBerry Desktop Software. You can also install the BlackBerry Device Manager on users' computers without installing the full BlackBerry Desktop Software. To download the BlackBerry Device Manager or the BlackBerry Desktop Software, visit na.blackberry.com/eng/support/downloads/.

You can also use the standalone application loader tool to install BlackBerry Java Applications in automated mode on BlackBerry devices. Automated mode installs the BlackBerry Java Application on BlackBerry devices without giving users the option to cancel the installation.

Advantages of this method include:

- The installation process is straightforward.
- Users are responsible for completing the installation.

Disadvantages of this method include:

- You cannot control when users install the BlackBerry Java Application.
- Users must connect the BlackBerry device to their computers.
- You must install the BlackBerry Desktop Software on users' computers.

Prerequisites: Installing BlackBerry Java Applications using the standalone application loader tool

BlackBerry device

- BlackBerry APIs and Java ME (standard on BlackBerry devices)

User's computer

- Windows 2000 or later, Windows XP, or Windows Vista
- BlackBerry Desktop Software version 4.0 or later
- BlackBerry Device Manager version 4.1 (for automated mode)
- Research In Motion USB drivers and USB connection

BlackBerry Java Application

- .alx file and .cod files: The .alx file is the application descriptor that provides information about the application and the location of the application's .cod files. A .cod file contains compiled and packaged application code. The standalone application loader tool requires these files to install the BlackBerry Java Application.
- required modules: Some BlackBerry Java Applications require modules that are part of the BlackBerry Device Software. The required modules are listed in the .alx file in a <requires> tag. If the required modules do not exist on the BlackBerry device, you must install the required BlackBerry Device Software on the BlackBerry device. For more

information about application dependencies, visit www.blackberry.com/developers to read the *BlackBerry Java Development Environment Development Guide*.

- required BlackBerry Java Applications: To configure a BlackBerry Java Application as required on a BlackBerry device, in the .alx file, after the copyright statement, add the following tag: <required>true</required>.

Add BlackBerry Java Application files to a shared network folder

Before you begin:

- The standalone application loader tool is installed when you install the BlackBerry Enterprise Server. Verify that the standalone application loader tool is installed in <*drive*>:\Program Files\Common Files\Research In Motion\AppLoader .
- Obtain the .alx and .cod files for the BlackBerry Java Application from the application developer, vendor, or wireless service provider.

1. In <*drive*:>\Program Files\Common Files\Research In Motion\Shared\Applications\ , create a folder with a unique name to contain the application files. Maintain the application's file structure.
2. Copy the .cod, .alx, and .dll files for the BlackBerry Java Application to the folder that you created.

Share the Research In Motion folder that contains the BlackBerry Java Application

1. Navigate to <*drive*>:\Program Files\Common Files\Research In Motion .
2. Right-click the **Research In Motion** folder. Click **Properties**.
3. On the **Sharing** tab, click **Share this folder**. Provide read-only permissions.
4. If necessary, configure other required options.
5. Click **OK**.

After you finish: Select a distribution method (for example, an email message or an intranet web page) that you can use to provide users with a link to the loader.exe file (for example, \\<*shared_computer_name*>\Research In Motion\Apploader \loader.exe .

Configure the standalone application loader tool to install the BlackBerry Java Application in automated mode

Use automated mode if you do not want to give users the option to cancel the installation of the BlackBerry Java Application.

Before you begin: Verify that BlackBerry Device Manager version 4.1 or later is installed on the user's computer.

When you distribute the link to the shared network folder to users, specify the loading command using the following format:

- USB: \\<*shared_computer_name*>\Research In Motion\Apploader\loader.exe /defaultUSB /forceload

Install the BlackBerry Java Application using the standalone application loader tool

Send these instructions to users.

Before you begin: Verify that the BlackBerry Desktop Software is installed on your computer. If it is not, contact your administrator.

1. Connect the BlackBerry device to your computer.
2. If prompted, type your BlackBerry device password.
3. Click **Next**.
4. On your computer, click the link to the loader.exe file that your administrator provided you with.
5. If a security warning displays, click **Run**.
6. Complete the instructions on the screen.
7. When the installation process completes, click **Close**.

Installing BlackBerry Java Applications using a web browser on BlackBerry devices

You can install BlackBerry Java Applications on BlackBerry devices over the wireless network. This method does not require users to connect their BlackBerry devices to their computers.

You can add the required files for the BlackBerry Java Application (a .jad file and the application .cod or .jar files) to a web server, and instruct users to navigate to the appropriate web address using a browser on their BlackBerry devices. Users can use the BlackBerry Browser or the wireless service provider's WAP Browser. When users access the web address, they can click a download option to install the BlackBerry Java Application on their BlackBerry devices.

This method has the following advantages:

- You do not have to install the BlackBerry Desktop Software on users' computers.
- Users do not have to connect their BlackBerry devices to their computers.
- Users are responsible for completing the installation.

This method has the following disadvantages:

- You cannot control when users install the BlackBerry Java Application.
- Installing a BlackBerry Java Application on BlackBerry devices over the wireless network can result in increased network usage.

Prerequisites: Installing BlackBerry Java Applications using a web browser on BlackBerry devices

BlackBerry device

- BlackBerry APIs and Java ME (standard on BlackBerry devices)

Web server

Configure the following MIME types on the web server to permit users to download and install BlackBerry Java Applications on BlackBerry devices:

- .cod files: application/vnd.rim.cod
- .jad files: text/vnd.sun.j2me.app-descriptor
- .jar files (optional): application/java-archive

BlackBerry Java Application

- .jad file: The .jad file is the application descriptor that provides information about the application and the location of the application's .cod or .jar files.
- .cod or .jar files: These files contain compiled and packaged application code.

Install the BlackBerry Java Application on a web server

Before you begin: Obtain the .jad and .cod files or .jar files for the BlackBerry Java Application from the application developer, vendor, or wireless service provider.

1. Create a web page that you can use to install the BlackBerry Java Application on BlackBerry devices.
2. Copy the application .jad and .cod files or .jar files to the web server that hosts the web page.

After you finish: Select a distribution method (for example, an email message or an intranet web page) that you can use to provide users with the web address for the web page that you created.

Install the BlackBerry Java Application using a web browser on the BlackBerry device

Send these instructions to users.

1. Open a web browser on the BlackBerry device.
2. Navigate to the web address that your administrator provided you with.
3. Click **Download**.

Configuring how users access enterprise applications and web content

14

Specifying a BlackBerry MDS Connection Service as a central push server

At least one BlackBerry MDS Connection Service in your organization's BlackBerry Domain must act as a central push server. Central push servers receive content push requests from server-side applications that are located on an application server or on a web server. Central push servers also manage push requests and send application data and application updates to BlackBerry device applications.

If a BlackBerry Domain includes one BlackBerry MDS Connection Service that is version 5.0 or later, by default, that BlackBerry MDS Connection Service is the central push server. If two BlackBerry MDS Connection Service instances that are version 5.0 or later exist in a BlackBerry Domain, by default, both instances are central push servers. If more than two BlackBerry MDS Connection Service instances (that are version 5.0 or later) exist in a BlackBerry Domain, the first two instances that start are central push servers. You can configure any BlackBerry MDS Connection Service in your organization's BlackBerry Domain to act as a central push server. If a BlackBerry MDS Connection Service in your organization's environment is earlier than version 5.0, it is not designated as a central push server automatically when it starts.

Related information

Configure multiple BlackBerry Enterprise Server instances to use the same BlackBerry MDS Connection Service, 79

Specify a BlackBerry MDS Connection Service as a central push server

You can specify more than one BlackBerry MDS Connection Service in your organization's BlackBerry Domain as a central push server. By default, if one or two BlackBerry MDS Connection Service instances exist in the BlackBerry Domain, those instances are central push servers.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. In the **General** section, in the **Is centralized push server** drop-down list, click **Yes**.
5. Click **Save all**.

After you finish:

- Notify the push application developers in your organization's environment that you have specified a new central push server.

Configuring how BlackBerry devices authenticate to content servers

If you configured the content servers in your organization's environment to use an authentication protocol to authenticate the sources of the data requests that they receive, you can control how BlackBerry devices authenticate to content servers to receive application data and application updates.

Configure how BlackBerry devices authenticate to content servers

You can configure whether BlackBerry devices authenticate to content servers directly, or whether the BlackBerry MDS Connection Service authenticates to content servers on behalf of BlackBerry devices. If you configure BlackBerry devices to authenticate directly to content servers but you do not configure an authentication method for BlackBerry MDS Connection Service connections, authenticated BlackBerry devices prompt users to provide login information every 60 minutes. The BlackBerry devices prompt users only if the connection to the content server persists for more than 60 minutes.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **HTTP** tab, in the **Protocol service information** section, in the **Authentication support enabled** drop-down list, perform one of the following actions:
   - If you want BlackBerry devices to authenticate to content servers directly, click **No**.
   - If you want the BlackBerry MDS Connection Service to store authentication information and perform HTTP authentication on behalf of BlackBerry devices, click **Yes**.
5. If necessary, in the **Authentication timeout** field, type the length of time, in milliseconds, that you want authentication information for BlackBerry devices to remain valid on the content server.

   By default, the authentication timeout limit is 1 hour.
6. Click **Save all**.

After you finish: If you set **Authentication support enabled** to **Yes**, configure the BlackBerry MDS Connection Service to authenticate to content servers that use NTLM, Kerberos, LTPA, or RSA Authentication Manager on behalf of BlackBerry devices.

Related information

Managing how users access enterprise applications and web content, 308

Configure the BlackBerry MDS Connection Service to authenticate BlackBerry devices to content servers that use NTLM

Before you begin: Configure the BlackBerry MDS Connection Service to authenticate to content servers on behalf of BlackBerry devices.

1. Navigate to <*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\MDS\Servers\Instance\config .
2. Configure the **MdsLogin.conf** file.

For more information about the Java Authentication and Authorization Service configuration file, visit http://java.sun.com/javase/6/docs/technotes/guides/security/jgss/tutorials/LoginConfigFile.html.

Configure the BlackBerry MDS Connection Service to authenticate BlackBerry devices to content servers that use Kerberos

Before you begin: Configure the BlackBerry MDS Connection Service to authenticate to content servers on behalf of BlackBerry devices.

1. Navigate to <*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\MDS\Servers\Instance\config .
2. Configure the **krb5.conf** file.

For more information about the Kerberos 5 configuration file, visit web.mit.edu/kerberos/www/krb5-1.3/krb5-1.3.3/doc/krb5-admin.html#krb5.conf.

Configure the BlackBerry MDS Connection Service to authenticate BlackBerry devices to content servers that use LTPA

BlackBerry devices that are running BlackBerry Device Software version 3.8 or later manage how HTTP cookies are stored and used to authenticate to content servers that use LTPA authentication technology. For BlackBerry devices that use previous versions of the BlackBerry Device Software, you must permit the BlackBerry MDS Connection Service to manage HTTP cookie storage on BlackBerry devices.

Before you begin: Configure the BlackBerry MDS Connection Service to authenticate to the content servers in your organization's environment on behalf of BlackBerry devices.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **HTTP** tab, in the **Protocol service information** section, in the **Cookie support enabled** drop-down list, click **Yes**.
5. Click **Save all**.

Configuring the BlackBerry MDS Connection Service to authenticate devices to the RSA Authentication Manager

You can configure the BlackBerry MDS Connection Service to require that BlackBerry device users pass RSA authentication when they access the Internet or intranet from BlackBerry devices. You can configure the BlackBerry MDS Connection Service to require that users use RSA authentication in one of the following scenarios:

- when users access every web site and intranet site from devices
- when users access intranet sites from devices
- when users access web addresses or intranet addresses that you specify

If you configure the BlackBerry MDS Connection Service to require that users use RSA authentication to access web addresses or intranet addresses that you specify, you can choose to apply this option to specific user accounts or to all user accounts that are associated with a BlackBerry Enterprise Server instance.

After the RSA Authentication Manager authenticates the devices, if you configured proxy authentication, the devices prompt users to authenticate to the proxy server.

Prerequisites: Configuring the BlackBerry MDS Connection Service to support RSA authentication when the BlackBerry MDS Connection Service runs on Windows Server 2008

- If required, remove the RSA Authentication Agent from the computer that hosts the BlackBerry MDS Connection Service.
- If required, in the RSA Authentication Manager, delete the node secret data for the computer that hosts the BlackBerry MDS Connection Service.
- If required, delete the node secret data that is located on the computer that hosts the BlackBerry MDS Connection Service.
- Retrieve the RSA Authentication API version 5.0.3.2 from RSA.

Configure the BlackBerry MDS Connection Service to support RSA authentication when the BlackBerry MDS Connection Service runs on Windows Server 2008

1. On the computer that hosts the BlackBerry MDS Connection Service, copy the **aceclnt.dll** file and **sdmsg.dll** file from the RSA Authentication API to one of the following folders:
    - If you are running a 32-bit version of Windows Server 2008, the <*drive*>:\WINDOWS\system32 folder

- If you are running a 64-bit version of Windows Server 2008, the <*drive*>:\WINDOWS\SysWow64 folder

2. In the RSA Authentication Manager, create an Agent Host record for the BlackBerry Enterprise Server. The RSA Authentication Manager generates an **sdconf.rec** file.
3. On the computer that hosts the BlackBerry MDS Connection Service, copy the **sdconf.rec** file that the RSA Authentication Manager generates to one of the following folders:
    - If you are running a 32-bit version of Windows Server 2008, the <*drive*>:\WINDOWS\system32 folder
    - If you are running a 64-bit version of Windows Server 2008, the <*drive*>:\WINDOWS\SysWow64 folder
4. In the Windows Services, restart the BlackBerry MDS Connection Service.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configure the BlackBerry MDS Connection Service to authenticate devices to the RSA Authentication Manager

Before you begin:

- Configure the BlackBerry MDS Connection Service to authenticate to the content servers in your organization's environment on behalf of BlackBerry devices.
- To specify the web addresses that require RSA authentication, configure URL patterns and access control rules that restrict user access to specific web addresses or intranet addresses.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **RSA** tab, in the **Protocol service information** section, in the **RSA® authentication support** drop-down list, select one of the following options:
    - If you want users to use RSA authentication when they access every web address or intranet address, select **Turn on globally**.
    - If you want users to use RSA authentication when they access the intranet only, select **Turn on for Intranet only**.
    - If you want users to use RSA authentication for web addresses or intranet addresses that you specify, select **Turn on for specific sites only**.
5. In the **RSA authentication timeout** field, type a number, in minutes, to specify how long devices that the RSA Authentication Manager authenticates can remain connected to your organization's network while the users are active.

    By default, the authenticated connection persists for 24 hours.

6. In the **RSA inactivity timeout** field, type a number, in minutes, to specify how long devices can remain connected to your organization's network while the users are inactive.

   By default, an authenticated connection persists for 60 minutes of user inactivity on the devices.

7. Click **Save all**.

Related information

Restarting BlackBerry Enterprise Server components, 392

Managing how users access enterprise applications and web content, 308

Configuring how the BlackBerry MDS Connection Service manages requests for web content

The BlackBerry MDS Connection Service manages requests for web content from the BlackBerry Browser and other applications on BlackBerry devices. You can configure how the BlackBerry MDS Connection Service manages these requests.

Configure the BlackBerry MDS Connection Service to manage HTTP cookie storage

By default, the BlackBerry MDS Connection Service does not manage HTTP cookie storage for BlackBerry devices. If the BlackBerry device requires JavaScript support for its HTTP requests, the BlackBerry device processes cookies.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **HTTP** tab, in the **Protocol service information** section, in the **Cookie support enabled** drop down list, click **Yes**.
5. Click **Save all**.

After you finish: To prevent the BlackBerry MDS Connection Service from managing HTTP cookie storage, change the **Cookie support enabled** drop-down list to **No**.

Configure the timeout limit for HTTP connections with BlackBerry devices

You can specify how long a BlackBerry MDS Connection Service waits for a BlackBerry device to send data to it before the BlackBerry MDS Connection Service closes the HTTP connection to the BlackBerry device. The default timeout limit is 120,000 milliseconds (2 minutes).

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **HTTP** tab, in the **Protocol service information** section, in the **Device connection timeout** field, type a number in milliseconds.
5. Click **Save all**.

Configure the timeout limit for HTTP connections with web servers

You can specify how long a BlackBerry MDS Connection Service waits for a web server to send data to it before the BlackBerry MDS Connection Service closes the HTTP connection to the web server. The default timeout limit is 120,000 milliseconds (2 minutes).

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **HTTP** tab, in the **Protocol service information** section, in the **Server connection timeout** field, type a number in milliseconds.
5. Click **Save all**.

Configure the maximum number of times that the BlackBerry Browser accepts HTTP redirections

HTTP redirection occurs when the BlackBerry Browser requests a web page from a web server and the web server redirects the request to a new web address for the page. The default limit is 5 redirections.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **HTTP** tab, in the **Protocol service information** section, in the **Maximum redirect connections** field, type a number.
5. Click **Save all**.

Permitting push applications to make trusted connections to a BlackBerry MDS Connection Service

To permit push applications to open trusted connections to a BlackBerry MDS Connection Service, you must create a key store (the webserver.keystore file) on the computer that hosts the BlackBerry MDS Connection Service. This key store permits the BlackBerry MDS Connection Service to accept HTTPS connections from push applications.

Push applications can use a BlackBerry MDS Connection Service certificate to open HTTPS connections to the BlackBerry MDS Connection Service to push application data and application updates to the BlackBerry devices that are assigned to that BlackBerry MDS Connection Service.

You can use the Java keytool to create a self-signed certificate for the BlackBerry MDS Connection Service, or you can import a signed certificate from a trusted public certification authority. You can use the Java keytool to export the BlackBerry MDS Connection Service certificate from the key store, and import the certificate to the key stores that the Java push applications use.

For more information about using the Java keytool, visit java.sun.com/javase/6/docs/technotes/tools/windows/keytool.html. For more information about the Apache Tomcat requirements, visit tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html.

Create a key store to store certificates for use with HTTPS connections

You must create a key store to store the certificates that permit the BlackBerry MDS Connection Service to accept HTTPS connections from push applications.

1. On the computer that hosts the BlackBerry MDS Connection Service, on the taskbar, click **Start** > **Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. On the **Mobile Data Service** tab, configure the key store information. Only one key store can exist. The file must be named webserver.keystore and it must be located at <*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\MDS\webserver .
3. Click **Create Keystore File**.
4. If prompted to overwrite a key store, click **Yes**.
5. Click **OK**.

Add a certificate for the BlackBerry MDS Connection Service

To permit server-side push applications to open trusted HTTPS connections to a BlackBerry MDS Connection Service and push application data and application updates to BlackBerry devices, you must add a certificate for the BlackBerry MDS Connection Service to the webserver.keystore file.

1. On the computer that hosts the BlackBerry MDS Connection Service, navigate to <*drive*>:\Program Files\Java \<*JRE_version*>\bin .
2. At the command prompt, perform one of the following tasks:

Task	Steps
Create a self-signed certificate for the BlackBerry MDS Connection Service and add it to the key store.	1. Type **keytool -genkey -alias tomcat -keyalg RSA -keystore webserver.keystore**. 2. Type the required information. 3. To confirm the information that you typed, type **Yes**.
Add a publicly signed certificate to the key store.	1. Type **keytool -import -trustcacerts -alias tomcat -file <*trustedserver.cer*> -keystore webserver.keystore**. 2. Type the key store password.

Task	Steps
	3. When prompted, click **Yes**.

3. Copy the key store file to <*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\MDS\webserver .

After you finish: Export the certificate for the BlackBerry MDS Connection Service to make it available to other applications.

Export the BlackBerry MDS Connection Service certificate to make it available to push applications

You must export the certificate for the BlackBerry MDS Connection Service so that you can import it to the key store of a server-side push application.

Before you begin: Add a self-signed or publicly signed certificate for the BlackBerry MDS Connection Service to the key store.

1. On the computer that hosts the BlackBerry MDS Connection Service, navigate to <*drive*>:\Program Files\Java \<*JRE_version*>\bin .
2. At the command prompt, type **keytool -export -alias tomcat -file <*server.cer*> -keystore <*drive*>:\Program Files \Research In Motion\BlackBerry Enterprise Server\MDS\webserver\webserver.keystore -storepass <*password*>** .
3. Type the key store password.

After you finish: Import the certificate for the BlackBerry MDS Connection Service to the key store of a push application.

Import the BlackBerry MDS Connection Service certificate to the key store of a push application

To permit a server-side push application to open trusted connections to the BlackBerry MDS Connection Service, you must add the certificate for the BlackBerry MDS Connection Service to the key store of the push application.

1. On the computer that hosts the BlackBerry MDS Connection Service, navigate to <*drive*>:\Program Files\Java \<*JRE_version*>\bin .
2. At a command prompt, type **keytool -import -trustcacerts -alias <*alias*> -file <*server.cer*> -keystore <*application_keystore*>** .
3. Type the key store password.
4. To add the certificate to the key store, at the prompt, type **Yes**.

After you finish: If the certificate does not exist, import the certificate to <*drive*>:\Program Files\Java\<*JRE version*>\lib \security\cacerts .

Permit push applications to select the transport protocol for PAP requests

By default, when a push application sends a PAP request to the BlackBerry MDS Connection Service, the BlackBerry MDS Connection Service directs requests to an HTTPS port. Because some applications require an HTTP port, you may want to change this default setting. You can configure the BlackBerry MDS Connection Service to permit the push application to select the transport protocol (HTTP or HTTPS) for PAP requests.

1. On the computer that hosts the BlackBerry MDS Connection Service, navigate to <*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\MDS\Servers\instance\config .
2. In a text editor, open the **rimpublic.properties** file.
3. In the **rimpublic.properties** file, on a new line, type **Delegate.push.initiator**=**true**.
4. Save and close the **rimpublic.properties** file.
5. Restart the BlackBerry MDS Connection Service.

Configuring a BlackBerry MDS Connection Service to trust web servers

You can configure the BlackBerry MDS Connection Service to permit BlackBerry devices to pull application data and updates from trusted or untrusted web servers. If you want to open trusted connections between web servers and the BlackBerry MDS Connection Service, you must import the certificate for the web server into the JRE certificates keystore file (JRE cacerts).

The BlackBerry MDS Connection Service supports LDAP, OCSP, and CRL to retrieve certificates and certificate status, and HTTPS and SSL/TLS for connections that use trusted certificates.

Specify whether the BlackBerry MDS Connection Service requires trusted HTTPS connections from web servers

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **HTTPS** tab, in the **Name** field, type the name of a web server.
5. In the **Service URL** field, type the regular expression for the web address of the web server. For example, type * to represent all web servers, or type **https://<*domain*>.com*** to specify all web servers in a specific domain.

   For more information about regular expressions in Java, visit java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html and java.sun.com/docs/books/tutorial/essential/regex/literals.html.
6. In the **Settings** section, in the **Allow untrusted servers** drop-down list, perform one of the following actions:
   - To permit only trusted HTTPS connections from the web server, click **No**.
   - To permit untrusted HTTPS connections from the web server, click **Yes**.
7. Click the **Add** icon.
8. Repeat steps 4 to 7 for each web server that you want to specify.
9. Click **Save all**.

After you finish: Restart the BlackBerry MDS Connection Service.

Related information

Add a retrieved certificate for a web server to the key store, 200

Restarting BlackBerry Enterprise Server components, 392

Specify whether the BlackBerry MDS Connection Service requires trusted TLS connections from web servers

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.

2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **TLS** tab, in the **Name** field, type the name of a web server.
5. In the **Service URL** field, type the regular expression for the web address of the web server.
6. In the **Settings** section, in the **Allow untrusted servers** drop-down list, perform one of the following actions:
   - To permit only trusted TLS connections from the web server, click **No**.
   - To permit untrusted TLS connections from the web server, click **Yes**.
7. Click the **Add** icon.
8. Repeat steps 4 to 7 for each web server that you want to specify.
9. Click **Save all**.

After you finish: Restart the BlackBerry MDS Connection Service.

Related information

Add a retrieved certificate for a web server to the key store, 200
Restarting BlackBerry Enterprise Server components, 392

Configuring certificate server information for the BlackBerry MDS Connection Service

The certificate for the BlackBerry MDS Connection Service permits push applications to make HTTPS connection to the BlackBerry MDS Connection Service. You can configure the BlackBerry MDS Connection Service to search for and retrieve certificates and the status of the certificates that external web servers use to make HTTPS connections.

To search for and retrieve certificates from an LDAP server, you can configure the BlackBerry MDS Connection Service to use LDAP or DSML. The BlackBerry MDS Connection Service searches each LDAP server using LDAP or DSML in the order that you specify. If you configure the BlackBerry MDS Connection Service to use both LDAP and DSML to search and retrieve certificates, the BlackBerry MDS Connection Service searches the servers using LDAP and then searches the servers using DSML. After the BlackBerry MDS Connection Service retrieves the certificate, the BlackBerry Enterprise Server sends the certificate to the BlackBerry device, and the BlackBerry device displays the certificate so that the user can accept it. The BlackBerry MDS Connection Service supports DSML version 2.

To search for and retrieve the status of the certificates, you can configure the BlackBerry MDS Connection Service to search the OCSP servers or CRL servers. If you search for the status of the certificates using an OCSP server or a CRL server, which server you choose to search for the status of the certificates first does not matter because each server creates a prioritized list automatically.

For more information about certificates, see the *BlackBerry Enterprise Solution Security Technical Overview*.

Configure the LDAP servers that the BlackBerry MDS Connection Service uses to retrieve certificates

You can create a user name and password so that the BlackBerry MDS Connection Service can authenticate to LDAP servers on behalf of BlackBerry devices.

If you change the LDAP port number or host server information, you must stop and restart the BlackBerry MDS Connection Service so that the BlackBerry MDS Connection Service can use the new port number or host server information immediately.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. On the **LDAP** tab, click **Edit component**.
4. Perform one of the following tasks:

Task	Steps
Create an LDAP server configuration.	1. In the **Name** field, type the LDAP server name. 2. In the **Service URL** field, type the web address for the server. 3. In the **Settings** section, configure the LDAP server settings. 4. Click the **Add** icon.
Change an existing LDAP server configuration.	1. Click the **Edit** icon beside the LDAP server. 2. In the **Settings** section, change the LDAP server settings. 3. Click the **Update** icon.

5. Click **Save all**.

After you finish:

- To configure the BlackBerry MDS Connection Service to retrieve the status of certificates, configure the OCSP and CRL server information.
- Add the communication information that you configured for the LDAP server to the BlackBerry MDS Connection Service configuration set.

Related information

Add communication information to a BlackBerry MDS Connection Service configuration set, 198
Assign a BlackBerry MDS Connection Service configuration set to a BlackBerry MDS Connection Service instance, 199
Restarting BlackBerry Enterprise Server components, 392

LDAP server settings

Field	Description
Base Query	This field specifies the base query for the default LDAP server. You can use %20 for spaces. Each LDAP server can host multiple Windows domains but can search in only one Windows domain at a time. You might need to configure a default base query for some LDAP servers.
Password and Confirm Password	These fields specify a password if the LDAP server requires simple authentication.
Query Limit	This field specifies the maximum number of entries that you want to return for each query.
Service URL	This field specifies the FQDN and port number of the LDAP server. You must use the <*FQDN*>:<*Port*> format.
User name	This field specifies the user name if the LDAP server requires simple authentication.

Configure the BlackBerry MDS Connection Service to use DSML to retrieve certificates

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. On the **DSML** tab, click **Edit component**.
4. In the **Protocol service information** section, in the **Query limit** field, type the maximum number of certificates that the BlackBerry MDS Connection Service can retrieve during each search it performs.
5. Perform one of the following tasks:

Task	Steps
Create a configuration for a DSML certificate server.	1. In the **Name** field, type a name for the DSML certificate server that you want the BlackBerry MDS Connection Service to search. 2. In the **Service URL** field, type the FQDN of the DSML certificate server (for example, http://server01.rim.com:1234/dsml/adssoap.dsmlx). 3. In the **Settings** section, if you do not want the BlackBerry MDS Connection Service to search the entire directory tree, in the **Base query** field, type the search base that the BlackBerry MDS Connection Service can use.

Task	Steps
	4. To permit the BlackBerry MDS Connection Service to authenticate with the DSML certificate server on behalf of BlackBerry devices, in the **User name** field, type the user name that the BlackBerry MDS Connection Service can use to authenticate with the DSML certificate server. 5. In the **Password** and **Confirm password** fields, type the password for the user name that the BlackBerry MDS Connection Service can use to authenticate with the DSML certificate server. 6. Click the **Add** icon.
Change a configuration for an existing DSML certificate server configuration.	1. Click the **Edit** icon that is beside the DSML certificate server that you want to change. 2. In the **Settings** section, change the DSML certificate server settings. 3. Click the **Update** icon.

6. Click **Save all**.

After you finish:

- To configure the BlackBerry MDS Connection Service to retrieve the status of certificates from an OCSP server or CRL server, you must configure the OCSP server and CRL server information.
- Add the communication information that you configured for the DSML server to the BlackBerry MDS Connection Service configuration set.

Related information

Assign a BlackBerry MDS Connection Service configuration set to a BlackBerry MDS Connection Service instance, 199
Add communication information to a BlackBerry MDS Connection Service configuration set, 198
Restarting BlackBerry Enterprise Server components, 392

Configure the OCSP servers that the BlackBerry MDS Connection Service uses to retrieve the status of certificates

You can configure the BlackBerry MDS Connection Service to authenticate to OCSP servers on behalf of BlackBerry devices and to retrieve the status of certificates.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. On the **OCSP** tab, click **Edit component**.
4. Perform the following actions:
    - Configure the BlackBerry MDS Connection Service to accept OCSP servers that BlackBerry devices specify.

- Configure the OCSP handler to use the OCSP responder extension in a certificate.

5. Perform one of the following tasks:

Task	Steps
Create an OCSP server configuration.	1. In the **Name** field, type the OCSP server name. 2. In the **Service URL** field, type the web address for the server. 3. Click the **Add** icon.
Change an existing OCSP server configuration.	1. Click the **Edit** icon that is beside the OCSP server that you want to change. 2. In the **Settings** section, change the OCSP server settings. 3. Click the **Update** icon.

6. Click **Save all**.

After you finish: Add the communication information that you configured for the OCSP server to the BlackBerry MDS Connection Service configuration set.

Related information

Add communication information to a BlackBerry MDS Connection Service configuration set, 198
Assign a BlackBerry MDS Connection Service configuration set to a BlackBerry MDS Connection Service instance, 199
Restarting BlackBerry Enterprise Server components, 392

Configure the CRL servers that the BlackBerry MDS Connection Service uses to retrieve the status of certificates

You can configure the BlackBerry MDS Connection Service to authenticate to CRL servers on behalf of BlackBerry devices and to retrieve the status of certificates.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. On the **CRL** tab, click **Edit component**.
4. In the **CRL Service information** section, perform the following actions:

   - Configure the BlackBerry MDS Connection Service to accept CRL servers that BlackBerry devices specify.
   - Configure the CRL handler to use the CRL responder extension in a certificate.

5. Perform one of the following tasks:

Task	Steps
Create a CRL server configuration.	1. Type the CRL server name and the web address for the server. 2. Click the **Add** icon.
Change an existing CRL server configuration.	1. Click the **Edit** icon beside the CRL server. 2. Click the **Accept** icon.

6. Click **Save all**.

After you finish: Add the communication information that you configured for the CRL server to the BlackBerry MDS Connection Service configuration set.

Related information

Add communication information to a BlackBerry MDS Connection Service configuration set, 198
Assign a BlackBerry MDS Connection Service configuration set to a BlackBerry MDS Connection Service instance, 199
Restarting BlackBerry Enterprise Server components, 392

Add communication information to a BlackBerry MDS Connection Service configuration set

A BlackBerry MDS Connection Service configuration set is a set of service configurations that the BlackBerry MDS Connection Service instances in your organization can use to communicate with a remote file system, an LDAP server, a DSML server, a CRL server, an OCSP server, or a certification authority. You must add the communication information that the BlackBerry MDS Connection Service requires to communicate with servers to a configuration set so that a BlackBerry MDS Connection Service instance can communicate with the servers after you assign the configuration set to the instance.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **Configuration Sets** tab, perform one of the following actions:
    - To create a configuration set, in the **Configuration set name** section, type a name and description for the configuration set.
    - To change an existing configuration set, click the **Edit** icon.
5. In the **Priority Service group** drop-down list, click the name of the service that you want to configure the communication method for.
6. In the **Service (Name : Description)** drop-down list, click the name of the communication method that you want to configure.
7. Click the **Add** icon.

8. To specify the communication method that the BlackBerry MDS Connection Service should try to connect to the server with first , click the **Up** and **Down** arrows. The BlackBerry MDS Connection Service resolves conflicts by applying communication methods in the order that you specify. The order of that you specify for LDAP, DSML, or file communication applies to each communication method separately. The order permits the BlackBerry MDS Connection Service to resolve conflicts between domains if you created multiple communication methods for a specific URL.
9. Perform one of the following actions:
    - To add a new configuration set, click the **Add** icon.
    - To update an existing configuration set, click the **Update** icon.
10. Click **Save all**.

After you finish:

- To confirm your changes, click the **View** icon.
- Assign the configuration set to a BlackBerry MDS Connection Service.

Assign a BlackBerry MDS Connection Service configuration set to a BlackBerry MDS Connection Service instance

You can assign a BlackBerry MDS Connection Service configuration set to a BlackBerry MDS Connection Service instance so that BlackBerry device users can access documents on remote file systems from devices, the BlackBerry MDS Connection Service can search for certificates and check for the status of the certificates from LDAP servers, DSML servers, CRL servers, or OCSP servers, and the BlackBerry MDS Connection Service can send certificate requests to a certificate authority.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click the instance that you want to change.
4. Click **Edit instance**.
5. On the **Component Configuration Sets** tab, in the **Available component configuration sets** section, in the **Service configuration sets** drop-down list, click the configuration set that you want to assign to the BlackBerry MDS Connection Service instance.
6. Click **Save all**.
7. To restart the BlackBerry MDS Connection Service instance, on the **Instance information** tab, in the **Status** list, click **Restart instance**.
8. To assign the BlackBerry MDS Connection Service configuration set to another BlackBerry MDS Connection Service instance, repeat steps 3 to 7.

Related information

Restarting BlackBerry Enterprise Server components, 392

Add a retrieved certificate for a web server to the key store

You can use the Java keytool to add a certificate for a web server to the BlackBerry MDS Connection Service key store. The certificate permits the BlackBerry MDS Connection Service to connect to the trusted web server.

1. Save the certificate from a secure web site to a .cer file.
2. On the computer that hosts the BlackBerry MDS Connection Service, copy the .cer file to <*drive*>:\Program Files\Java\<*JRE_version*>\lib\security .
3. At a command prompt, navigate to <*drive*>:\Program Files\Java\<*JRE_version*>\bin .
4. Type **keytool -import -trustcacerts -alias** <***alias_name***> **-file** <***cert_filename***> **-keystore ..\lib\security\cacerts** .
5. Type the key store password.
6. To add the certificate to the key store, at the command prompt, type **Yes**.

After you finish: For more information about using the Java keytool, visit java.sun.com/javase/6/docs/technotes/tools/windows/keytool.html.

Permitting users to access intranet sites on BlackBerry devices using global login information

To permit users to access intranet sites on BlackBerry devices without having to specify their user names and passwords, you can configure a global user name and password. When users try to access an intranet site, the BlackBerry MDS Connection Service checks to see if you configured global login information, and validates the login information. If authentication succeeds, users can access intranet sites without providing their user names and passwords. If authentication fails, users must type their user names and passwords before they can access intranet sites.

Configure global login information for intranet site access

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. On the **HTTP** tab, click **Edit component**.
4. In the **Protocol service information** section, in the **Authentication support enabled** drop-down list, click **Yes**.
5. In the **Name** section, type a global name, and type the web address of the intranet site in the **Service URL** section.
6. In the **Settings** section, type a user name and password.
7. Click **Save all**.

Configuring how the BlackBerry MDS Connection Service connects to BlackBerry devices

Specify the maximum amount of data that a BlackBerry MDS Connection Service can send to BlackBerry devices

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **General** tab, in the **Flow control** section, in the **Maximum data amount permitted per connection** field, type a number, in KB.

5. Click **Save all**.

Specify the pending content timeout limit for a BlackBerry MDS Connection Service

You can specify how long a BlackBerry MDS Connection Service waits for acknowledgment from a BlackBerry device before it deletes pending content for the BlackBerry device.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to specify the content timeout limit for.
3. Click **Edit instance**.
4. On the **General** tab, in the **Flow control** section, in the **Flow control timeout** field, type a number, in milliseconds.
5. Click **Save all**.

Permit Java applications to use scalable socket connections with a BlackBerry MDS Connection Service

Before you begin: Verify that your system memory supports scalable socket connections.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to permit scalable socket connections on.
3. Click **Edit instance**.
4. On the **General** tab, in the **Socket connection settings** section, in the **Use scalable sockets** options list, click **Yes**.
5. Click **Save all**.

Specify the thread pool size of a BlackBerry MDS Connection Service

You can specify the maximum number of threads that a BlackBerry MDS Connection Service can process at the same time.

Before you begin: Verify that your system memory can support the thread pool size that you want to specify.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to specify the thread pool size for.
3. Click **Edit instance**.
4. On the **General** tab, in the **Socket connection settings** section, in the **Thread pool size** field, type a number between 100 and 1000.
5. Click **Save all**.

Specify the maximum number of scalable socket connections

You can specify the maximum number of scalable socket connections that can be open at the same time between BlackBerry devices and a BlackBerry MDS Connection Service.

Before you begin: Verify that your system memory can support the number of scalable socket connections that you want to specify.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to specify the maximum number of scalable socket connections for.
3. Click **Edit instance**.
4. On the **General** tab, in the **Socket connection settings** section, in the **Use scalable sockets** options, select the **Yes** option.
5. In the **Maximum simultaneous scalable sockets** field, type a number between 100 and 3500.

   By default, the maximum number of scalable socket connections is 2000.
6. Click **Save all**.

Prevent the BlackBerry MDS Connection Service from using scalable HTTP

By default, the BlackBerry MDS Connection Service 5.0 SP2 or later uses scalable HTTP, which permits the BlackBerry MDS Connection Service to use fewer system resources and to establish more socket connections at one time than previous versions of the BlackBerry MDS Connection Service. When a BlackBerry MDS Connection Service uses scalable HTTP, it streams data to and from BlackBerry devices instead of storing and forwarding the data. If you want a BlackBerry

MDS Connection Service to process data as it did in previous versions of the BlackBerry Enterprise Server, you can prevent a BlackBerry MDS Connection Service from using scalable HTTP.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to prevent from using scalable HTTP.
3. Click **Edit instance**.
4. On the **General** tab, in the **Socket connection settings** section, in the **Use scalable HTTP** drop-down list, click **No**.
5. Click **Save all**.

Specify the port number that the web server listens on for push application requests

You can specify the port number that the web server listens on for HTTP requests and HTTPS requests from server-side push applications. You should change the default port parameters only if a port conflict exists with another service on the same computer.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to specify the port number for.
3. Click **Edit instance**.
4. On the **General** tab, in the **Connection** section, perform one of the following actions:
   - To specify the port for HTTP requests, in the **Web server listen port** field, type the port number.
   - To specify the port for HTTPS requests, in the **Web server SSL listen port** field, type the port number.
5. Click **Save all**.

After you finish:

- Restart the BlackBerry MDS Connection Service.
- Notify your organization's push application developers that you changed the port number that the web server listens on for push application requests.

Related information

Restarting BlackBerry Enterprise Server components, 392

Specify how often a BlackBerry MDS Connection Service polls for configuration information

You can specify how often a BlackBerry MDS Connection Service polls the BlackBerry Configuration Database for changes to the administration settings for the BlackBerry MDS Connection Service and BlackBerry Collaboration Service. The default interval is 5 minutes.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want change.
3. Click **Edit instance**.
4. On the **General** tab, in the **Database** section, in the **Database admin configuration cycle timer** field, type a time, in minutes.
5. Click **Save all**.

Setting up the messaging environment

15

Creating email message filters

You can create email message filters to define which email messages the BlackBerry Enterprise Server forwards from users' email applications to their BlackBerry devices. When users receive email messages in the incoming message queue, the BlackBerry Enterprise Server applies email message filters to determine how to direct the messages: forward, forward with priority, or do not forward to the BlackBerry devices.

Email message filters that you create and apply override the email message filters that users create using the BlackBerry Desktop Manager, the BlackBerry Web Desktop Manager, or their BlackBerry devices. You can specify the order that the BlackBerry Messaging Agent applies the email message filters in.

You can create the following types of email message filters:

- global filters: apply to all users on the BlackBerry Enterprise Server
- user filters: apply to specific users on the BlackBerry Enterprise Server

Users cannot view or change global filters. If you define global filters, you must explain to users that some of the email message filters that they created might not apply to incoming messages.

If you change global filters, the BlackBerry Enterprise Server applies the changes immediately.

Create an email message filter that applies to all user accounts on a BlackBerry Enterprise Server

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Email message filters** tab, in the **Email message filter name** field, type a name for the email message filter.

5. In the **Email message filter rules** section, configure the options for the email message filter. Use semicolons (;) to separate multiple items that you specify.

   If you specify multiple users in the **From** or **Sent to** fields, or multiple subject terms in the **Subject** field, the message filter is applied to email messages that contain any of the users or terms that you specify. All of the users or terms that you specify do not have to be satisfied for the message filter to be applied.

6. Perform one of the following tasks:

   - To create an email message filter that does not deliver email messages that match the filter criteria to BlackBerry devices, select **Do not forward email messages to the device**.
   - To create an email message filter that forwards email messages that match the filter criteria to BlackBerry devices, select **Forward email messages to the device**.

7. Click the **Add** icon.
8. To move the email message filter higher or lower in the list, click the **Up** or **Down** icons.
   The BlackBerry Enterprise Server applies email message filters in the order that they are listed in. Organize the email message filters from the least restrictive to the most restrictive.
9. Repeat steps 4 to 8 for each email message filter that you want to add.
10. Click **Save all**.

Turn on an email message filter that applies to all user accounts on a BlackBerry Enterprise Server

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Email message filters** tab, click the **Edit** icon beside the email message filter you want to turn on.
5. In the **Enabled** drop down list, click **Yes**.
6. Click **Save all**.
   The BlackBerry Administration Service applies email message filters in the order that they are listed in.

Create an email message filter that applies to a specific user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.

2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Email** tab, in the **Email message filter name** field, type a name for the email message filter.
8. In the **Email message filter rules** section, configure the options for the email message filter. Use semicolons (;) to separate multiple items that you specify.

   If you specify multiple users in the **From** or **Sent to** fields, or multiple subject terms in the **Subject** field, the message filter is applied to email messages that contain any of the users or terms that you specify. All of the users or terms that you specify do not have to be satisfied for the message filter to be applied.
9. Perform one of the following tasks:
   - To create an email message filter that does not deliver email messages that match the filter criteria to BlackBerry devices, select **Do not forward email messages to the device**.
   - To create an email message filter that forwards email messages that match the filter criteria to BlackBerry devices, select **Forward email messages to the device**.
10. Click the **Add** icon.
11. To move the email message filter higher or lower in the list, click the **Up** or **Down** icons.
    The BlackBerry Enterprise Server applies email message filters in the order that they are listed in. Organize the email message filters from the least restrictive to the most restrictive.
12. Click **Continue to user information edit**.
13. Click **Save all**.

Turn on an email message filter that applies to a specific user account

1. In the BlackBerry Administration Service, in the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Email** tab, click the **Edit** icon beside the email message filter that you want to turn on.

8. In the **Enabled** drop-down list, click **Yes**.
9. Click **Continue to user information edit**.
10. Click **Save all**.
The BlackBerry Administration Service applies email message filters in the order that they are listed in.

Copying existing email message filters to another BlackBerry Enterprise Server

You can copy the existing email message filters for a BlackBerry Enterprise Server and apply them to other instances of the BlackBerry Enterprise Server. To create a copy of existing email message filters, you can export the existing email message filters for a BlackBerry Enterprise Server as an .xml file. You can then import the .xml file so that you can use it with another instance of the BlackBerry Enterprise Server.

Export email message filters for a BlackBerry Enterprise Server

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. On the **Email message filters** tab, click **Export email message filters**.
4. Click **Download file**.
5. Save the .xml file.

Import email message filters for a BlackBerry Enterprise Server

Before you begin: Export email message filters for a BlackBerry Enterprise Server.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.

4. On the **Email message filters** tab, click **Import email message filters**.
5. In the **Import email message filters** section, click **Browse**. Navigate to the .xml file that contains the email message filters that you want to import.
6. Click **Import email message filters**.
7. Click **Save all**.

Copying existing email message filters to user accounts

You can copy the existing email message filters for a user account and apply them to other user accounts. To create a copy of existing email message filters, you must export the existing email message filters for a user account as an .xml file. You can then import the .xml file so that you can use it with other user accounts.

Export email message filters for a user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. In the **Messaging configuration** section, click **Default configuration**.
6. On the **Email** tab, click **Export email message filters**.
7. Click **Download file**.
8. Save the .xml file.

Import email message filters for a user account

Before you begin: Export email message filters for a user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for the user account.

4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Email** tab, at the bottom of the screen, click **Import email filters**.
8. In the **Import email message filters** section, click **Browse**. Navigate to the .xml file that contains the email message filters that you want to import.
9. Click **Import email message filters**.
10. Click **Continue to user information edit**.
11. Click **Save all**.

Extension plug-ins for processing messages

You can add extension plug-ins to a BlackBerry Messaging Agent. The BlackBerry Messaging Agent uses extension plug-ins to process and make changes to email messages and attachments that the BlackBerry Messaging Agent sends to and receives from BlackBerry devices. For example, you can add an extension plug-in to modify the signature in email messages.

Before you add an extension plug-in to the BlackBerry Administration Service, you must install the extension plug-in application on the computer the hosts the BlackBerry Enterprise Server. By default, each BlackBerry Messaging Agent in your organization's BlackBerry Domain includes the extension plug-in BBAttachBESExtension, which connects the BlackBerry Messaging Agent to the BlackBerry Attachment Service so that the BlackBerry Attachment Service can process email message attachments. If you add multiple extension plug-ins to a BlackBerry Messaging Agent, you can define the order that the BlackBerry Messaging Agent uses the extension plug-ins to process email messages in.

Install an extension plug-in application

To add an extension plug-in to the BlackBerry Administration Service, you must first install the application for the extension plug-in on the computer that hosts the BlackBerry Enterprise Server.

Before you begin: Copy the .dll file for the extension plug-in application to the computer that hosts the BlackBerry Enterprise Server.

1. On the computer that hosts the BlackBerry Enterprise Server, on the **Start** menu, click **Run**.
2. Type **regedit**.
3. Click **OK**.
4. Perform one of the following actions:

- If you are running a 32-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\Research In Motion \BlackBerry Enterprise Server\Agents.
- If you are running a 64-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\WOW6432Node \Research In Motion\BlackBerry Enterprise Server\Agents.

5. If necessary, create a DWORD value named **PlugIns**.
6. Double-click the **PlugIns** DWORD value.
7. In the **Value data** field, type **Name=<*DLL_Name*> Data=<*DLL_Path*>** , where <*DLL_Name*> is a descriptive name of the .dll file and <*DLL_Path*> is the full path and file name for the .dll file.
8. Click **OK**.

After you finish:

- Restart the BlackBerry Enterprise Server.
- Add the extension plug-in to a BlackBerry Messaging Agent.

Related information

Restarting BlackBerry Enterprise Server components, 392

Add an extension plug-in to a BlackBerry Messaging Agent

Before you begin: Install an extension plug-in application on the computer that hosts the BlackBerry Enterprise Server.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Extension plug-ins** tab, in the **Extension plug-in name** field, type the name of the extension plug-in that you want to add.
5. Click the **Add** icon.
6. Repeat steps 4 and 5 for each extension plug-in that you want to add.
7. If necessary, click the **Up** and **Down** icons to set the order that the BlackBerry Messaging Agent uses the extension plug-ins to process email messages in.
8. Click **Save all**.

Change how a BlackBerry Messaging Agent uses extension plug-ins

The BlackBerry Messaging Agent uses a BlackBerry Enterprise Server extension process to load extension plug-ins to process email messages. If you do not add an extension plug-in to the BlackBerry Administration Service, and you install the extension plug-in application on the computer that hosts the BlackBerry Enterprise Server, the extension plug-in is loaded directly by the BlackBerry Messaging Agent instead of the extension process. To stabilize and manage your organization's messaging environment, you can change how the BlackBerry Controller starts extension processes. For example, you can configure the BlackBerry Controller to start one extension process for all extension plug-ins, or you can configure the BlackBerry Controller to start separate extension processes for each extension-plug in.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Extension plug-ins** tab, in the **Extension mode** section, in the **Extension mode** drop-down list, perform one of the following actions:
   - To configure the BlackBerry Controller to start a single extension process that loads all extension plug-ins for all BlackBerry Messaging Agent instances, click **single**.
   - To configure the BlackBerry Controller to start a dedicated extension process for each BlackBerry Messaging Agent instance, click **perAgent**.
   - To configure the BlackBerry Controller to start a dedicated extension process that loads each extension plug-in, click **perExtension**. Each BlackBerry Messaging Agent uses the same extension process to process a specific extension plug-in.
   - To configure the BlackBerry Controller to start a dedicated extension process for each extension plug-in for each BlackBerry Messaging Agent, click **perAgentperExtension**.
5. Click **Save all**.

Mapping contact information fields for synchronization and contact lookups

You can map contact information fields from the email applications on users' computers to the contact list fields on the BlackBerry devices. The information in the fields in the email applications synchronizes to the fields on the BlackBerry devices. You can create the following types of field mappings on the BlackBerry Enterprise Server:

- global field mappings: apply to all user accounts in a BlackBerry Domain
- user field mappings: apply to specific user accounts

You can map up to four fields that users define in the contact information on their computers to their BlackBerry devices. When users request a remote contact lookup from the contact list, the fields that you configure display on BlackBerry devices.

Map a contact information field in an email application to contact list fields on BlackBerry devices

1. In the BlackBerry Administration Service, on the **Servers and components menu**, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Synchronization**.
2. Click **Edit component**.
3. On the **Mappings for organizer data synchronization** tab, for each type of organizer data, select the option in the drop-down lists that you want to map the information to on BlackBerry devices.
4. Click **Save all**.

After you finish: To return the organizer data to the default settings, edit each mapping version by selecting the **Edit** icon, select **Reset to default** and select **Save all** after modifying each mapping version.

Map a contact list field in an email application to a contact list field on a BlackBerry device

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.

4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Mappings for organizer data synchronization** tab, in the **Mappings for organizer data synchronization** section, select the **Turned on** option.
8. In the appropriate drop-down lists, select the fields on the BlackBerry device that you want to map the information to.
9. Click **Continue to user information edit**.
10. Click **Save all**.

Map a contact information field in an email application to contact list fields on BlackBerry devices

You can map up to four contact list fields that users define in an email application to BlackBerry devices.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **Blackerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **Synchronization**.
3. Click **Edit component**.
4. On the **Mappings for organizer data synchronization** tab, in the **Other mappings** section, select each **User defined string** contact list field that you want to map to BlackBerry devices.
5. Click **Save all**.

After you finish: To return the organizer data to the default settings, edit each mapping version by selecting the **Edit** icon, select **Reset to default** and select **Save all** after modifying each mapping version.

Map a contact list field in an email application to a contact list field on a BlackBerry device

You can map up to four contact list fields that users define in an email application to a BlackBerry device.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.

6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Mappings for organizer data synchronization** tab, in the **Mappings for organizer data synchronization** section, select the **Turned on** option.
8. In the **Other mappings** section, in each **User defined string** drop-down list, select the contact field that you want to map to the BlackBerry device.
9. Click **Continue to user information edit**.
10. Click **Save all**.

Configuring BlackBerry devices to enroll certificates over the wireless network

16

You can configure the BlackBerry Enterprise Server to permit BlackBerry devices to enroll certificates that the devices can use with any PKI-enabled application or process. You can permit devices to enroll the certificates instead of instructing users to send the certificates to themselves in an email message or use the certificate synchronization tool in the BlackBerry Desktop Software. When you configure the BlackBerry Enterprise Server to permit devices to enroll certificates, you can control how users request certificates and which certification authority issues the certificates.

For example, you might want Wi-Fi enabled BlackBerry devices to enroll certificates so that they can authenticate to an enterprise Wi-Fi network.

You can enroll certificates from one of the following certification authorities:

- RSA certification authority
- Microsoft standalone certification authority
- Microsoft enterprise certification authority

During the enrollment process, the BlackBerry MDS Connection Service can verify the certificate if the certificate includes an email address in the subject DN. The BlackBerry MDS Connection Service verifies the certificate by checking if the email address in the subject DN of the certificate matches the email address that is assigned to the device. For more information about the enrollment process, see the *BlackBerry Enterprise Solution Security Technical Overview*.

You can make the certificate enrollment process required so that devices automatically start the certificate enrollment process after the devices receive the updated IT policy from the BlackBerry Enterprise Server. If you do not make the certificate enrollment process required, you must instruct users to start the CA Profile Manager on the devices manually.

Configure the certificate information using IT policies

You must configure the certificate information that BlackBerry devices can use to create certificate requests so that the certificate enrollment process can occur.

If you configured the BlackBerry MDS Connection Service to retrieve the status of the certificates using an OCSP server or a CRL server and pull authorization is turned on, devices may not be able to enroll some certificates over the mobile network. The devices might not be able to enroll some certificates because, devices that initiate the request to the web addresses follow pull authorization rules that restrict access to some of the web addresses for OCSP servers and CRL servers.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. Click an IT policy.
4. Click **Edit IT policy**.
5. On the **Certificate Authority Profile** tab, change the appropriate values for the IT policy rules.
6. Click **Save All**.

After you finish: For more information about the IT policy rules, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Related information
Assigning IT policies and resolving IT policy conflicts, 49

Configure the BlackBerry MDS Connection Service to connect to the certificate authority

If your organization's environment includes a Microsoft enterprise certification authority, the certification authority requires Windows authentication, and a certification authority administrator must approve certificate requests, you must configure the BlackBerry MDS Connection Service with the server name of the certification authority and the certification authority credentials so that the BlackBerry MDS Connection Service can send certificate requests to the certification authority.

Before you begin: Create a custom template on the certification authority that does not permit the subject name to originate from information in Microsoft Active Directory.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **HTTP** tab, in the **Name** field, type the certificate authority name.
5. In the **Service URL** field, type the URL that the BlackBerry MDS Connection Service can use to send certificate requests to the certification authority using the following format: http://<*FQDN_of_CA_server*>:<*port_number*>/* (for

example, http://myca.mycompany.com:80/*). Use <*port_number*>/* to make sure that the BlackBerry MDS Connection Service can access all the URLs for the certification authority.

6. In the **Settings** section, in the **User name** field, type the name of a certification authority administrator account that can approve certificate requests using one of the following formats: domain\username or domain@username.
7. In the **Password** and **Confirm password** fields, type the password for the certification authority administrator account.
8. Click the **Add** icon.
9. Click **Save all**.

After you finish:

- Write down the URL for the certification authority that you typed in the Service URL field. You must add the <*FQDN_of_CA_server*> that you configured in step 5 to the Certificate Authority Host IT policy rule, and the <*port_number*> that you configured in step 5 to the Certificate Authority Port IT policy rule.
- Add the certification authority information to a BlackBerry MDS Connection Service configuration set.

Add communication information to a BlackBerry MDS Connection Service configuration set

A BlackBerry MDS Connection Service configuration set is a set of service configurations that the BlackBerry MDS Connection Service instances in your organization can use to communicate with a remote file system, an LDAP server, a DSML server, a CRL server, an OCSP server, or a certification authority. You must add the communication information that the BlackBerry MDS Connection Service requires to communicate with servers to a configuration set so that a BlackBerry MDS Connection Service instance can communicate with the servers after you assign the configuration set to the instance.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **Configuration sets** tab, perform one of the following actions:
   - To create a configuration set, in the **Configuration set name** section, type a name and description for the configuration set. Click the **Add** icon.
   - To change an existing configuration set, click the **Edit** icon.
5. In the **Priority Service group** drop-down list, click the name of the service that you want to configure the communication method for.
6. In the **Service (Name : Description)** drop-down list, click the name of the communication method that you want to configure.

7. Click the **Add** icon.
8. To specify the communication method that the BlackBerry MDS Connection Service should try to connect to the server with first , click the **Up** and **Down** arrows. The BlackBerry MDS Connection Service resolves conflicts by applying communication methods in the order that you specify. The order of that you specify for LDAP, DSML, or file communication applies to each communication method separately. The order permits the BlackBerry MDS Connection Service to resolve conflicts between domains if you created multiple communication methods for a specific URL.
9. Perform one of the following actions:
   - To add a new configuration set, click the **Add** icon.
   - To update an existing configuration set, click the **Update** icon.
10. Click **Save all**.

After you finish:

- To confirm your changes, click the **View** icon.
- Assign the configuration set to a BlackBerry MDS Connection Service.

Assign a BlackBerry MDS Connection Service configuration set to a BlackBerry MDS Connection Service instance

You can assign a BlackBerry MDS Connection Service configuration set to a BlackBerry MDS Connection Service instance so that BlackBerry device users can access documents on remote file systems from devices, the BlackBerry MDS Connection Service can search for certificates and check for the status of the certificates from LDAP servers, DSML servers, CRL servers, or OCSP servers, and the BlackBerry MDS Connection Service can send certificate requests to a certificate authority.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Component configuration sets** tab, in the **Available component configuration sets** section, in the **Service configuration sets** drop-down list, click the configuration set that you want to assign to the BlackBerry MDS Connection Service instance.
5. Click **Save all**.
6. To restart the BlackBerry MDS Connection Service instance, on the **Instance information** tab, in the **Status** list, click **Restart instance**.

7. To assign the BlackBerry MDS Connection Service configuration set to another BlackBerry MDS Connection Service instance, repeat steps 3 to 7.

Add certificate information to a Wi-Fi profile

You must add the name of the certification authority profile that contains certificate information to a Wi-Fi profile. The name of the certification authority profile is required so that the certificate enrollment process can create a certificate that the BlackBerry device uses for Wi-Fi authentication. You can find the name of the certification authority profile in the Certificate Authority Profile Name IT policy rule.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to change.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, in the **Associated Certificate Authority Configuration** field, type the name of the certification authority profile.
6. Click **Save All**.

After you finish:

- Assign the Wi-Fi profile to a user account.
- Assign the IT policy that includes the certificate information to the user account.
- Send the IT policy to the device.

Managing an enrolled certificate

After a BlackBerry device enrolls a certificate, the CA Profile Manager monitors the certificate's expiry date and revocation status. When the expiry date approaches or the certification authority revokes the certificate, the CA Profile Manager generates a new public-private key pair, and starts the certificate enrollment process for a new certificate.

The certificate enrollment process can also start again if you change the following IT policy rules and resend the IT policy:

- Certificate Authority Profile Name
- Certificate Authority Type
- Certificate Authority Host
- Common Name Components

- Custom Microsoft Certificate Authority Certificate Template
- Distinguished Name Components
- Key Algorithm
- Key Length
- Microsoft Certificate Authority Certificate Template
- RSA Certificate Authority Certificate ID
- RSA Jurisdiction ID

A certificate enrollment process does not delete the existing certificate from the device key store or notify the certification authority that the certificate is no longer in use. The BlackBerry Enterprise Server deletes the existing certificate from the BlackBerry Configuration Database when the certificate enrollment process starts for a new certificate.

Also, if a certificate is expired or revoked, you or a BlackBerry device user can update the certificates on the device using the certificate synchronization tool in the BlackBerry Desktop Software or by copying an updated certificate from a media card or smart card.

For more information about deleting or revoking certificates, see the user guide for the device.

Change the polling interval, logging, and pool size for the BlackBerry MDS Connection Service connection to the certificate authority

You can turn on logging or change the polling interval and pool size for the BlackBerry MDS Connection Service connection to the certificate authority, as required by your organization's environment.

1. On the computer that hosts the BlackBerry MDS Connection Service, navigate to <*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\MDS\Servers\instance\config .
2. In a text editor, open the **rimpublic.properties** file.
3. In the **rimpublic.properties** file, type the appropriate properties and values.
4. Save and close the **rimpublic.properties** file.
5. In the Windows Services, restart the BlackBerry MDS Connection Service service.

Related information

Restarting BlackBerry Enterprise Server components, 392

Properties in the rimpublic.properties file

Property	Description
application.handler.pkcs10.pollinginterval	If the certificate authority requires a certificate administrator to approve certificate requests, this property specifies the interval, in minutes, that the BlackBerry MDS Connection Service waits before it requests an update about pending certificate requests from the certificate authority. The default interval is 60 minutes.
application.handler.pkcs10.poolsize	If the certificate authority requires a certificate administrator to approve certificate requests, this property specifies the maximum number of simultaneous worker threads that can manage pending certificate requests. The default pool size is 100 worker threads.
application.handler.pkcs10.logging	This property specifies whether to turn on logging for the PKCS#10 protocol service. The valid values are True and False. The PKCS#10 protocol service writes the log information to the MDAT log file. By default, logging is turned off.

Making the BlackBerry Web Desktop Manager available to users

17

Installing the client components of the BlackBerry Web Desktop Manager on users' computers

By default, when users open and log in to the BlackBerry Web Desktop Manager for the first time, the browser prompts them to accept a client authentication certificate and install the required RIMWebComponents.cab file. The RIMWebComponents.cab file provides the BlackBerry Device Manager and USB drivers that users require to use the BlackBerry Web Desktop Manager. To install the RIMWebComponents.cab file, users must log in to their computers as a local administrator.

If you use Microsoft Active Directory in your organization's environment, consider creating Windows GPOs to install the client components of the BlackBerry Web Desktop Manager on users' computers automatically. When you use Windows GPOs, the browser does not display the security warning or installation prompts to users, and users do not require local administrator permissions to complete the installation process.

Related information

Configuring the BlackBerry Web Desktop Manager, 230

Publish the client files for the BlackBerry Web Desktop Manager in a Windows GPO for Windows XP

If you use Microsoft Active Directory, you can create a Windows GPO to make sure that the browser settings are correct for your organization's environment. Alternatively, you can check the browser settings on users' computers and, if necessary, change them manually.

1. In the BlackBerry Enterprise Server installation files, navigate to tools/RIMWebComponents .
2. Copy the **RIMWebComponents.msi** file to a shared network folder.
3. In Microsoft Active Directory Users and Computers, right-click the organizational unit that you want to assign the Windows GPO to. Click **Properties**.
4. On the **Group Policy** tab, click **New**.
5. In the **Name** field, type a name for the new GPO.
6. In the list of GPOs, click the GPO name.
7. Click **Edit**.
8. In the **Group Policy Editor** menu, click **User Configuration** > **Software Settings**.
9. Right-click **Software Installation**. Click **New** > **Package**.
10. Type the UNC path and name of the **RIMWebComponents.msi**. The path must be typed in UNC format (for example, \\ComputerName\Applications\Testing).
11. Click **Open**.
12. In the **Deploy Software** window, click **Advanced**.
13. Click **OK**.
14. In the **Group Policy Object** properties window, on the **Deployment** tab, under **Deployment type**, click **Published**.
15. In the **Installation user interface options** menu, click **Basic**.
16. If the computer runs Windows Server 2003, perform the following actions:
    a. On the **Deployment** tab, click **Advanced**.
    b. Click **Include OLE class and product information**.
17. Click **OK**.

After you finish: Perform one of the following actions:

- On each user's computer that runs a 32-bit version of Windows, add the registry key HKEY_LOCAL_MACHINE\Software \Microsoft\WindowCurrentVersion\Internet Settings\UseCoInstall.
- On each user's computer that runs a 64-bit version of Windows, add the registry key HKEY_LOCAL_MACHINE\Software \WOW6432Node\Microsoft\WindowCurrentVersion\Internet Settings\UseCoInstall.

Publish the client files for the BlackBerry Web Desktop Manager in a Windows GPO for Windows Vista

Before you begin:

- Add the web address for the BlackBerry Administration Service to the list of trusted web sites in the web browser.
- Download and install the Microsoft Group Policy Management Console with Service Pack 1. For more information about installing the service pack, see www.microsoft.com.

1. Open the Microsoft Exchange Management Console.
2. Click **File** > **Add/Remove Snap-in**.
3. In the **Available Snap-ins** list, click **Group Policy Management**.
4. Click **Add.**
5. Click **OK.**
6. Expand **Group Policy Management** > **Forest**> **Domains**.
7. Click the domain name.
8. Right-click the organizational unit that you want to assign the Windows GPO to.
9. Click **Create a GPO in this domain, and link it here**.
10. In the **Name** field, type a name for the new GPO.
11. Click **OK**.
12. Right-click the GPO that you just created.
13. Click **Edit**.
14. On the **Computer Configuration** menu, click **Policies**.
15. Expand **Administrator Templates**.

16. Expand **Windows Components**.
17. Click **ActiveXInstaller Service**.
18. Right-click **Approved Installation Sites for ActiveX Controls**.
19. Select **Properties**.
20. On the **Settings** tab, click **Enabled**.
21. Click **Show**.
22. Click **Add**.
23. In the **Enter the name of the item to be added** field, type the web address for the BlackBerry Administration Service.
24. In the **Enter the value of the item to be added** field, type **2,2,1,0**.
25. In each dialogue box, click **OK**.

Configure the Microsoft ActiveX Installer on Windows Vista

1. On the computer that hosts the BlackBerry Web Desktop Manager, click **Start** > **Control Panel** > **Programs and Features**.
2. Click **Turn Windows Features On or Off**.
3. Select **ActiveX Installer Service**.
4. Click **OK**.

Configure users' computers to install the client file for the BlackBerry Web Desktop Manager automatically

You can create a new Windows GPO so that you can add the registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\UseCoInstall to users' computers. When you add the registry key, the users' computers install the RIMWebComponents.msi file and other Microsoft ActiveX controls automatically. The Windows GPO adds the registry key to computers in the organizational unit that you assigned the GPO to.

1. On the computer that hosts Microsoft Active Directory, in a new text file, copy and paste the following lines:

```
CLASS MACHINE
CATEGORY !!RegistrySettings
KEYNAME "Software\Microsoft\Windows\CurrentVersion\Internet Settings"
;KEYNAME "Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings"
POLICY !!EnableActiveXInstallFromAD
EXPLAIN !!EnableActiveXInstallFromAD_Explain
VALUENAME "UseCoInstall"
VALUEON NUMERIC 1
VALUEOFF NUMERIC 0
END POLICY
END CATEGORY
[strings]
EnableActiveXInstallFromAD="Allow user computers to install administrator-approved Microsoft ActiveX components."
EnableActiveXInstallFromAD_Explain="Allow user computers to install administrator-approved Microsoft ActiveX components."
RegistrySettings="Registry Settings"
```

2. Name the file **EnableActiveXInstallFromAD.adm** and save it.
3. In Microsoft Active Directory Users and Computers, right-click the organizational unit that you want to assign the Windows GPO to. Click **Properties**.
4. On the **Group Policy** tab, click **New**.
5. In the **Name** field, type a name for the new GPO.
6. In the list of GPOs, click the GPO name. Click **Edit**.
7. In the **Group Policy Object Editor** list, click **Computer Configuration** > **Administrative Templates**.
8. Right-click **Administrative Templates**. Perform one of the following actions:
   - If the computer uses Windows 2000 Server, clear the **View** – **Show Policies Only** option.
   - If the computer uses Windows Server 2003, click **View** – **Filtering**. Clear the **Only show policy settings that can be fully managed** check box.
9. Right-click **Administrative Templates**. Click **Add/Remove Templates**.
10. Add the EnableActiveXInstallFromAD.adm custom administrative template to the Windows GPO.
11. Click **Administrative Templates** > **Registry Settings**.
12. Double-click **Allow user computers to install administrator-approved Microsoft ActiveX components**.

13. Click **Enabled**.
14. Click **OK**.

After you finish: For more information about registry-based Windows GPOs, visit technet.microsoft.com to read *Using Administrative Template Files with Registry-Based Group Policy*.

Make the BlackBerry Web Desktop Manager available to users

The BlackBerry Web Desktop Manager web address is https://<*full_computer_name*> /webdesktop/login. If you customized the BlackBerry Web Desktop Manager text colors or image and you want to display the changes on the login screen, you must direct users to https://<*full_computer_name*>/webdesktop/app?page=Login&service=page&orgId=0.

Send users the following information:

- BlackBerry Web Desktop Manager web page address
- login information that you configured for the users in your messaging environment
- if necessary, the name of the domain that your messaging server is located in

Configuring the BlackBerry Web Desktop Manager

18

You can configure the BlackBerry Web Desktop Manager to permit users to perform administrative tasks such as creating a password for wireless activation, locking a lost or stolen BlackBerry device, deleting data from a device, or deactivating a device.

You can also customize the UI of the BlackBerry Web Desktop Manager by changing the text colors or displaying a custom image, such as your organization's logo, to match the design of your organization's intranet.

For more information about the IT policies that control the tasks that users can perform in the BlackBerry Web Desktop Manager, see the *BlackBerry Enterprise Server Policy Reference Guide* .

For more information about using the BlackBerry Web Desktop Manager to update the BlackBerry Device Software, see the *BlackBerry Device Software Update Guide* .

Permit users to perform administrative tasks using the BlackBerry Web Desktop Manager

You can permit users to perform the following administrative tasks using the BlackBerry Web Desktop Manager:

- specify an enterprise activation password for a BlackBerry device
- specify a new device password and lock a device
- delete all device data and deactivate a device
- assign a new device to a user account

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution Topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service**.
3. Click **Edit component**.
4. On the **BlackBerry Web Desktop Manager information** tab, change **Allow users to perform self service tasks** to **Yes**.
5. Click **Save all**.

Permit users to activate devices using the BlackBerry Web Desktop Manager

You can specify whether users can use the BlackBerry Web Desktop Manager to activate BlackBerry devices using a wired connection to a computer.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution Topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service**.
3. Click **Edit component**.
4. On the **BlackBerry Web Desktop Manager information** tab, perform one of the following actions:
   - To permit users to activate or re-activate devices, change **Allow user wireline activation** to **Activate Any PIN**.
   - To permit users to activate new devices only, change **Allow user wireline activation** to **Activate Unused PIN only**.
   - To prevent users from activiating devices, change **Allow user wireline activation** to **No**.
5. Click **Save all**.

Permit users to back up and restore data using the BlackBerry Web Desktop Manager

You can specify whether users can back up and restore data on BlackBerry devices using the BlackBerry Web Desktop Manager.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution Topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service**.
3. Click **Edit component**.
4. On the **BlackBerry Web Desktop Manager information** tab, change **Allow users to back up and restore data** to **Yes**.
5. Click **Save all**.

After you finish: To prevent users from backing up and restoring data from their BlackBerry devices, change **Allow users to backup and restore data** to **No**.

Configure the domains for backing up data using the BlackBerry Web Desktop Manager

You can specify the domains that users' computers are located in so that you can limit which users can back up data on their BlackBerry devices using the BlackBerry Web Desktop Manager.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution Topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service** .
3. Click **Edit component**.
4. On the **BlackBerry Web Desktop Manager information** tab, in the **Device backup domains** field, type a domain that permits the user to back up data.
5. Click the **Add** icon.
6. Repeat steps 4 and 5 for each domain that you want to add.
7. Click **Save all**.

Change the text colors in the BlackBerry Web Desktop Manager

You can change the text colors in BlackBerry Web Desktop Manager to match the colors that your organization uses for UIs.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service**.
3. On the **Font colors** tab, click **Edit Component**.
4. Type the name of the color, in hexadecimal format, for the color of the BlackBerry Web Desktop Manager text that you want to change.

5. Click **Save All**.

BlackBerry Web Desktop Manager text colors

Parameter	Description	Default
Font color 1	This text color specifies the hexadecimal color value of the description text in the BlackBerry Web Desktop Manager.	#000000 (black)
Font color 2	This text color specifies the hexadecimal color value of the copyright text in the BlackBerry Web Desktop Manager.	#788cb6 (steel blue)
Font color 3	This text color specifies the hexadecimal color value of the text in the BlackBerry Web Desktop Manager error messages.	#ff0000 (red)
Font color 4	This text color specifies the hexadecimal color value of the text in the BlackBerry Web Desktop Manager information messages.	#6c4091 (purple)
Font color 5	This text color specifies the hexadecimal color value of unavailable links in the BlackBerry Web Desktop Manager. For example, text for options that you make unavailable using IT policy rules use this parameter.	#a1a1a4 (grey)
Font color 6	This text color specifies the hexadecimal color value of the text in the BlackBerry Web Desktop Manager headers, and the text in the tab links that point to web pages that the user is not currently visiting.	#ffffff (white)
Font color 7	This text color specifies the hexadecimal color value of the text in the available BlackBerry Web Desktop Manager menu and text in the option links.	#005387 (blue)
Font color 8	This text color specifies the hexadecimal color value of the BlackBerry Web Desktop Manager link text when a user pauses a cursor on a link.	#8cb811 (green)

Display a custom image in the BlackBerry Web Desktop Manager

You can display a custom image, such as your organization's logo, in the upper-right corner of the BlackBerry Web Desktop Manager. The image file that you specify must be a .jpg or .gif file that is located on a trusted web site.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution Topology** > **BlackBerry Domain** > **Component view** .
2. Click **BlackBerry Administration Service**.
3. Click **Edit component**.
4. On the **Company logos** tab, type the HTTPS URL for your organization's logo.
5. Click **Save all**.

Display the domain name on the login page of the BlackBerry Web Desktop Manager

You can specify the domain name that appears automatically in the Domain field when users browse to the BlackBerry Web Desktop Manager login page. You can specify only one domain name. You can also provide the domain name to users when you send their login information to them.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution Topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service**.
3. Click **Edit component**.
4. On the **Microsoft® Active Directory® authentication** tab, in the **Login domain** section, in the **Default domain** field, type the name of the default domain that users log in from.
5. Click **Save all**.

Creating and configuring Wi-Fi profiles and VPN profiles

19

Creating and configuring Wi-Fi profiles

You can use Wi-Fi configuration settings and optional VPN configuration settings to manage BlackBerry devices that can operate on both mobile and Wi-Fi networks.

You can manage the configuration settings for user accounts that are associated with a BlackBerry Enterprise Server by creating Wi-Fi profiles. You can create and assign one or more Wi-Fi profiles to a user account or to a group using a process that is similar to the process you use to create an IT policy and assign it to a user account.

For more information, see the *BlackBerry Enterprise Server Feature and Technical Overview*.

Prerequisites: Creating Wi-Fi profiles and VPN profiles

You must install and configure wireless access points for your organization’s enterprise Wi-Fi network. Perform the following actions:

- Verify that the access points comply with the IEEE 802.11a standard, IEEE 802.11b standard, or IEEE 802.11g standard.
- Verify the number of connections for each access point to make sure that the access points can manage additional traffic.
- Verify that users can roam between access points.
- Refer to the documentation for the access points to complete a site survey and assign channels.
- If your organization does not use a switched enterprise Wi-Fi network and your organization has multiple subnets, configure the subnets to cover the same physical area. The configuration can affect how users send or receive calls.
- Assign an SSID to each access point or each group of access points that share an SSID.
- If users can roam between the access points, configure all of the relevant SSID profiles on each access point.
- If your organization uses NAT traversal, verify that the access points support NAT traversal.

You must configure authentication and encryption for the access points. Perform the following actions:

- Configure authentication using a supported authentication method. For example, if your organization uses layer 2 access security, verify that your organization uses one of the supported layer 2 security methods.
- Configure encryption using a supported encryption method.

If your organization’s environment requires a VPN concentrator, configure a VPN concentrator for VPN access security using IPsec VPN. See the administrator for your organization’s firewall or VPN concentrator to determine the appropriate configuration settings.

You must configure firewall settings. Perform the following actions:

- If your organization use a proxy firewall, configure the proxy server so that it is transparent to users.
- Verify that the IP addresses for the BlackBerry Domain that are relevant to your organization’s environment are permitted addresses.
- Verify that you add the IP address of the BlackBerry Router to the DNS server.

Configure the ports for the Wi-Fi network.

You must configure access to the DHCP server and DNS server. Perform the following actions:

- If necessary, configure your organization’s enterprise Wi-Fi network to access the DHCP server.
- If you do not use static IT addresses, use the DNS lookup tool on a Wi-Fi enabled BlackBerry device to verify that the BlackBerry device can access the DHCP server.
- Use the DNS lookup tool on a Wi-Fi enabled BlackBerry device to verify that the BlackBerry device can access one or more DNS servers.

If your organization uses an AAA server, you must configure it. Perform the following actions:

- Configure the AAA server to support the Wi-Fi authentication method that your organization uses.
- Permit all access points to use the AAA server.

If you configure service-specific access security, create a captive portal login.

You must configure user accounts in your organization's environment. Perform the following actions:

- Create authentication credentials for the user accounts.
- If your organization uses EAP-TLS, EAP-TTLS, or PEAP authentication methods, permit the BlackBerry Enterprise Server to access to the PKI infrastructure and certificates.

Add the MAC addressses of every BlackBerry device that you permit to access a specific enterprise Wi-Fi network (an allowed list) or prevent from accessing a specific enterprise Wi-Fi network (a restricted list) to the controller for each access point.

Connection types and port numbers for a Wi-Fi network

Port assignments might vary by mobile network provider.

Item	Connection type	Default port number	Where to configure the connection
incoming connection from a BlackBerry device to the BlackBerry Router	TCP	4101	Windows registry
outgoing connection from a BlackBerry device to the BlackBerry Router for a direct Wi-Fi connection to the BlackBerry Infrastructure	TCP	443	—

Create a Wi-Fi profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Create Wi-Fi profile**.
3. In the **Name** field, type a name for the Wi-Fi profile.
4. Click **Save**.

After you finish: Configure the Wi-Fi profile.

Create a Wi-Fi profile based on an existing Wi-Fi profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to copy.
4. Click **Copy profile**.
5. Type a name for the new Wi-Fi profile.
6. Click **Save**.

After you finish: Configure the Wi-Fi profile.

Configure a Wi-Fi profile on a BlackBerry device

You can instruct BlackBerry device users to perform the following task if you want users to configure a Wi-Fi profile for the Wi-Fi networks that you did not create a Wi-Fi profile for in the BlackBerry Administration Service. By default, new Wi-Fi profiles appear at the end of the Wi-Fi profile list on the BlackBerry device.

1. On the Home screen or in the application list, click **Manage Connections**.
2. Click **Set Up Wi-Fi Network**.
3. Perform the instructions on the screen.
4. On the **Wi-Fi Setup Complete** screen, perform any of the following actions:
   - To change the order of the Wi-Fi profiles, click **Prioritize Wi-Fi Profiles**.
   - To specify registration information for the Wi-Fi network, click Wi-Fi Hotspot Login.
5. Click **Finish**.

Assign a Wi-Fi profile to a group

You can assign one or more Wi-Fi profiles to a group.

Before you begin: Create and configure a Wi-Fi profile.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. In the **Manage groups** section, click the group that you want to assign a Wi-Fi profile to.
4. On the **Wi-Fi profiles** tab, click **Edit group**.
5. In the **Available Wi-Fi profiles** list, click the profile that you want to assign to the group and click **Add**. Repeat for any additional profiles that you want to assign to the group.
6. Click **Save all**.

When you assign a Wi-Fi profile to a group that has at least one user account assigned to it, the BlackBerry Administration Service creates jobs to deliver the resulting objects to BlackBerry devices.

Assign a Wi-Fi profile to a user account

You can assign more than one Wi-Fi profile to a user account.

Before you begin: Create and configure a Wi-Fi profile.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for one or more user accounts.
4. Click the name of the user account that you want to assign a Wi-Fi profile to.
5. Click **Edit user**.
6. On the **Wi-Fi profiles** tab, in the **Wi-Fi profile name** section, in the drop-down list, click the Wi-Fi profile.
7. If required, in the **Wi-Fi user specific settings** section, specify the login information for the Wi-Fi profile.
8. Click the **Add** icon.
9. Click **Save all**.

When you assign a Wi-Fi profile to a user account, the BlackBerry Administration Service creates a job to deliver the resulting object to the BlackBerry device.

Configure a Wi-Fi profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of a Wi-Fi profile.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, change the values for the configuration settings.
6. Click **Save All**.

After you finish:

- For information about the Wi-Fi configuration settings, see the *BlackBerry Enterprise Server Policy Reference Guide*.
- If the Wi-Fi network includes a captive portal, verify that you changed the Wi-Fi Enable Authentication Page option to True to permit users to access the captive portal using the WLAN Login browser on their BlackBerry devices.
- To update the BlackBerry device information immediately, resend the IT policy to the BlackBerry device.

Creating and configuring VPN profiles

Wi-Fi enabled BlackBerry devices have built-in VPN clients that supports several types of VPN concentrators.

To create a VPN profile, you configure the VPN configuration settings (for example, the IP address of the VPN concentrator, user names and passwords, and cryptographic methods that the BlackBerry Enterprise Server uses) on a BlackBerry device or using a VPN profile or IT policy. You can assign one or more VPN profiles to a user account or to a group. If a user account has a VPN profile, you can associate the VPN profile with the Wi-Fi profile for the user account.

Depending on your organization's security policy, you can save a user name and password to a BlackBerry device to prevent the BlackBerry device from prompting the user for the login information the first time (or each time) the BlackBerry device connects to the enterprise Wi-Fi network.

Create a VPN profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Create VPN profile**.
3. In the **Name** field, type a name for the VPN profile.
4. Click **Save**.

After you finish: Configure the VPN profile.

Create a VPN profile based on an existing VPN profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage VPN profiles**.
3. Click the name of the VPN profile that you want to copy.
4. Click **Copy profile**.
5. Type a name for the new VPN profile.
6. Click **Save**.

After you finish: Configure the VPN profile.

Configure a VPN profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage VPN profiles**.
3. Click the name of the VPN profile.

4. Click **Edit profile**.
5. On the **VPN profile settings** tab, change the values for the configuration settings.
6. Click **Save All**.

After you finish:

- For information about VPN configuration settings, see the *BlackBerry Enterprise Server Policy Reference Guide*.
- To update BlackBerry device information immediately, resend the IT policy to the BlackBerry device.

Assign a VPN profile to a group

You can assign one or more VPN profiles to a group.

Before you begin: Create and configure a VPN profile.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. In the **Manage groups** section, click the group that you want to assign a VPN profile to.
4. On the **VPN profiles** tab, click **Edit group**.
5. In the **Available VPN profiles** list, click the profile that you want to assign to the group and click **Add**. Repeat for any additional profiles that you want to assign to the group.
6. Click **Save**.

When you assign a VPN profile to a group that has at least one user account assigned to it, the BlackBerry Administration Service creates jobs to deliver the resulting objects to BlackBerry devices.

Assign a VPN profile to a user account

You can assign one or more VPN profile to a user account.

Before you begin: Create and configure a VPN profile.

1. In the BlackBerry Administration Service, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. Click the display name for the user account.
5. Click **Edit user**.
6. On the **VPN profiles** tab, in the **VPN profile name** section, in the drop-down list, click the appropriate VPN profile.

7. If required, in the **VPN user specific settings** section, specify the login information that you want to associate with the VPN profile.
8. Click the **Add** icon.
9. Click **Save All**.

When you assign a VPN profile to a user account, the BlackBerry Administration Service creates a job to deliver the resulting object to the BlackBerry device.

Associate a VPN profile with a Wi-Fi profile

To permit a BlackBerry device to connect to a Wi-Fi network using a VPN session, you must associate a VPN profile with a Wi-Fi profile that you assigned to the user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, in the **Wi-Fi associations** section, in the **Associated VPN Profile** drop-down list, click the VPN profile that you want to associate with the Wi-Fi profile.
6. Click **Save All**.

After you finish: To update the BlackBerry device information immediately, resend the IT policy to the BlackBerry device.

Delete a Wi-Fi profile

Before you begin: Verify that the Wi-Fi profile is not assigned to a user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of a Wi-Fi profile.
4. Click **Delete profile**.
5. Click **Yes - Delete the profile**.

Delete a VPN profile

Before you begin: Verify that the VPN profile is not assigned to a user account or associated with a Wi-Fi profile.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage VPN profiles**.
3. Click the name of a VPN profile.
4. Click **Delete profile**.
5. Click **Yes - Delete the profile**.

Importing profile information from a .csv file

You can update the Wi-Fi profiles and VPN profiles that you want to assign to user accounts and the user names and passwords for the profiles by importing a .csv file using the BlackBerry Administration Service. When you import profile information from a file, you can configure the profile information for multiple user accounts at the same time.

The .csv file must contain the following information:

- user accounts that you want to update
- names of profiles that you want to change
- whether you want to add, remove, or change the profiles

Best practices: Creating a .csv file that contains profile information that you want to import

Consider the following guidelines:

- Specify only one action that you want the BlackBerry Enterprise Server to perform in each row of the file.
- To assign more than one action to a user account, create multiple rows for the user account.
- If you are using a text editor to create the .csv file, include a comma (,) after the value that appears in each field in each row. If a field does not contain a value, include only a comma in the field.
- If you are using a text editor to create the .csv file, include a character return at the end of each row.

- If you are using a text editor to create the .csv file, use quotation marks (" ") if the value for a field contains a space (for example, "Westlee Barichak").
- Add no more than 2000 actions to a file.
- Assign a maximum of 32 profiles to BlackBerry devices that are running BlackBerry Device Software versions that are earlier than 4.5.0.
- Assign a maximum of 64 profiles to BlackBerry devices that are running BlackBerry Device Software version 4.5.0 and later.

Create a .csv file that contains profile information that you want to import

Before you begin: Using the BlackBerry Administration Service, create profiles and specify the configuration settings for the profiles.

1. Using the BlackBerry Administration Service, export user information for the user accounts that you want to update profile information for to a .csv file.
2. In any application that permits you to update .csv files, add the following fields to the .csv file that you exported in step 1:
   - Attribute Name
   - Attribute Type
   - Action
   - User Name
   - Password
3. Configure the fields for each user account in the file.
4. Save the changes.

Example: Adding profile information to user accounts

```
"User Id","Display Name","PIN","Email Address","Logon Name","Attribute
Name","Attribute Type","Action","User Name","Password"
"16","Westlee Barichak","","wbarichak@example.com",,"wifi_1","WLAN","ADD","test
user","test password"
"17","Jovanka Buac","","jbuac@example.com",,"vpn_1","VPN","ADD"
"8","Sherisse Da
Silva","2072C4B7","sdasilva@example.com",,"wifi_1","WLAN","ADD","wlan_user","wlan_pa
ss"
"8","Sherisse Da Silva","2072C4B7","sdasilva@example.com",,"vpn_1","VPN","ADD"
```

Example: Changing profile information that you assigned to user accounts

```
"User Id","Display Name","PIN","Email Address","Logon Name","Attribute
Name","Attribute Type","Action","User Name","Password"
"16","Westlee
Barichak","","wbarichak@rim.com",,"wlan_1","WLAN","UPDATE","update_username","update
_password"
"8","Sherisse Da
Silva","2072C4B7","sdasilva@.rim.com",,"wifi_1","WLAN","UPDATE","update_username","u
pdate_password"
```

Example: Removing profile information from user accounts

```
"User Id","Display Name","PIN","Email Address","Logon Name","Attribute
Name","Attribute Type","Action","User Name","Password"
"8","Lou Sicoli","2072C4B7","lsicoli@example.com",,"wlan_1","WLAN","DELETE"
"9","Sarah Symonds","2072C4B7","ssymonds@example.com",,"vpn_1","VPN","DELETE"
"16","Westlee Barichak","","wbarichak@example.com",,"wlan_1","WLAN","DELETE"
"16","Westlee Barichak","","wbarichak@example.com",,"vpn_1","VPN","DELETE"
```

Related information

Export a list of user accounts, 87

Fields in the .csv file that contains profile information

The following table describes the fields that you can configure in a .csv file. The BlackBerry Administration Service uses the fields in the .csv file to update profile information that you assigned to user accounts.

Field	Description
User Id	This field specifies the user identifier that the BlackBerry Enterprise Server creates for each user account. You must specificy a value in this field.
Display Name	This field specifies the user name for the user account.
PIN	This field specifies the BlackBerry device PIN.
Logon Name	This field specifies the name that the user can use to log in to the BlackBerry Administration Service or BlackBerry Web Desktop Manager.
Attribute Name	This field specifies the name of the Wi-Fi profile or VPN profile. You must specify a value in this field.
Attribute Type	This field specifies whether the profile is a Wi-Fi profile or VPN profile. You must specify either WLAN or VPN as the value in this field.
Action	This field specifies whether you want to add, remove, or update the profile. You must specify ADD, DELETE, or UPDATE as the value in this field.

Field	Description
User Name	This field specifies the user name that the BlackBerry device can use to access the enterprise Wi-Fi network or VPN, if a user name is required.
Password	This field specifies the password that the BlackBerry device can use to access the enterprise Wi-Fi network or VPN, if a password is required. You can include quotation marks (" ") in the password.

Import profile information from a .csv file

The BlackBerry Administration Service processes actions in the order that they appear in the .csv file. If two actions that you listed in the file contradict each other, the action that appears closer to the end of the file is the action that the BlackBerry Administration Service processes. If the BlackBerry Administration Service notices an error that is specific to an action during the import process (for example, you formatted an action incorrectly in the .csv file), the BlackBerry Administration Service continues to process the remaining actions in the file and displays an error message for the action that the BlackBerry Administration Service could not process.

1. In the BlackBerry Administration Service, expand **User** > **Manage users**.
2. In the **Search for users** section, click **Update Wi-Fi Information for users from a list**.
3. Click **Browse**.
4. Navigate to the .csv file that you want to import.
5. Click **Open**.
6. Click **Save**.

Configuring encryption and authentication methods for Wi-Fi enabled BlackBerry devices

20

For information about the encryption and authentication methods for Wi-Fi connections, see the *BlackBerry Enterprise Solution Security Technical Overview*.

Configuring WEP encryption

WEP encryption uses matching encryption keys that are located at wireless access points and wireless clients to secure wireless communication.

To configure WEP encryption, you must distribute the WEP keys in the Wi-Fi profiles that you assign to user accounts. The BlackBerry Enterprise Server sends the WEP key information when users activate Wi-Fi enabled BlackBerry devices.

The WEP keys on BlackBerry devices must match the WEP keys that are located at the access points.

You can configure four WEP keys and a default key ID. The WEP key numbering on BlackBerry devices does not match the WEP key numbering in the configuration settings of the Wi-Fi profile for the enterprise Wi-Fi network. For example, WEP key 1 on the BlackBerry device is WEP key 0 in the configuration settings, and WEP key 2 on the BlackBerry device is WEP key 1 in the configuration settings. You type or copy the WEP keys for the access points as a string of hexadecimal digits.

BlackBerry devices do not support a WEP passphrase.

Configure WEP keys for BlackBerry devices using a Wi-Fi profile

If BlackBerry device users in your organization's environment use BlackBerry 7270 smartphones, you must configure WEP keys using IT policy rules instead of configuration settings.

Before you begin: Obtain the WEP keys for the wireless access point. For more information, see the documentation for the access point.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to change.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, configure the values for the following configuration settings:
   - Wi-Fi WEP Key 1
   - Wi-Fi WEP Key 2
   - Wi-Fi WEP Key 3
   - Wi-Fi WEP Key 4
6. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Enterprise Server Policy Reference Guide*.
- Assign the Wi-Fi profile to the user accounts.
- Resend the IT policy that you assign to the user accounts to Wi-Fi enabled BlackBerry devices.

Related information

Creating and configuring Wi-Fi profiles, 235

Configuring PSK encryption

The IEEE 802.1X™ standard specifies PSK encryption as an access control method for enterprise Wi-Fi networks. You can use PSK encryption in small office and home environments where it is not feasible to configure server-based authentication.

To configure PSK encryption, you must distribute a passphrase to Wi-Fi enabled BlackBerry devices that matches the key or passphrase for the wireless access points. You must distribute the passphrase using the Wi-Fi profiles that you assign to user accounts. The BlackBerry Enterprise Server sends the passphrase when users activate the BlackBerry devices.

For more information about how the BlackBerry Enterprise Solution supports PSK encryption, see the *BlackBerry Enterprise Server Security Technical Overview*.

Configure PSK encryption data for BlackBerry devices using a Wi-Fi profile

If BlackBerry device users in your organization's environment use BlackBerry 7270 smartphones, you must configure passphrases using IT policy rules instead of configuration settings.

Before you begin: Obtain the passphrase for the wireless access point. For more information, see the documentation for the access point.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to change.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, in the **Wi-Fi Preshared Key** field, type the passphrase.
6. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Enterprise Server Policy Reference Guide*.
- Assign the Wi-Fi profile to the user accounts.
- Resend the IT policy that you assign to the user accounts to Wi-Fi enabled BlackBerry devices.

Related information

Creating and configuring Wi-Fi profiles, 235

Configuring LEAP authentication

LEAP authentication is a proprietary authentication method that was developed by Cisco Systems. LEAP authentication provides one-side, server-based authentication between an enterprise Wi-Fi network and Wi-Fi enabled BlackBerry devices and provides per-client dynamic generation of WEP keys and automatic WEP key updates during a session.

BlackBerry devices support LEAP authentication that uses a user name and password. You must distribute the user name and password using a Wi-Fi profile that you assign to user accounts. BlackBerry devices use a one-way function to encrypt passwords before they send the passwords to the authentication server.

For more information about how the BlackBerry Enterprise Solution supports LEAP authentication, see the *BlackBerry Enterprise Server Security Technical Overview*.

Configure LEAP authentication data for BlackBerry devices using a Wi-Fi profile

If BlackBerry device users in your organization's environment use BlackBerry 7270 smartphones, you must configure user names and passwords using IT policy rules instead of configuration settings.

Before you begin:

- Using the wireless access point, configure the LEAP settings to accept SSID association requests from users that have the credentials that you specify or to identify the authentication server that the Wi-Fi enabled BlackBerry devices use to verify user credentials. For more information, see the documentation for your organization's access points.
- Configure strong password policies if Wi-Fi network authentication uses LEAP authentication.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to change.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, perform the following actions:
    - In the **Wi-Fi User Name** field, type the user name for LEAP authentication.
    - In the **Wi-Fi User Password** field, type the password for LEAP authentication.
6. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Enterprise Server Policy Reference Guide*.
- Assign the Wi-Fi profile to the user accounts.
- Resend the IT policy that you assign to the user accounts to BlackBerry devices.

Related information

Creating and configuring Wi-Fi profiles, 235

Configuring PEAP authentication

If your organization implements PEAP authentication, Wi-Fi enabled BlackBerry devices must authenticate to an authentication server before they can connect to the enterprise Wi-Fi network.

PEAP authentication requires that BlackBerry devices trust the authentication server certificate. To trust the authentication server certificate, BlackBerry devices must trust the certificate authority that issued the certificate. A certificate authority that the BlackBerry devices and the authentication server trust mutually must generate the certificate for the authentication server.

Each BlackBerry device stores a list of explicitly trusted certificate authority certificates. BlackBerry devices that use PEAP authentication require the root certificate for the certificate authority that issued the certificate.

To distribute the root certificate to BlackBerry devices, you can use the certificate synchronization tool in the BlackBerry Desktop Manager. You must configure a Wi-Fi profile to provide the user name and password for authentication.

For more information about how the BlackBerry Enterprise Solution supports PEAP authentication, see the *BlackBerry Enterprise Server Security Technical Overview*.

Configure PEAP authentication data for BlackBerry devices using a Wi-Fi profile

If BlackBerry device users in your organization's environment use BlackBerry 7270 smartphones, you must configure user names and passwords using IT policy rules instead of configuration settings.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to configure.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, perform the following actions:
   - In the **Wi-Fi User Name** field, type the user name for PEAP authentication.
   - In the **Wi-Fi User Password** field, type the password for PEAP authentication.
6. If necessary, on the **Wi-Fi profile settings** tab, configure the following configuration settings:
   - Wi-Fi Link Security
   - Wi-Fi Hard Token Required
   - Wi-Fi Server Subject
   - Wi-Fi Server SAN
   - Wi-Fi Disable Server Certificate Validation
7. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Enterprise Server Policy Reference Guide*.
- Resend the IT policy that you assign to the user accounts to BlackBerry devices.
- Distribute the certificates.

Related information

Creating and configuring Wi-Fi profiles, 235

Prerequisites: Distributing a certificate using the BlackBerry Desktop Manager

- Using a public or private certificate authority, obtain or generate a digital certificate for the authentication server. The root.der certificate file is stored in the location where the certificate was created. For example, the authentication server stores a self-signed certificate locally.
- Configure each wireless access point as a client of the authentication server. You must use the same authentication version on clients and servers. For more information, see the documentation for the access points.
- Use the certificate management features of Microsoft Active Directory to download the root certificate from the certificate authority server to the computer.

Distribute a certificate using the BlackBerry Desktop Manager

If a BlackBerry device requires the root certificate for the certificate authority, a client certificate, or both, you can distribute the certificates using BlackBerry Desktop Manager. The BlackBerry device can add the certificates to the list of explicitly trusted certificate authority certificates or the list of client certificates.

1. On the user’s computer, right-click the certificate. Click **Install certificate**.
2. Click **Next**.
3. Click **Place all certificates in the following store**.
4. Click **Browse**.
5. Perform one of the following actions:
    - If you are distributing a root certificate, click **Trusted Root Certification Authorities**.
    - If you are distributing a client certfticate, click **Personal**
6. Click **OK**.
7. Click **Finish**.

8. In the **Security Warning** dialog box, click **Yes**.
9. Connect the BlackBerry device to the BlackBerry Desktop Manager.
10. In the BlackBerry Desktop Manager, select the **Certificate Synch** tool.
11. Type a password that you can use as the keystore password.
12. Perform one of the following actions:
    - If you are distributing a root certificate, on the **Root Certificates** tab, select the certificate that you add to the certificate list on the BlackBerry device.
    - If you are distributing a client certificate, on the **Personal** tab, select the certificate that you want to add to the certificate list on the BlackBerry device.

Users cannot find the certificate synchronization tool in the BlackBerry Desktop Manager

Possible cause

The certificate synchronization tool was not installed when the user installed the BlackBerry Desktop Manager.

Possible solution

Instruct the user to re-install the BlackBerry Desktop Manager using the custom installation option. During the custom installation process, the user can install the certificate synchronization tool.

Configure PEAP configuration settings in the Wi-Fi profile on a BlackBerry device

If you do not configure the PEAP configuration settings using the BlackBerry Administration Service, instruct users to configure the settings in the Wi-Fi profile on the BlackBerry device.

1. On the BlackBerry device, in the device options, click **Wi-Fi Connections**.
2. Click the Wi-Fi profile that you want to configure.
3. Click **Edit**.
4. In the **Security Type** list, select **PEAP**.
5. Type the user name and password for the messaging server.
6. In the **CA certificate** list, click the certificate for the authentication server.
7. Select the **Inner link security type**.
8. If your organization does not use EAP-MS-CHAPv2, if necesssary, in the **Token** list, select the token type.

9. If necesssary, in the **Server subject** field, type the server name in the server certificate, in URL format (for example, server1.domain.com or server1.domain.net). If you leave the field blank, the BlackBerry device skips over it during server authentication.
10. If necesssary, in the **Server SAN** field, type the alternative name for the server, in URL format (for example, server1.domain.com or server1.domain.net). If you leave the field blank, the BlackBerry device skips over it during server authentication.
11. If your organization uses dynamic IP addresses, verify that the **Automatically obtain IP address and DNS** option is selected.
12. Verify that the **Allow inter-access point handover** option is selected.
13. If necesssary, select the **Prompt before connection** check box. If you do not select the check box, the BlackBerry device connects to an available wireless access point automatically.
14. If necesssary, select the **Notify on authentication failure** check box.
15. If necesssary, select the VPN profile.

Configuring EAP-TLS authentication

If your organization implements EAP-TLS authentication, Wi-Fi enabled BlackBerry devices must authenticate to an authentication server so that they can connect to the enterprise Wi-Fi network.

EAP-TLS authentication requires that BlackBerry devices trust the authentication server certificate and use a client-side certificate as the supplicant credentials. To trust the authentication server certificate, BlackBerry devices must trust the certificate authority that issued the certificate. A certificate authority that the BlackBerry devices and the authentication server trust mutually must generate the certificate for the authentication server and the certificate for each BlackBerry device.

BlackBerry devices that use EAP-TLS authentication require a client certificate and the root certificate for the certificate authority server that created the certificate for the authentication server. You can obtain and install both certificates using the same distribution method.

To distribute the certificates to BlackBerry devices, you can use the certificate synchronization tool in the BlackBerry Desktop Manager, or you can enroll the certificate over the wireless network. You must configure a Wi-Fi profile to provide the user name and password for authentication.

For more information about how the BlackBerry Enterprise Solution supports EAP-TLS authentication, see the *BlackBerry Enterprise Server Security Technical Overview*.

Configure EAP-TLS authentication data for BlackBerry devices using a Wi-Fi profile

If BlackBerry users in your organization's environment use BlackBerry 7270 smartphones, you must configure user names and passwords using IT policy rules instead of configuration settings.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to change.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, perform the following actions:
   - In the **Wi-Fi User Name** field, type the user name for EAP-TLS authentication.
   - In the **Wi-Fi User Password** field, type the password for EAP-TLS authentication.
6. If required, configure the following configuration settings:
   - Wi-Fi Link Security
   - Wi-Fi Hard Token Required
   - Wi-Fi Server Subject
   - Wi-Fi Server SAN
   - Wi-Fi Disable Server Certificate Validation
7. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Enterprise Server Policy Reference Guide*.
- Resend the IT policy that you assign to the user accounts to Wi-Fi enabled BlackBerry devices.
- Distribute the certificates.

Related information

Prerequisites: Distributing a certificate using the BlackBerry Desktop Manager, 252
Creating and configuring Wi-Fi profiles, 235

Configure EAP-TLS configuration settings in the Wi-Fi profile on a BlackBerry device

If you do not configure the EAP-TLS configuration settings using the BlackBerry Administration Service, instruct the users to configure the settings in the Wi-Fi profile on the Wi-Fi enabled BlackBerry device.

1. On the BlackBerry device, in the device options, click **Wi-Fi Connections**.
2. Click the Wi-Fi profile that you want to change.
3. Click **Edit**.
4. If a warning about a VPN profile appears, click **OK**. EAP-TLS does not require a VPN profile.
5. In the **Security Type** list, select **EAP-TLS**.
6. Type the user name and password for the messaging server.
7. In the **CA certificate** list, click the root certificate for the certificate authority that created the authentication server certificate.
8. In the **Client certificate** list, click the user certificate.
9. If necessary, in the **Server subject** field, type the server name in the server certificate, in URL format (for example, server1.domain.com or server1.domain.net). If you leave the field blank, the BlackBerry device skips over it during server authentication.
10. If necessary, in the **Server SAN** field, type the alternative name for the server, in URL format (for example, server1.domain.com or server1.domain.net). If you leave the field blank, the BlackBerry device skips over it during server authentication.
11. If your organization uses dynamic IP addresses, verify that the **Automatically obtain IP address and DNS** option is selected.
12. Verify that the **Allow inter-access point handover** option is selected.
13. If necessary, select the **Prompt before connection** check box. If you do not select the check box, the BlackBerry device connects to an available wireless access point automatically.
14. If necessary, select the **Notify on authentication failure** check box.

Configuring EAP-TTLS authentication

If your organization implements EAP-TTLS authentication, Wi-Fi enabled BlackBerry devices must authenticate to an authentication server so that they can connect to the enterprise Wi-Fi network.

EAP-TTLS authentication requires that BlackBerry devices trust the authentication server certificate. To trust the authentication server certificate, BlackBerry devices must trust the certificate authority that issued the certificate. A certificate authority that the BlackBerry devices and the authentication server trust mutually must generate the authentication server certificate.

Each BlackBerry device stores a list of explicitly trusted certificate authority certificates. BlackBerry devices that use EAP-TTLS authentication require the root certificate for the certificate authority that created the authentication server certificate.

To distribute the root certificate to BlackBerry devices, you can use the certificate synchronization tool in BlackBerry Desktop Manager or you can enroll the certificate over the wireless network.

For more information about how the BlackBerry Enterprise Solution supports EAP-TTLS authentication, see the *BlackBerry Enterprise Server Security Technical Overview*.

Configure EAP-TTLS authentication data for BlackBerry devices using a Wi-Fi profile

If BlackBerry device users in your organization's environment use BlackBerry 7270 smartphones, you must configure user names and passwords using IT policy rules instead of configuration settings.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to change.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, perform the following actions:
   - In the **Wi-Fi User Name** field, type the user name for EAP-TTLS authentication.
   - In the **Wi-Fi User Password** field, type the password for EAP-TTLS authentication.
6. If required, configure the following configuration settings:
   - Wi-Fi Link Security
   - Wi-Fi Hard Token Required
   - Wi-Fi Server Subject
   - Wi-Fi Server SAN
   - Wi-Fi Disable Server Certificate Validation
7. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Enterprise Server Policy Reference Guide*.
- Resend the IT policy that you assign to the user accounts to Wi-Fi enabled BlackBerry devices.
- Distribute the certificates.

Related information

Prerequisites: Distributing a certificate using the BlackBerry Desktop Manager, 252
Creating and configuring Wi-Fi profiles, 235

Configure EAP-TTLS configuration settings in the Wi-Fi profile on a BlackBerry device

If you do not configure the EAP-TTLS configuration settings using the BlackBerry Administration Service, instruct a user to configure the settings in the Wi-Fi profile on the Wi-Fi enabled BlackBerry device.

1. On the BlackBerry device, in the device options, click **Wi-Fi Connections**.
2. Click the Wi-Fi profile that you want to change.
3. Click **Edit.**
4. In the **Security Type** list, select **EAP-TTLS**.
5. Type the user name and password for the messaging server.
6. In the **CA certificate** list, click the root certificate for the certificate authority that created the authentication server certificate.
7. In the **Inner link security type** list, select **EAP-MS-CHAPv2**.
8. If necessary, in the **Server subject** field, type the server name in the server certificate, in URL format (for example, server1.domain.com or server1.domain.net). If you leave the field blank, the BlackBerry device skips over it during server authentication.
9. If necessary, in the **Server SAN** field, type the alternative name for the server, in URL format (for example, server1.domain.com or server1.domain.net). If you leave the field blank, the BlackBerry device skips over it during server authentication.
10. If your organization use dynamic IP addresses, verify that the **Automatically obtain IP address and DNS** option is selected.
11. Verify that the **Allow inter-access point handover** option is selected.
12. If necesssary, select the **Prompt before connection** check box. If you do not select the check box, the BlackBerry device connects to an available wireless access point automatically.
13. Verify that the **Allow inter-access point handover** option is selected.
14. If necessary, select the **Notify on authentication failure check box**.

Configuring EAP-FAST authentication

EAP-FAST is an authentication method that was developed by Cisco Systems. Similar to PEAP authentication, EAP-FAST authentication encrypts EAP transactions within a TLS tunnel. Although PEAP uses a server-side digital certificate to configure the TLS tunnel, EAP-FAST uses a .pac file.

The .pac file that the BlackBerry devices and the authentication server share contains secret keys that are unique to the BlackBerry devices. The EAP-FAST master key on the authentication server generates the .pac file. EAP-FAST uses the .pac file to open the TLS tunnel and authenticates the user credentials through the TLS tunnel.

Configure EAP-FAST authentication

1. Distribute the .pac file to the wireless client over a network connection that is designed to be secure using automatic PAC provisioning.
2. Configure each wireless access point to connect to the access control server and a DHCP server.
3. Verify that the DHCP server can provide the following information to the wireless client:
    - IP address or network
    - default gateway
    - IP address of the DNS server
4. Configure the access control server.

After you finish:

- For information about the automatic provisioning process, see the documentation for your organization’s authentication server.
- For information about configuring wireless access points, see the documentation for the access points.
- For information about configuring the access control server, see the documentation for the access control server.

Related information

Prerequisites: Distributing a certificate using the BlackBerry Desktop Manager, 252
Creating and configuring Wi-Fi profiles, 235

Send EAP-FAST authentication data to a BlackBerry device using a Wi-Fi profile

If BlackBerry users in your organization's environment use BlackBerry 7270 smartphones, you must configure user names and passwords using IT policy rules instead of configuration settings.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to configure.
4. Click **Edit profile**.
5. In the **Wi-Fi profile settings** tab, perform the following actions:
   - In the **Wi-Fi User Name** field, type the user name for PEAP authentication.
   - In the **Wi-Fi User Password** field, type the password for PEAP authentication.
6. If required, configure the following configuration settings:
   - Wi-Fi Link Security
   - Wi-Fi Inner Authentication Mode
   - Wi-Fi Hard Token Required
   - Wi-Fi Server Subject
   - Wi-Fi Server SAN
   - Wi-Fi EAP-FAST Provisioning method
   - Wi-Fi Disable Server Certificate Validation
7. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Enterprise Server Policy Reference Guide*.
- Resend the IT policy that you assign to the user accounts to BlackBerry devices.
- Distribute the certificates.

Configure EAP-FAST configuration settings in the Wi-Fi profile on BlackBerry devices

If you do not configure the EAP-FAST configuration settings using the BlackBerry Administration Service, instruct users to configure the settings in the Wi-Fi profile on the Wi-Fi enabled BlackBerry device.

1. On the BlackBerry device, in the device options, click **Wi-Fi Connections**.
2. Click the Wi-Fi profile that you want to change.
3. Click **Edit.**
4. In the **Security Type** list, select **EAP-FAST**.
5. Type the user name and password for the messaging server.
6. In the **Inner link security** list, click the security type.
7. If necessary, in the **Token** list, select the token type.
8. If your organization uses dynamic IP addresses, verify that the **Automatically obtain IP address and DNS** option is selected.
9. If necesssary, select the **Prompt before connection** check box. If you do not select the check box, the BlackBerry device connects to an available wireless access point automatically.
10. If necessary, select the **Notify on authentication failure** check box.

Configuring software tokens for BlackBerry devices

The BlackBerry Enterprise Server is designed to work with the RSA Authentication Manager to provide software token support for use with layer 2 and layer 3 Wi-Fi authentication on Wi-Fi enabled BlackBerry devices.

When you configure a software token for users, BlackBerry devices are designed to use the passcode to authenticate the users to the Wi-Fi network and VPNs automatically using the PEAPv1, EAP-GTC, and EAP-TTLS or EAP-GTC authentication methods.

You can configure multiple software tokens for each user. For example, you can configure one software token that a user can use with Wi-Fi authentication and a second software token that a user can use with VPN authentication. When users try to open a Wi-Fi or VPN connection that requires two-factor authentication on the BlackBerry devices, the BlackBerry devices prompt the users to type the software token PIN and submit the current tokencode for the connection type to create the passcode for two-factor authentication.

For more information about how the BlackBerry Enterprise Server supports software tokens, see the *BlackBerry Enterprise Solution Security Technical Overview*.

Prerequisites: Configuring BlackBerry devices for RSA authentication

To perform tasks in the RSA Authentication Manager, see the RSA Authentication Manager documentation, and the documentation for the RSA SecurID token.

- In the RSA Authentication Manager, configure the following policies for the PINs of the software tokens in your organization's environment:
    - whether a PIN is required for authentication
    - whether a PIN is defined by the user or generated by the RSA Authentication Manager
    - whether a PIN is alphanumeric or numeric only
    - whether a PIN has a fixed length or a variable length, with a minimum of four characters and a maximum of eight characters

- Import the token seed file (also known as the *.sdtid file) that contains the UID for each software token into the RSA Authentication Manager Database.
- In the RSA Authentication Manager Database, create a user record for each software token holder.
- In the RSA Authentication Manager Administration application, configure the following parameters for the software token seed file:
  - serial number
  - cryptographic algorithm
  - user account that you can assign the software token to
  - password to protect the software token seed file
- Communicate the password to the user.

Configure BlackBerry devices for RSA authentication

Software tokens use the UID and current time to authenticate the Wi-Fi enabled BlackBerry devices to the RSA Authentication Manager. To permit BlackBerry devices to authenticate to the RSA Authentication Manager, you must synchronize the time and date on BlackBerry devices with the time and date on the computer that hosts the RSA Authentication Manager, even though the RSA Authentication Manager is designed to accommodate time differences of up to three minutes.

Instruct users to use one of the following methods to synchronize the date, time, and time zone settings on the BlackBerry devices with the RSA Authentication Manager:

- Adjust the time on BlackBerry devices using the Date/Time option on the BlackBerry devices manually.
- Use the BlackBerry Desktop Manager to synchronize the date and time on the BlackBerry devices with the date and time on the users' computers.

After you finish:

- Assign the Wi-Fi profile to the user accounts.
- Resend the IT policy to BlackBerry devices.

Configure RSA authentication over a Wi-Fi network using a software token

You must add the serial number of the software token that the Wi-Fi enabled BlackBerry devices can use to a Wi-Fi profile so that RSA authentication can occur over Wi-Fi connections.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to change.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, in the **Wi-Fi Token Serial Number** field, type the serial number of the software token.
6. Click **Save All**.

After you finish:

- Assign the Wi-Fi profile to the user accounts.
- Resend the IT policy that you assign to the user accounts to BlackBerry devices.

Configure RSA authentication over a VPN network using a software token

You must add the serial number of the software token that the Wi-Fi enabled BlackBerry device can use to a VPN profile so that RSA authentication can occur over VPN connections.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy** > **Wi-Fi configuration**.
2. Click **Manage VPN profiles**.
3. Click the name of the VPN profile that you want to change.
4. Click **Edit profile**.
5. On the **VPN profile settings** tab, in the **VPN Token Serial Number** field, type the serial number of the software token.

6. Click **Save All**.

After you finish:

- Assign the VPN profile to the user accounts.
- Resend the IT policy that you assign to the user accounts to BlackBerry devices.

Assign software tokens to a user account

You must assign the software tokens that BlackBerry device users can use to authenticate to a Wi-Fi network or VPN network to the user accounts. Depending on the number of software token records that are available to you, you can assign up to three software tokens to each user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. Click the display name for the user account.
5. Click **Edit user**.
6. On the **Software tokens** tab, type the serial number of the software token.
7. To import the software token seed file for the user account, perform the following actions:
   a. Click **Browse**.
   b. Navigate to the software token seed file for the user account.
   c. Click **Open**.
8. If you configured a password in the RSA Authentication Manager so that you can encrypt the .sdtid file, type and confirm the password.
9. In the **Timeout (minutes)** field, type the length of time, in minutes, that the Wi-Fi enabled BlackBerry device takes to cache the PIN.
10. Click the **Add** icon.
11. Click **Save all**.

Changing the security settings of the BlackBerry Administration Service and BlackBerry Web Desktop Manager

22

Import a new SSL certificate for the BlackBerry Administration Service and BlackBerry Web Desktop Manager

When you install the BlackBerry Administration Service and BlackBerry Web Desktop Manager, the setup application generates an SSL certificate to protect the HTTPS connection. You can import a self-signed SSL certificate or a trusted certificate that a certification authority signs after the installation process completes. If you configure a BlackBerry Administration Service pool, you must generate an SSL certificate that uses the name of the BlackBerry Administration Service pool.

For more information about using the keytool, visit java.sun.com/javase/6/docs/technotes/tools/windows/keytool.html.

Before you begin: If you want to use a trusted certificate, copy the root certificate of the certification authority to the computer that hosts the BlackBerry Administration Service.

1. On a computer that hosts a BlackBerry Administration Service instance, in <*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\BAS\bin\web.keystore , back up the **web.keystore** file.
2. Using the keytool in <*drive*>:\Program Files\Java\<*JRE_version*>\bin , delete the default SSL certificate that the setup application generated (for example, keytool -delete -alias httpssl -keystore "<*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\BAS\bin\web.keystore").
3. Using the keytool and the SSL password that you specified when you installed the BlackBerry Administration Service, generate a new entry and private key in the web.keystore file (for example, keytool -genkey -alias httpssl -keypass <*password*> -keystore "<*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\BAS\bin

\web.keystore"). When the keytool prompts you for the first name and last name, type the pool name of the BlackBerry Administration Service. You can find the pool name in the **Administration Service** – **High Availability** tab.

4. If you want to use a trusted certificate, using the keytool, import the root certificate of the certification authority (for example, keytool -import -alias <*ca_alias_name*> -file <*root_certificate_file*>.cer -trustcacerts -keystore "<*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\BAS\bin\web.keystore").
5. Using the keytool, generate a certificate signing request (for example, keytool -certreq -alias httpssl -file <*certreq_filename*>.csr -keystore "<*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\BAS\bin\web.keystore").
6. Send the certificate signing request to a certification authority so that the certification authority can create the certificate.
7. When the certification authority returns the certificate, copy it into a text file and save it with a .cer extension.
8. Using the keytool, import the certificate to the web.keystore file (for example, keytool -import -alias httpssl -keystore "<*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\BAS\bin\web.keystore" -file "<*certificate_filename*>.cer").
9. In the Windows Services, restart the BlackBerry Administration Service services.
10. Complete the following actions on each computer that hosts a BlackBerry Administration Service instance:
    a. Copy the web.keystore file in the <*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\BAS\bin folder from the BlackBerry Administration Service that you updated to the other BlackBerry Administration Service instances.
    b. In the Windows registry, copy the WebKeyStorePass value in the HKEY_CURRENT_USER\Software\Research In Motion\BlackBerry Enterprise Server\Administration Service\Key Store from the BlackBerry Administration Service that you updated to the other BlackBerry Administration Service instances.
    c. In the Windows Services, restart the BlackBerry Administration Service services.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configuring Microsoft Active Directory authentication in an environment that includes a resource forest

If your organization's environment includes a resource forest that is dedicated to running Microsoft Exchange, you can configure the BlackBerry Administration Service to use Microsoft Active Directory authentication to log in BlackBerry device users that have user accounts that are located in trusted account forests. The BlackBerry Administration Service can use Microsoft Active Directory authentication to log users into the BlackBerry Administration Service console and the BlackBerry Web Desktop Manager.

You must install the BlackBerry Enterprise Server in the resource forest if a resource forest exists in your organization's environment. In the resource forest, you create a mailbox for each user account and associate the mailboxes with the user accounts that are located in the account forests. When you associate the mailboxes in the resource forest with the user accounts in the account forests, the user accounts obtain full access to the mailboxes and the user accounts in the account forests are connected to the Microsoft Exchange server.

To authenticate users who log in to the BlackBerry Administration Service or BlackBerry Web Desktop Manager, the BlackBerry Administration Service must read the user information that is stored in the global catalog servers that are part of the resource forest. To configure the BlackBerry Administration Service to authenticate user accounts that are associated with mailboxes in the resource forest, you must create a Microsoft Active Directory account for the BlackBerry Administration Service that is located in a Windows domain that is part of the resource forest. During the BlackBerry Enterprise Server installation process, you provide the Windows domain, user name, and password for the Microsoft Active Directory account, and, if required, the names of the global catalog servers that the BlackBerry Administration Service can use. You can change the Windows domain, user name, and password for the Microsoft Active Directory account and global catalog servers after the installation process completes.

For more information, visit technet.microsoft.com to read *Using a Dedicated Exchange forest*.

Related information

Restarting BlackBerry Enterprise Server components, 392

Change the information for Microsoft Active Directory authentication

Before you begin:

- Create a Microsoft Active Directory account for the BlackBerry Administration Service that is located in a Windows domain that is a part of the resource forest. When you create the account, specify a password that meets the security requirements of your organization and configure the following password settings:
  - the user is not required to change the password at next login
  - the user's password never expires

1. In the BlackBerry Administration Service, expand **BlackBerry solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service**.
3. On the **Microsoft® Active Directory® authentication** tab, click **Edit component**.
4. In the **User name** field, type the name for the Microsoft Active Directory account that has permission to access the user containers and read the user objects that are stored in the global catalog servers that are located in the resource forest.
5. In the **Password** field and **Confirm password** field, type the password for the Microsoft Active Directory account.

6. In the **User domain** field, type the name of the Windows domain that is a part of the resource forest.
7. In the **Global Catalog search base** field, perform one of the following actions:
   - To permit the BlackBerry Administration Service to search the global catalog, leave the **Global Catalog search base** field blank.
   - To control which user accounts the BlackBerry Administration Service can authenticate with, type the distinguished name of the user container (for example, OU=sales,DC=example,DC=com).
8. If you want the BlackBerry Administration Service to find all of the global catalog servers in the resource forest automatically, in the **Global Catalog server discovery** drop-down list, click **Automatic**.
9. If you want to configure which global catalog servers the BlackBerry Administration Service can access, in the **Global Catalog server discovery** drop-down list, click **Select server from the list below** and perform the following actions:
   a. In the **Global Catalog server** section, type the FQDN of the global catalog server that you want the BlackBerry Administration Service to access (for example, globalcatalog01.example.com). You must type the FQDN of a global catalog server that is located in the Windows domain that the Microsoft Active Directory account located in.
   b. Click the **Add** icon.
   c. Perform this step for each global catalog server that you want the BlackBerry Administration Service to access.
10. Click **Save All**.

The BlackBerry Administration Service validates the information for Microsoft Active Directory authentication. If the information is valid, the BlackBerry Administration Service implements the changes immediately and you do not need to restart the BlackBerry Administration Service services. If the information is invalid, the BlackBerry Administration Service prompts you to specify correct information.

Configuring single sign-on authentication for the BlackBerry Administration Service and BlackBerry Web Desktop Manager

If you configure the BlackBerry Administration Service to support Microsoft Active Directory authentication, you can turn on single sign-on authentication. Single sign-on authentication permits you to access the BlackBerry Administration Service and BlackBerry device users to access the BlackBerry Web Desktop Manager without requiring that you or the users type a Microsoft Active Directory user name and password. By default, if you log in to the BlackBerry Administration Service or users log in to the BlackBerry Web Desktop Manager using Microsoft Active Directory authentication, the browser prompts you or the users to type a Microsoft Active Directory user name and password. If you turn on single sign-on authentication, and you log in to a computer using a Microsoft Active Directory account, you can bypass the login screen and access the BlackBerry Administration Service and BlackBerry Web Desktop Manager directly. The BlackBerry Monitoring Service does not support single sign-on authentication.

Before you turn on single sign-on, you must configure constrained delegation for the Microsoft Active Directory account for the BlackBerry Administration Service.

Configure constrained delegation for the Microsoft Active Directory account to support single sign-on authentication

1. Use the Windows Server ADSI Edit tool to add the following SPNs for the BlackBerry Administration Service pool to the Microsoft Active Directory account :
   - HTTP/<*BAS_pool_FQDN*> (for example, HTTP/BASconsole104.example.com)
   - BASPLUGIN111/<*BAS_pool_FQDN*> (for example, BASPLUGIN111/BASconsole104.example.com)
2. If you create separate pools of BlackBerry Administration Service instances and BlackBerry Web Desktop Manager instances in the BlackBerry Administration Service pool, add the HTTP/<BAS_pool_FQDN> SPN for each pool to the Microsoft Active Directory account.
3. Configure the Microsoft Active Directory account for constrained delegation using the following settings:
   - trust this user for delegation to specific services only
   - use Kerberos only
4. In the Microsoft Active Directory account properties, on the **Delegation** tab, add BASPLUGIN111/<BAS_pool_FQDN> to the list of services.

After you finish: For more information about configuring constrained delegation for the Microsoft Active Directory account so you can access the BlackBerry Administration Service, visit www.blackberry.com/btsc to read article KB22717.

Turn on single sign-on authentication for the BlackBerry Administration Service

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service**.
3. On the **Microsoft® Active Directory® authentication** tab, click **Edit component**.

4. In the **Login domain** section, in the **Single sign-on authentication for BlackBerry Administration Service turned on** drop-down list, click **Yes.**
5. To configure the Microsoft Active Directory account for each forest, in the **Account forest name** section, type the user domain name, user name, and password for the Microsoft Active Directory account.
6. Click **Save all**.
7. In the Windows Services, restart all of the BlackBerry Enterprise Server services.
8. Instruct all administrators and device users to add the web addresses for the BlackBerry Administration Service and BlackBerry Web Desktop Manager to the list of web sites in the local intranet zone and install the certificate for the BlackBerry Administration Service or BlackBerry Web Desktop Manager in the certificate store of their computers.

BlackBerry Administration Service web addresses and BlackBerry Web Desktop Manager web addresses that support BlackBerry Administration Service single sign-on

If you configure BlackBerry Administration Service single sign-on, you must instruct administrators and BlackBerry Web Desktop Manager users to access the BlackBerry Administration Service console and BlackBerry Web Desktop Manager using the following web addresses:

- https://<*BAS_pool_FQDN*>/webconsole/login
- https://<*BAS_pool_FQDN*>/webdesktop/login

Single-sign authentication takes precedence over other authentication methods that permit administrators and users to log in to the BlackBerry Administration Service console or BlackBerry Web Desktop Manager. If the security policies in your organization require that administrators or users use another authentication method, you must instruct administrators or users to access the BlackBerry Administration Service console or BlackBerry Web Desktop Manager using the following web addresses:

- https://<*BAS_pool_FQDN*>/webconsole/app
- https://<*BAS_pool_FQDN*>/webdesktop/app

For example, the security policies in your organization might require that administrators log in using BlackBerry Administration Service single sign-on and BlackBerry Web Desktop Manager users log in using IBM® Lotus Notes® user names and passwords. In this scenario, you can instruct administrators to log into the BlackBerry Administration Service console using the web address https://<*BAS_pool_FQDN*>/webconsole/login and instruct BlackBerry Web Desktop Manager users to log in to BlackBerry Web Desktop Manager using the web address https://<*BAS_pool_FQDN*>/webdesktop/app.

Changing password settings for BlackBerry Administration Service authentication

If you use BlackBerry Administration Service authentication in your organization's environment, you can change the minimum password length and the number of days until passwords expire to meet the requirements of your organization's security policies.

By default, the minimum password length is four characters and a password expires after 365 days. If you set the password expiry to 0, passwords do not expire. If you change the minimum password length, administrators who have passwords that do not meet the new minimum length are not required to change the passwords until the passwords expire. If you change the password expiry to a shorter period, administrators who are logged in with passwords that are older than the new expiry remain logged in and are required to change the password at the next log in.

The password for the BlackBerry Administration Service administrator account that was created when the BlackBerry Device Service was installed does not expire unless it is changed.

Change password settings for BlackBerry Administration Service authentication

1. In the BlackBerry Administration Service, on the **Servers and components** menu, click **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service**.
3. Click **Edit component**.
4. In the **Security settings** section, change the minimum password length and number of days until the password expires.
5. Click **Save all**.

Regenerate the system credentials for the BlackBerry Administration Service

The setup application generates the system credentials for the BlackBerry Administration Service during the installation process. The BlackBerry Administration Service uses the system credentials when it communicates with other BlackBerry Enterprise Server components. If you suspect that the system credentials are compromised, you can regenerate them on the database server.

Before you begin: Verify that you have database owner permissions for the BlackBerry Configuration Database.

1. On all of the computers that host BlackBerry Administration Service instances, in the Windows Services, stop the BlackBerry Administration Service services.
2. On the database server, on the BlackBerry Configuration Database, run the following SQL statement: `DELETE from BASTraits WHERE PlugInId=8 AND TraitId=0`.
3. On a computer that hosts a BlackBerry Administration Service instance, in the Windows Services, start the BlackBerry Administration Service services.
4. On the computers that host the remaining BlackBerry Administration Service instances, in the Windows Services, start the BlackBerry Administration Service services.

Related information

Restarting BlackBerry Enterprise Server components, 392

Protecting and redistributing devices

23

Preparing a device for redistribution to a new user

You can prepare a BlackBerry device for redistribution to a new BlackBerry device user by performing one of the following actions:

- use the security options on the device to permanently delete all user data
- connect the device to the BlackBerry Administration Service and delete all user data from the device permanently
- connect the device to the BlackBerry Administration Service and delete all user data permanently and remove the BlackBerry Device Software

For more information about using the security options on the device to permanently delete all user data, see the user guide for the device.

After the new user receives the device, you must activate it.

Related information

Assigning BlackBerry devices to user accounts, 92

Use the BlackBerry Administration Service to delete user data and assign the device to a new user

1. Connect the BlackBerry device to the computer that you used to log in to the BlackBerry Administration Service.
2. If you receive a prompt, type the device password.
3. In the BlackBerry Administration Service, on the **Devices** menu, click **Attached devices** > **Manage current device**.
4. Click **Remove user data from current device**.
5. Click **Yes – Remove user data**.

6. Click **Assign current device**.
7. Search for the new user account that you want to assign the device to.
8. Select the user name.
9. Click **Associate user**.
   After you assign the user account to the device, the activation process begins automatically.
10. On the **Devices** menu, click **Attached devices** > **Device software**.
11. Install the applications that the user requires on the device.

Use the BlackBerry Administration Service to delete device data and disable the device before assigning the device to a new user

If you perform this task, you are deleting all device data permanently and disabling the device. You may have to reinstall the BlackBerry Device Software before you assign the device to a new user.

1. Connect the BlackBerry device to the computer that you used to log in to the BlackBerry Administration Service.
2. If you receive a prompt, type the device password.
3. In the BlackBerry Administration Service, on the **Devices** menu, click **Attached devices** > **Manage current device**.
4. Click **Delete all device data and disable device**.
5. Click **Yes – Delete all device data and disable device**.
6. If necessary, reinstall the BlackBerry Device Software using the application loader tool in the BlackBerry Administration Service, BlackBerry Desktop Software, or BlackBerry Web Desktop Manager.
7. Activate the device.

After you finish: For more information about installing the BlackBerry Device Software, see the *BlackBerry Device Software Update Guide*.

Related information

Assigning BlackBerry devices to user accounts, 92

Deleting only work data from a device

To help secure your organization's data on a personal BlackBerry device, you can permit your organization to delete work data from a device when a user no longer works at your organization. You can use the BlackBerry Administration Service to require that a personal device remove only work data when the device receives the Delete only the organization data and remove device IT administrative command over the wireless network. All personal data remains on the device. A BlackBerry device user cannot use the device or make emergency calls while the device deletes the work data.

The device permanently deletes the following work data:

Item	Description
email messages	• email messages that are sent to the user's work email account and the email messages that the user sends from the work email account • draft email messages that the user creates using their work email account
attachments	attachments that are sent to the user's work email account and the attachments that the user sends from the work email account
calendar entries	calendar entries that the user creates using their work calendar
contacts	contacts that the BlackBerry Enterprise Server synchronizes with the user's work email account
memos	all memos
tasks	all tasks
call history	although the device defines phone data for personal use, the call history entries are deleted when you delete work data
call logs	although the device classifies phone data as personal data, the call log files are deleted when you delete work data
the BlackBerry Browser cache	although the device specifies the BlackBerry Browser for personal use, the BlackBerry Browser cache is deleted when you delete work data
files	• files that the user accesses and downloads from your organization's network using the Files application • files on media cards that are created by applications that can access work data (except for media applications) • work data is not deleted from the media card if the media card is not available when the device deletes work data, however the user cannot access work data on the media card after the device removes work data
IT policy	IT policy that is associated with your organization
PIN encryption key	references to your organization's PIN encryption key
device transport key	references to the device transport key which prevents the device from communicating with the BlackBerry Enterprise Server
work service books	service books on the device that the device classifies for work use

Delete only work data from a device

Before you begin: If you want to remove your organization's applications from the BlackBerry device, create a software configuration that includes the applications and set the disposition of all work applications to Disallowed in the software configuration. Assign the software configuration to the user account to send it to the device. For more information, see the *BlackBerry Enterprise Server Administration Guide*.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the PIN for the user account.
5. In the **Device activation** list, click **Delete only the organization data and remove device**.
6. Optionally, in the **Removing users and devices** section, in the **Actions** drop-down list, perform one of the following actions:
   - To delete a user account from the BlackBerry Enterprise Server but retain the BlackBerry Enterprise Server information in the user's mailbox, click **Delete the user**.
   - In a Microsoft Exchange environment, to delete a user account from the BlackBerry Enterprise Server and remove the BlackBerry Enterprise Server information from the user's mailbox, click **Delete the user and remove BlackBerry information from the user's messaging system**.
   - In an IBM Lotus Domino environment, to delete a user account from the BlackBerry Enterprise Server and remove the BlackBerry Enterprise Server information from the user's mailbox, click **Delete the user and remove the profile document and the state database**.
   - To disable a user account from the BlackBerry Enterprise Server but retain the BlackBerry Enterprise Server information in the user's mailbox, click **Disable as BlackBerry user**.
   - In a Microsoft Exchange environment, to disable a user account from the BlackBerry Enterprise Server and remove the BlackBerry Enterprise Server information from the user's mailbox, click **Disable the user and remove BlackBerry information from the user's messaging system**.
   - In a Lotus Domino environment, to disable a user account from the BlackBerry Enterprise Server and remove the BlackBerry Enterprise Server information from the user's mailbox, click **Disable the user and remove the profile document and the state database**.
7. Click **Yes - Delete only the organization data and remove device**.

Using IT administration commands to protect a lost or stolen device

The BlackBerry Enterprise Server includes IT administration commands that you can send over the wireless network to protect sensitive data on a BlackBerry device. You can use the commands to lock the device, permanently delete work data, permanently delete user information and application data, and return the device settings to the default values.

IT administration command	Description
Specify new device password and lock device	This command creates a new password and locks a device over the wireless network. You can communicate the new password to the user verbally when the BlackBerry device user locates the device. When the user unlocks the device, the device prompts the user to accept or reject the new password. You can use this command if the device is lost. If you or a user turned on content protection and a device is running BlackBerry Device Software 4.3.0 or later, you can use this command. If you or a user turned on two-factor content protection, you cannot use this command.
Delete only the organization data and remove device	This command permanently deletes all work data that the device stores and removes the device from the BlackBerry Enterprise Server. All personal data remains on the device. You can send this command to a personal device when a user no longer works at your organization and you want to delete work data from the device. You can also specify whether you want to delete or disable a user account from the BlackBerry Enterprise Server after the device deletes all work data.
Delete all device data and remove device	This command permanently deletes all user information and application data that the device stores. You can configure the following options when you use this command: • specify a delay, in hours, that must occur before the device starts to delete all the user information and application data • require the device to return to its factory default settings when it receives this command • specify whether to permit the user to stop permanently deleting data from the device and making the device unavailable during the delay period You can send this command to a device that you want to distribute to another user in your organization, or to a device that is lost and that the user might not recover.

IT administration command	Description
	You can also specify whether you want to delete or disable a user account from the BlackBerry Enterprise Server after the device deletes all user information and application data.

Protect a stolen device

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the PIN for the user account.
5. In the **Device activation** list, click **Delete all device data and remove device**.
6. Click **Yes - Delete all device data and remove device**.
7. Optionally, in the **Removing users and devices** section, in the **Actions** drop-down list, perform one of the following actions:
   - To delete a user account from the BlackBerry Enterprise Server but retain the BlackBerry Enterprise Server information in the user's mailbox, click **Delete the user**.
   - To delete a user account from the BlackBerry Enterprise Server and remove the BlackBerry Enterprise Server information from the user's mailbox, click **Delete the user and remove BlackBerry information from the user's messaging system**.
   - To disable a user account from the BlackBerry Enterprise Server but retain the BlackBerry Enterprise Server information in the user's mailbox, click **Disable as BlackBerry user**.
   - To disable a user account from the BlackBerry Enterprise Server and remove the BlackBerry Enterprise Server information from the user's mailbox, click **Disable the user and remove BlackBerry information from the user's messaging system**.

After you finish:

- Verify that the BlackBerry device received the command.
- Contact your organization's wireless service provider to turn off the service for a device after you send the IT administration command that deletes all of the device data and deactivates the device.

Protect a lost device

If a user misplaces a BlackBerry device or if a device is stolen, you can protect the data on the device by locking the device or making it unavailable.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the PIN for the user account.
5. In the **Device activation** section, click **Specify new device password and lock device**.
6. Type and confirm an activation password. For devices that are running BlackBerry Device Software version 4.1 and earlier, the password must not contain special characters. Some devices do not support special characters and do not unlock when a user types a password that contains special characters.
7. Click **Specify new device password and lock device**.

Protect a lost device that a user might not recover

If a BlackBerry device is lost but the device user might recover it, you can protect the information on the device by scheduling it to start deleting all user information and application data and to become unavailable after a period of time that you specify. You can also specify whether the user can cancel the scheduled command if the user recovers the device.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the PIN for the user account.
5. In the **Device activation** section, click **Delete all device data and remove device**.
6. In the **Erase Data Settings** section, perform the following actions:
   - In the **Erase Data Delay (hours)** field, type the number of hours that must elapse before the BlackBerry device starts deleting user information and application data.
   - In the **Allow User Override** drop-down list, click **Yes** to permit the user to cancel the scheduled command on the BlackBerry device if the user recovers it.
7. Optionally, in the **Removing users and devices** section, in the **Actions** drop-down list, perform one of the following actions:
   - To delete a user account from the BlackBerry Enterprise Server but retain the BlackBerry Enterprise Server information in the user's mailbox, click **Delete the user**.
   - To delete a user account from the BlackBerry Enterprise Server and remove the BlackBerry Enterprise Server information from the user's mailbox, click **Delete the user and remove BlackBerry information from the user's messaging system**.
   - To disable a user account from the BlackBerry Enterprise Server but retain the BlackBerry Enterprise Server information in the user's mailbox, click **Disable as BlackBerry user**.

- To disable a user account from the BlackBerry Enterprise Server and remove the BlackBerry Enterprise Server information from the user's mailbox, click **Disable the user and remove BlackBerry information from the user's messaging system**.

8. Click **Yes - Delete all device data and remove device**.

Managing administrator accounts

24

Change role permissions

To turn on or turn off permissions for administrator accounts, you can change the permissions for the roles that you assigned to the administrator accounts. If an administrator account is a member of a group that you assigned roles to, you can also turn on or turn off the permissions for the administrator account by changing the permissions for the roles that you assign to the group.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Role**.
2. Click **Manage roles**.
3. In the list of existing roles, click the name of the role that you want to change the permissions for.
4. Click **Edit role**.
5. Switch the appropriate tabs to change the appropriate permissions.
6. Click **Save all**.

After you finish: Instruct administrators to log out of the BlackBerry Administration Service and log in again so that the changes can take effect immediately.

Change the roles for an administrator account

To reflect the changes to an administrator's responsibilities in your organization, you can add or remove one or more administrative roles for the administrator account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.

2. Click **Manage users**.
3. Search for an administrator account.
4. In the search results, click the display name for the administrator account.
5. Click **Edit user**.
6. On the **Roles** tab, in the **Available roles** and **Current roles** lists, add or remove the appropriate roles.
7. Click **Save all**.

Related information
Administrative roles and permissions, 29

Delete a role

You can delete a role when you no longer require it in your organization's environment.

Before you begin: Verify that the role is not assigned to any administrator accounts or groups.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Role**.
2. Click **Manage roles**.
3. In the list of existing roles, click the name of the role that you want to delete.
4. Click **Delete role**.
5. Click **Yes - Delete the role**.

Delete an administrator account

You can delete an administrator account when you no longer require it in your organization's environment.

Before you begin: If the administrator is also a BlackBerry device user, remove the BlackBerry device from the administrator account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Administrator User**.
2. Click **Manage users**.
3. Search for an administrator account.
4. In the search results, click the display name for the administrator account.

5. In the **Status** list, click **Delete user**.
6. Click **Yes - Delete the user**.

Managing groups and user accounts

25

Managing groups

You can reduce the time that you spend managing user accounts by creating groups of similar user accounts 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.

You can assign properties to user accounts and administrator accounts at the individual level, group level, or domain level. The BlackBerry Administration Service applies properties to user accounts and administrator accounts using the following hierarchy:

- The properties at the individual level override the properties at the group level.
- The properties at the group level override the properties at the domain level.

After you add a user account or administrator account to a group, you can override the properties that you configured for the account at the group level or domain level by changing the properties at the user account level.

If you remove a user account or administrator account from a group, the account name remains in the global users list but it does not appear in the group list.

You can either create user-specific groups and assign roles to those groups or use the default user groups that contain pre-existing roles.

If you are managing a large number of groups (over 3000) using the BlackBerry Administration Service in a single domain, your organization's environment might experience a performance impact.

Using default groups to manage user accounts and administrator accounts

The BlackBerry Enterprise Server installation includes default groups that have preconfigured administrative roles. You can use the default groups in your organization's environment instead of creating specific administrative groups. Each default group consists of a set of preconfigured rules which specify the information that administrators can view and the tasks that they can perform using the BlackBerry Administration Service and BlackBerry Monitoring Service.

The default groups ensure users without administrative privileges cannot escalate their permissions, for example, junior administrators cannot escalate their roles to senior administrator roles.

Default group	Description of the default group
Administrators	This is a preconfigured group for BlackBerry Administration Service administrators. This groups has the permissions assigned to the Security role. Administrators in this group are responsible for ensuring all Junior Helpdesk administrators are added to the Junior Helpdesk group.
Help desk representatives	This is a preconfigured group for help desk administrators. This group has the permissions assigned to the Junior Helpdesk role. Junior Helpdesk administrators in this group can perform basic administrative tasks such as adding users to groups and assigning BlackBerry devices to BlackBerry device users. The Junior Helpdesk role can only add users to the Web Desktop Users group and the Junior Helpdesk group.
BlackBerry Web Desktop Manager users	This is a preconfigured group for BlackBerry Web Desktop Manager users. BlackBerry Web Desktop Manager users in this group do not have any BlackBerry Administration Service administrative permissions. Users in this group can perform basic administrative tasks on their own user account using the BlackBerry Web Desktop Manager such as setting an activation password or locking their BlackBerry device.

Remove a user account from a group

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. Click the group name.
4. In the **Manage users in group membership** list, click **Remove users from group membership**.
5. Search for a user account.
6. Select the check boxes beside the display names for the user accounts that you want to remove.
7. Click **Remove from group membership**.

Change the properties of a group

After you create a group, specify the properties that you want to apply to all user and administrator accounts in the group. You can copy the properties from one group to another. When you add user accounts or administrator accounts to a group, the group properties apply to the new accounts automatically.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. Click the group name.
4. Click **Edit group**.
5. Switch between the appropriate tabs and make the appropriate changes.
6. Click **Save all**.

Rename a group

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. Click the group name.
4. Click **Edit group**.
5. In the **Group information** section, in the **Name** field, type a new name for the group.
6. Click **Save all**.

Delete a group

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. Click the group name.
4. Click **Delete group**.
5. Click **Yes - Delete the group**.

Managing user accounts

You can move user accounts from one user group to another or from one BlackBerry Enterprise Server to another in the BlackBerry Domain. If you move a user account from one BlackBerry Enterprise Server to another, the destination BlackBerry Enterprise Server sends new service books to the BlackBerry device over the wireless network.If you are moving a user's mailbox to a different Microsoft Exchange Server and moving the user account to a different BlackBerry Enterprise Server, first move the user's mailbox to the destination mail server. Do not move the user account until the destination BlackBerry Enterprise Server recognizes the new mailbox location.

If you move a user mailbox or change its display name on the messaging server, the BlackBerry Enterprise Server is designed to update the user account within 15 minutes of when the change occurs. If you move a hidden mailbox that does not appear in the contact list, you must update the user account that is associated with the BlackBerry Enterprise Server manually.

When you delete a user account, you can retain the user account information in the BlackBerry Enterprise Server. You can activate the user account again, or the user can continue to use the BlackBerry device as a BlackBerry Desktop Redirector. When you activate a user account that you retained, the user account will have the same settings it had before you deleted it.

Move a user account to a different group

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. On the **Groups** tab, in the **Current groups** list, click the group that you want to to remove the user from.
7. Click **Remove**.
8. In the **Available groups** list, click the group that you want to move the user account to.
9. Click **Add**.
10. Click **Save all**.

Move a user account from one BlackBerry Enterprise Server to another

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for one or more user accounts.
4. In the search results, select one or more user accounts.
5. In the **BlackBerry Enterprise Server status** list, click **Switch BlackBerry user to different BlackBerry Enterprise Server**.
6. In the **Available BlackBerry Enterprise Server instances** list, click the BlackBerry Enterprise Server that you want to move the user accounts to.
7. Click **Next**.
8. A message appears indicating that some of the user accounts might have pending deployment tasks. Perform one of the following actions:
    - If you want to cancel any pending deployment tasks and move all of the user accounts, click **Yes - Switch the users and fail the deployment tasks**.
    - If you do not want to move the user accounts that have pending deployment tasks, click **No - Switch only the users that have no existing deployment tasks**.

Delete a user account from the BlackBerry Enterprise Server

Before you begin: Verify that the primary BlackBerry Enterprise Server is running.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. In the **BlackBerry Enterprise Server status** list, click **Disable as BlackBerry user**.
6. Perform one of the following actions:
    - To retain the BlackBerry Enterprise Server information in the user’s mailbox, click **Yes - Disable as BlackBerry user**.

- To delete the BlackBerry Enterprise Server information from the user’s mailbox, click **Yes - Disable as BlackBerry user and remove information from the user's mail system**.

7. Click **Back to search**.
8. In the **Search users** > **User criteria** section, type the display name for the user account.
9. Click the display name for the user account.
10. In the **Status** list, click **Delete user**.

Update a user account manually

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. In the **Status** list, click **Reload user**.

Add an administrator role to a user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. On the **Roles** tab, in the **Available roles** list, click the role that you want to assign to the user account.
7. Click **Add**.
8. Click **Save all**.

Update the contact list manually

You can update the contact list in the BlackBerry Configuration Database so that you can include any organizational changes or updates in the contact list. The amount of time that the BlackBerry Mail Store Service requires to update the contact list depends on the contact list size.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **Email**.
3. Click **Refresh available user list from company directory**.

Resend service books to a BlackBerry device

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the BlackBerry device PIN.
5. In the **Communications** list, click **Resend service books to a device**.

Managing the delivery of BlackBerry Java Applications, BlackBerry Device Software, and device settings to BlackBerry devices

26

Managing the default distribution settings for jobs

When you create a software configuration and assign it to user accounts, change a software configuration that you assigned to user accounts, or assign or change an IT policy, the BlackBerry Administration Service creates jobs to deliver the resulting objects or settings to BlackBerry devices. You can change the default settings that control how the BlackBerry Administration Service creates jobs and delivers job tasks to BlackBerry devices. You can also change the default settings that the BlackBerry Administration Service uses to deliver IT policies, BlackBerry Java Applications, BlackBerry Device Software, and standard application settings to BlackBerry devices.

Change default settings for a job schedule

When you create a software configuration and assign it to user accounts, when you change a software configuration that you assigned to user accounts, or assign or change an IT policy, the BlackBerry Administration Service creates jobs to deliver the resulting objects or settings to BlackBerry devices. A job consists of multiple tasks. Each task delivers a specific object or setting to a BlackBerry device, for example, upgrading BlackBerry Device Software, installing or removing a BlackBerry Java Application, or sending updated IT policy settings or application settings.

You can change the default settings for a job to control how the BlackBerry Administration Service processes jobs. If you change the default settings for a job, your organization's environment might experience a performance impact.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Specify job schedule settings**.
3. Click **Edit job schedule settings**.
4. In the **Default delay for each job** section, in the **Default delay** field, type the number of minutes that the BlackBerry Administration Service waits before it creates and processes a job.

   The default value is 15 minutes.
5. In the **General** section, in the **Mark job as failed** field, type the number of days that the BlackBerry Administration Service waits before it defines a job that was not delivered to BlackBerry devices as failed.

   The default value is 30 days.
6. In the **Purge jobs** field, type the number of days that the BlackBerry Administration Service waits before it deletes a failed job or a completed job.

   The default value is 7 days.
7. Click **Save all**.

Change how IT policies are sent to BlackBerry devices

You can change the settings that the BlackBerry Administration Service uses to send all IT policy settings and updates to BlackBerry devices. If you change the default settings for IT policy distribution, your organization's environment might experience a performance impact.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Specify IT policy distribution settings**.
3. Click **Edit distribution settings**.
4. Perform any of the following tasks:

Task	Steps
Change the default recurrence day for sending IT policy updates.	1. Click the **Edit** icon for the default recurrence day. 2. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, select the recurrence days. 3. In the **Start time** drop-down list, click the appropriate option. If necessary, set the start time and end time. 4. Click the **Update** icon. By default, the recurrence day is Every day and the start time is All day.
Add a new recurrence day for sending IT policy updates.	If you want to add more than one recurrence day for sending IT policy updates, the schedules for the separate recurrence days cannot overlap.

Task	Steps
	1. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, select the recurrence days. 2. In the **Start time** drop-down list, click the appropriate option. If necessary, set the start time and end time. 3. Click the **Add** icon.

5. On the **System throttling** tab, in the **Maximum number of simultaneous tasks per BlackBerry Administration Service instance** field, type the maximum number of tasks that you want the BlackBerry Enterprise Server to process at the same time.

   The default value is 1000.

6. On the **Job throttling** tab, to turn on throttling for all IT policy tasks in jobs, select **Enabled to reduce load on system**.
7. If necessary, in the **Default throttling for all IT policy tasks in each job in a time window** section, in the **Maximum number of simultaneous tasks per BlackBerry Administration Service instance** field, type the maximum number of IT policy tasks that you want the BlackBerry Enterprise Server to process at the same time.

   The default value is 25.

8. If necessary, in the **Total number of tasks per time window per BlackBerry Administration Service instance** field, type the total number of IT policy tasks that you want the BlackBerry Enterprise Server to process during each processing interval.

   The default value is 150.

9. Click **Save all**.

Change how to install, update, or remove BlackBerry Java Applications

You can change the settings that the BlackBerry Administration Service uses to install and update BlackBerry Java Applications on BlackBerry devices, and remove BlackBerry Java Applications on BlackBerry devices. If you change the default application distribution settings, your organization's environment might experience a performance impact.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Specify application distribution settings**.
3. Click **Edit distribution settings**.
4. Perform any of the following tasks:

Task	Steps
Change the default recurrence day for installing, upgrading, or removing BlackBerry Java Applications.	1. Click the **Edit** icon for the default recurrence day. 2. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, select the recurrence days. 3. In the **Start time** drop-down list, click the appropriate option. If necessary, change the start time and end time. 4. Click the **Update** icon. By default, the recurrence day is Every day and the start time is All day.
Add a new recurrence day for installing, upgrading, or removing BlackBerry Java Applications.	If you want to add more than one recurrence day, the schedules for the separate recurrence days cannot overlap. 1. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, select the recurrence days. 2. In the **Start time** drop-down list, click the appropriate option. If necessary, change the start time and end time. 3. Click the **Add** icon.

5. On the **System throttling** tab, in the **Maximum number of simultaneous tasks per BlackBerry Administration Service instance** field, type the maximum number of tasks that you want the BlackBerry Enterprise Server to process at the same time.

   The default value is 1000.

6. On the **Job throttling** tab, to turn on throttling for all application tasks in jobs, select **Enabled to reduce load on system**.
7. If necessary, in the **Default throttling for all application tasks in each job in a time window** section, in the **Maximum number of simultaneous tasks per BlackBerry Administration Service instance** field, type the maximum number of application tasks that you want the BlackBerry Enterprise Server to process simultaneously.

   The default value is 25.

8. If necessary, in the **Total number of tasks per time window per BlackBerry Administration Service instance** field, type the total number of application tasks that you want the BlackBerry Enterprise Server to process during each processing interval.

   The default value is 150.

9. Click **Save all**.

Change how to install or update the BlackBerry Device Software

You can change the settings that the BlackBerry Administration Service uses to install or upgrade the BlackBerry Device Software on BlackBerry devices. If you change the default distribution settings for the BlackBerry Device Software, your organization's environment might experience a performance impact.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Specify BlackBerry Device Software distribution settings**.
3. Click **Edit distribution settings**.
4. Perform any of the following tasks:

Task	Steps
Change the recurrence day for installing, updating, or removing the BlackBerry Device Software.	1. Click the **Edit** icon for the recurrence day. 2. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, select the recurrence days. 3. In the **Start time** drop-down list, click the appropriate option. If necessary, change the start time and end time. 4. Click the **Update** icon. By default, the recurrence day is Every day and the start time is All day.
Add a recurrence day for installing, updating, or removing the BlackBerry Device Software.	To add more than one recurrence day, the schedules for the separate recurrence days cannot overlap. 1. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, select the recurrence days. 2. In the **Start time** drop-down list, click the appropriate option. If necessary, change the start time and end time. 3. Click the **Add** icon.

5. On the **System throttling** tab, in the **Maximum number of simultaneous tasks per BlackBerry Administration Service instance** field, type the maximum number of BlackBerry Device Software tasks that you want the BlackBerry Enterprise Server to process at the same time.

   The default value is 1000.

6. On the **Job throttling** tab, to turn on throttling for all BlackBerry Device Software tasks in jobs, select **Enabled to reduce load on system**.
7. If necessary, in the **Default throttling for all BlackBerry Device Software tasks in each job in a time window** section, in the **Maximum number of simultaneous tasks per BlackBerry Administration Service instance** field, type the

maximum number of BlackBerry Device Software tasks that you want the BlackBerry Enterprise Server to process at the same time.

The default value is 25.

8. If necessary, in the **Total number of tasks per time window per BlackBerry Administration Service instance** field, type the total number of BlackBerry Device Software tasks that you want the BlackBerry Enterprise Server to process during each processing interval.

   The default value is 150.

9. Click **Save all**.

Change how the BlackBerry Enterprise Server sends standard application settings to BlackBerry devices

BlackBerry Device Software configurations include standard application settings that you can use to control calendar, email, and contact list settings on BlackBerry devices. You can change how the BlackBerry Enterprise Server sends the settings to and updates the settings on BlackBerry devices. If you change the default distribution settings for the standard application settings, your organization's environment might experience a performance impact.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Specify BlackBerry Device Software application distribution settings**.
3. Click **Edit distribution settings**.
4. Perform any of the following tasks:

Task	Steps
Change the recurrence day for sending or updating standard application settings.	1. Click the **Edit** icon for the default recurrence day. 2. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, click the recurrence days. 3. In the **Start time** drop-down list, click the appropriate recurrence option. If necessary, change the start time and end time. 4. Click the **Update** icon. By default, the recurrence day is Every day and the start time is All day.
Add a recurrence day for sending or updating standard application settings.	To add more than one recurrence day, the schedules for the separate recurrence days cannot overlap. 1. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, click the recurrence days. 2. In the **Start time** drop-down list, click the appropriate recurrence option. If necessary, change the start time and end time.

Task	Steps
	3. Click the **Add** icon.

5. On the **System throttling** tab, in the **Maximum number of simultaneous tasks per BlackBerry Administration Service instance** field, type the maximum number of tasks that you want the BlackBerry Enterprise Server to process at the same time.

   The default value is 1000.

6. On the **Job throttling** tab, to turn on throttling for all tasks for standard application settings in jobs, click **Enabled to reduce load on system**.
7. If necessary, in the **Default throttling for all BlackBerry Device Software application settings tasks in each job in a time window** section, in the **Maximum number of simultaneous tasks per BlackBerry Administration Service instance** field, type the maximum number of tasks for standard application settings that you want the BlackBerry Enterprise Server to process at the same time.

   The default value is 25.

8. If necessary, in the **Total number of tasks per time window per BlackBerry Administration Service instance** field, type the total number of tasks for standard application settings that you want the BlackBerry Enterprise Server to process during each processing interval.

   The default value is 150.

9. Click **Save all**.

Managing the distribution settings for a specific job

When you create a software configuration and assign it to user accounts, change a software configuration that you assigned to user accounts, or assign or change an IT policy, the BlackBerry Administration Service creates jobs to deliver the resulting objects or settings to BlackBerry devices. Before the BlackBerry Administration Service delivers a specific job, you can change the delivery schedule of the job, priority of the job, and how the job delivers IT policies, BlackBerry Java Applications, BlackBerry Device Software, and standard application settings to BlackBerry devices.

If you do not change the schedule, priority, or distribution settings for a job, the job uses the default schedule and distribution settings that you configure in the BlackBerry Administration Service.

Specify the start time and priority for a job

If a job has not started running, you can specify when you want the job to start. If you do not specify the start time for a job, the job starts according to the distribution settings that you configured in the BlackBerry Administration Service. You can also change the priority of a job. By default, all jobs have a medium priority. If you change the priority of a job to low, the BlackBerry Enterprise Server processes it after the jobs with a medium or high priority. The BlackBerry Enterprise Server processes jobs with a high priority before it processes jobs with a medium or low priority.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Manage deployment jobs**.
3. Search for the job that you want to change.
4. In the search results, click the ID of the job that you want to change.
5. Click **Edit job**.
6. In the **Priority** drop-down list, click the appropriate priority for the job.
7. In the **Job Schedule** section, in the **Effective Date** field, select the start date for the job.
8. Click **Save all**.

Change how a job sends IT policies to BlackBerry devices

You can change how the BlackBerry Administration Service sends IT policy settings and changes in a specific job to BlackBerry devices. You can change a job's distribution settings for IT policies only if the job is not running. If you changing the IT policy distribution settings for a job, your organization's environment might experience a performance impact.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Manage deployment jobs**.
3. Search for the job that you want to change.
4. In the search results, click the ID of the job that you want to change.
5. Click **Edit job**.
6. On the **IT Policy Distribution** tab, perform any of the following tasks:

Task	Steps
Change the default recurrence day for sending IT policy changes.	1. Click the **Edit** icon for the default recurrence day.

Task	Steps
	2. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, select the recurrence days. 3. In the **Start time** drop-down list, click the appropriate option. If necessary, change the start time and end time. 4. Click the **Update** icon. By default, the recurrence day is Every day and the start time is All day.
Add a new recurrence day for sending IT policy changes.	If you want to add more than one recurrence day for sending IT policy changes, the schedules for the separate recurrence days cannot overlap. 1. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, select the recurrence days. 2. In the **Start time** drop-down list, click the appropriate option. If necessary, change the start time and end time. 3. Click the **Add** icon.

7. To turn on throttling for all IT policy tasks in the job, in the **Default throttling enablement for all IT policy tasks in each job in a time window** section, select **Enabled to reduce load on system**.
8. If necessary, in the **Default throttling for all IT policy tasks in each job in a time window** section, in the **Maximum number of simultaneous tasks per BlackBerry Administration Service instance** field, type the maximum number of IT policy tasks in the job that you want the BlackBerry Enterprise Server to process at the same time.

   The default value is 25.
9. If necessary, in the **Total number of tasks per time window per BlackBerry Administration Service instance** field, type the total number of IT policy tasks in the job that you want the BlackBerry Enterprise Server to process during each processing interval.

   The default value is 150.
10. Click **Save all**.

Change how a job sends BlackBerry Java Applications to BlackBerry devices

You can change how the BlackBerry Administration Service installs, updates, or removes the BlackBerry Java Applications in a specific job on BlackBerry devices. You can change a job's distribution settings for applications only if the job is not running. If you change the default application distribution settings, your organization's environment might experience a performance impact.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.

2. Click **Manage deployment jobs**.
3. Search for the job that you want to change.
4. In the search results, click the ID of the job that you want to change.
5. Click **Edit job**.
6. On the **Application Distribution** tab, perform any of the following tasks:

Task	Steps
Change the default recurrence day for installing, upgrading, or removing BlackBerry Java Applications.	1. Click the **Edit** icon for the default recurrence day. 2. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, select the recurrence days. 3. In the **Start time** drop-down list, click the appropriate option. If necessary, change the start time and end time. 4. Click the **Update** icon. By default, the recurrence day is Every day and the start time is All day.
Add a new recurrence day for installing, upgrading, or removing BlackBerry Java Applications.	If you want to add more than one recurrence day, the schedules for the separate recurrence days cannot overlap. 1. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, select the recurrence days. 2. In the **Start time** drop-down list, click the appropriate option. If necessary, change the start time and end time. 3. Click the **Add** icon.

7. To turn on throttling for all application tasks in the job, on the **Default throttling enablement for all application tasks in each job in a time window** section, select **Enabled to reduce load on system**.
8. If necessary, in the **Default throttling for all application tasks in each job in a time window** section, in the **Maximum number of simultaneous tasks per BlackBerry Administration Service instance** field, type the maximum number of application tasks in the job that you want the BlackBerry Enterprise Server to process at the same time.

   The default value is 25.
9. If necessary, in the **Total number of tasks per time window per BlackBerry Administration Service instance** field, type the total number of application tasks in the job that you want the BlackBerry Enterprise Server to process during each processing interval.

   The default value is 150.
10. Click **Save all**.

Change how a job sends the BlackBerry Device Software to BlackBerry devices

You can change how the BlackBerry Administration Service installs or updates the BlackBerry Device Software in a specific job on BlackBerry devices. You can change the distribution settings for a job for the BlackBerry Device Software only if the job is not running. If you change the default distribution settings for BlackBerry Device Software, your organization's environment might experience a performance impact.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Manage deployment jobs**.
3. Search for a job.
4. In the search results, click the ID of the appropriate job.
5. Click **Edit job**.
6. On the **BlackBerry Device Software Distribution** tab, perform any of the following tasks:

Task	Steps
Change the recurrence day for installing, updating, or removing BlackBerry Device Software.	1. Click the **Edit** icon for the recurrence day. 2. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, click the number of recurrence days. 3. In the **Start time** drop-down list, click the appropriate option. If necessary, change the start time and end time. 4. Click the **Update** icon. By default, the recurrence day is Every day and the start time is All day.
Add a new recurrence day for installing, updating, or removing BlackBerry Device Software.	To add more than one recurrence day, the schedules for the separate recurrence days cannot overlap. 1. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, click the recurrence days. 2. In the **Start time** drop-down list, click the appropriate recurrence option. If necessary, change the start time and end time. 3. Click the **Add** icon.

7. To turn on throttling for all BlackBerry Device Software tasks in jobs, in the **Default throttling enablement for all BlackBerry Device Software tasks in each job in a time window** section, click **Enabled to reduce load on system**.

8. If necessary, in the **Default throttling for all BlackBerry Device Software tasks in each job in a time window** section, in the **Maximum number of simultaneous tasks per BlackBerry Administration Service instance** field, type the maximum number of BlackBerry Device Software tasks in the job that you want the BlackBerry Enterprise Server to process at the same time.

   The default value is 25.

9. If necessary, in the **Total number of tasks per time window per BlackBerry Administration Service instance** field, type the total number of BlackBerry Device Software tasks in the job that you want the BlackBerry Enterprise Server to process during each processing interval.

   The default value is 150.

10. Click **Save all**.

Change how a job sends standard application settings to BlackBerry devices

BlackBerry Device Software configurations include standard application settings that you can use to control calendar, email, and contact list settings on BlackBerry devices. You can change how the BlackBerry Administration Service sends settings and updates in jobs to BlackBerry devices. If you change the default distribution settings for the standard application settings in BlackBerry Device Software configurations, your organization's environment might experience a performance impact.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Manage deployment jobs**.
3. Search for a job.
4. In the search results, click the ID of the appropriate job.
5. Click **Edit job**.
6. On the **BlackBerry Device Software Application Settings Distribution** tab, perform any of the following tasks:

Task	Steps
Change the recurrence day for sending or updating standard application settings.	1. Click the **Edit** icon for the recurrence day. 2. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, select the number of recurrence days. 3. In the **Start time** drop-down list, click the appropriate recurrence option. If necessary, change the start time and end time. 4. Click the **Update** icon. By default, the recurrence day is Every day and the start time is All day.

Task	Steps
Add a recurrence day for sending or updating standard application settings.	To add more than one recurrence day, the schedules for the separate recurrence days cannot overlap. 1. In the **Scheduled deployment day(s)** drop-down list, click the appropriate recurrence option. If necessary, click the recurrence days. 2. In the **Start time** drop-down list, click the appropriate recurrence option. If necessary, change the start time and end time. 3. Click the **Add** icon.

7. To turn on throttling for all tasks for standard application settings in the job, in the **Default throttling enablement for all BlackBerry Device Software application tasks in each job in a time window** section, click **Enabled to reduce load on system**.
8. If necessary, in the **Default throttling for all BlackBerry Device Software Application Settings tasks in each job in a time window** section, in the **Maximum number of simultaneous tasks per BlackBerry Administration Service instance** field, type the maximum number of tasks for standard application settings in the job that you want the BlackBerry Enterprise Server to process at the same time.

   The default value is 25.
9. If necessary, in the **Total number of tasks per time window per BlackBerry Administration Service instance** field, type the total number of tasks for standard application settings in the job that you want the BlackBerry Enterprise Server to process during each processing interval.

   The default value is 150.
10. Click **Save all**.

Managing BlackBerry Java Applications on BlackBerry devices

Make a BlackBerry Java Application unavailable for installation

You can delete a BlackBerry Java Application and all versions of the application from the application repository if you do not want to make the BlackBerry Java Application available to add to software configurations. You cannot delete a

BlackBerry Java Application from the application repository if the BlackBerry Java Application is in a software configuration.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software** > **Applications**.
2. Click **Manage applications**.
3. Search for a BlackBerry Java Application.
4. In the search results, click the name of the application.
5. Click **Delete application**.
6. Click **Yes - Delete the application and all application versions**.

Remove a BlackBerry Java Application from BlackBerry devices over the wireless network

You can remove a BlackBerry Java Application, the collaboration client, or the BlackBerry MDS Runtime from BlackBerry devices over the wireless network.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software**.
2. Click **Manage software configurations**.
3. Click a software configuration.
4. Click **Edit software configuration**.
5. On the **Applications** tab, click the **Delete** icon for the application.
6. Perform one of the following actions:
   - If you configured the software configuration to permit unlisted applications on BlackBerry devices and you want to permit users to install the application as an unlisted application, or if you configured the software configuration to not permit unlisted applications on BlackBerry devices, click **Save all**.
   - If you configured the software configuration to permit unlisted applications on BlackBerry devices, and you do not want to permit users to install the application on their BlackBerry devices, perform steps 7 to 12.
7. Click **Add applications to software configuration**.
8. Search for the application that you want to remove.
9. In the search results, select the application.
10. In the **Disposition** drop-down list for the application, click **Disallowed**.
11. Click **Add to software configuration**.
12. Click **Save all**.

Managing software configurations

Remove a software configuration from a group

If you remove a software configuration from a group, the applications in the software configuration are removed from the BlackBerry devices that are associated with the user accounts that belong to the group.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. Click a group.
4. Click **Edit group**.
5. On the **Software configuration** tab, in the **Current software configurations** list, click a software configuration.
6. Click **Remove**.
7. Repeat steps 5 and 6 for each software configuration you want to remove.
8. Click **Save all**.

Remove a software configuration from multiple user accounts

If you remove a software configuration from multiple user accounts, the applications in the software configuration are removed from the BlackBerry devices that are associated with the user accounts.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for one or more user accounts.
4. Select one or more user accounts.
5. In the **Remove from user configuration** list, click **Remove software configuration**.
6. In the **Available software configurations** list, click a software configuration.
7. Click **Remove**.
8. Repeat steps 6 and 7 for each software configuration that you want to remove from the user accounts.

9. Click **Save**.

Remove a software configuration from a user account

If you remove a software configuration from a user account, the applications in the software configuration are removed from the BlackBerry device associated with the user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for one or more user accounts.
4. In the search results, click the display name for a user account.
5. Click **Edit user**.
6. On the **Software configuration** tab, in the **Current software configurations** list, click a software configuration.
7. Click **Remove**.
8. Repeat steps 6 and 7 for each software configuration that you want to remove.
9. Click **Save all**.

Delete a software configuration

You can delete a software configuration that is not assigned to a user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Software**.
2. Click **Manage software configurations**.
3. Click a software configuration.
4. Click **Delete software configuration**.
5. Click **Yes - Delete the software configuration**.

Managing how users access enterprise applications and web content

27

Restricting user access to content on web servers

You can prevent BlackBerry device users from accessing specific web servers using the BlackBerry Browser or applications on BlackBerry devices. To specify the web servers that you want users to access, you can turn on pull authorization to restrict access to all types of web content and create pull rules to specify a list of web servers that you permit users to access. Alternatively, you can create pull rules that specify a list of restricted web servers.

When you create pull rules, you can specify whether users must authenticate using RSA authentication, integrated Windows authentication, or both before the users can access the web servers.

Restrict requests for content on web servers from BlackBerry devices

Turn on pull authorization for a BlackBerry MDS Connection Service to restrict the web addresses that users assigned to that BlackBerry MDS Connection Service can request when the users connect to the Internet or to your organization's intranet from their BlackBerry devices.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. In the **Access control** section, in the **Pull authorization** drop-down list, click **Yes**.

5. Click **Save all**.

Users cannot access web content on their BlackBerry devices until you permit the users to access specific web servers using pull rules.

After you finish: To permit users to access specific web servers, specify allowed web address patterns and assign the web address patterns to a pull rule, and assign the pull rule to a user account or group.

Specify web address patterns

You can create pull rules that specify which web address patterns users can and cannot use to access web servers from the BlackBerry Browser and other applications on their BlackBerry devices. To create a pull rule, you must first specify web address patterns (for example, specify addresses with domains that are allowed). You can assign the web address patterns to a pull rule that you create, and specify whether access to web servers that match the web address patterns is permitted or restricted on BlackBerry devices. After you create a pull rule, you must assign it to user accounts or groups.

A web site that uses DNS load balancing returns a single IP address to the BlackBerry MDS Connection Service but might use multiple IP addresses to provide access to the web site. As a result, the BlackBerry MDS Connection Service might not be able to restrict BlackBerry devices from accessing the web site.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **Pull URL patterns** tab, in the appropriate protocol section, type the web address pattern of a web server that you want to control access to. The web address patterns are based on Java regular expressions (for example, **.*\..*domain.***).
5. Click the **Add** icon.
6. Click **Save all**.

After you finish: Create web address patterns for each web server that you want to permit users to access. Create a pull rule that permits users to access the web servers that match the web address patterns.

Create a pull rule

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **Access control rules** tab, in the **Rule name** field, type a name for the pull rule.

5. In the **Control type** drop-down list, click **Pull**.
6. Click the **Add** icon.
7. Click **Save all**.

After you finish: Restrict or permit web address patterns using a pull rule.

Restrict or permit web addresses and Intranet addresses using a pull rule

Before you begin:

- Create a pull rule.
- If you want BlackBerry device users to use RSA authentication to access web servers, configure the BlackBerry MDS Connection Service to authenticate BlackBerry devices to the RSA Authentication Manager.
- If you want users to use integrated Windows authentication when they access the web servers, configure the BlackBerry MDS Connection Service to authenticate devices to Microsoft Active Directory.

A web site that uses DNS load balancing returns a single IP address to the BlackBerry MDS Connection Service but might use multiple IP addresses to provide access to the web site. As a result, the BlackBerry MDS Connection Service might not be able to restrict BlackBerry devices from accessing the web site.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **Access control rules** tab, click the **Edit** icon for a pull rule.
5. In the **URL pattern group** drop-down list, click the protocol for the address that you want to assign to the pull rule.
6. In the **URL pattern** drop-down list, click the address that you want to assign to the pull rule.
7. In the **Allowed** drop-down list, perform one of the following actions:
    - To prevent users from accessing web servers that match the address, click **Deny**.
    - To permit users to access web servers that match a specific address, click **Allow**.
8. If necessary, in the **Authentication** drop-down list, perform one of the following actions:
    - To require that a user enter authentication credentials to access content on a web site, click **Access control rules only**. The device user is not prompted to enter authentication credentials if they are not required by the web site.
    - To require that the BlackBerry MDS Connection Service authenticates a user using integrated Windows authentication, click **Integrated**.

- To require that a user authenticates to the RSA Authentication Manager using RSA authentication, click **RSA**.
- To require that the BlackBerry MDS Connection Service authenticates the user using integrated Windows authentication and that a user authenticates to the RSA Authentication Manager using RSA authentication, click **Integrated and RSA**.

9. Click the **Add** icon.
10. Repeat steps 5 to 8 for each address that you want to assign to the pull rule.
11. Click **Save all**.

After you finish: Assign the pull rule to a group or user account.

Assign a pull rule to the members of a group

Before you begin: Create a pull rule. Assign web address patterns to the pull rule.

1. In the BlackBerry Administration Service, in the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Click **View more criteria**.
4. Search for a group.
5. Click **Select all results in the entire set**.
6. In the **Add to user configuration** list, click **Add pull rule**.
7. In the **Available pull rules** list, click a pull rule.
8. Click **Add**.
9. Click **Save**.

Assign a pull rule to user accounts

Before you begin: Create a pull rule. Assign web address patterns to the pull rule.

1. In the BlackBerry Administration Service, in the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for one or more user accounts.
4. Select the appropriate user accounts.
5. In the **Add to user configuration** list, click **Add pull rule**.
6. In the **Available pull rules** list, click a pull rule.

7. Click **Add**.
8. Click **Save**.

Restricting user access to media content in the BlackBerry Browser

You can use standard definitions for MIME media types so that you can restrict the media types that the BlackBerry MDS Connection Service can send to the BlackBerry Browser and other applications on BlackBerry devices.

For more information about MIME media types, visit www.iana.org.

Prevent users from accessing specific media types

You can configure the BlackBerry MDS Connection Service instances in your organization's environment to prevent users from accessing every format of a media type (for example, video), or a specific format of a media type (for example, .mp3), using the BlackBerry Browser and other applications on a BlackBerry device.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. In the **Media content type** field, type the media type and subtype using standard definitions for MIME media types. Use the format *<type>/<subtype>*.
5. In the **Disallow content** drop-down list, click **Yes**.
6. Click the **Add** icon.
7. Click **Save all**.

Configure download limits for media content types

You can configure the BlackBerry MDS Connection Service instances in your organization's environment to limit the size of media content that BlackBerry device users can download to BlackBerry devices during each connection. Each request for data that the device makes to the BlackBerry MDS Connection Service is a connection. If you do not configure a limit for media content types, the default values apply.

Before you begin: For more information about MIME media types, visit www.iana.org/assignments/media-types.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. In the **Media content type** field, type the media type and subtype using standard definitions for MIME media types. Use the format *<type>/<subtype>*. You can substitute an asterisk (*) to represent all types or subtypes except for the types you have already configured. Some examples of entries for the **Media content type** field include application/msword, application/pdf, video/mpeg, application/*, image/*, */*.
5. In the **Maximum KB/Connection** field, type the maximum size (in KB) of content that a user can download to the device, during each connection to the BlackBerry MDS Connection Service.
6. In the **Disallow content** drop-down list, click **No**.
7. Click the **Add** icon.
8. Click **Save all**.

Related information

Default download limits for media content types, 313

Default download limits for media content types

BlackBerry device users can only download a specific amount of media content to BlackBerry devices with each connection. You can configure a limit in the BlackBerry Administration Service. If you do not configure a limit, the default limit applies. The following table lists the default values.

There is no limit for the amount of media content that users can download using HTTP POST.

MIME type	Maximum number of bytes per connection (KB)
application/msword	2048
application/pdf	2048
application/vnd.ms-excel	2048
application/vnd.ms-powerpoint	2048
application/vnd.oma.drm.message	5120
application/vnd.oma.dm.message	5120
multimedia types such as audio and video	32,768
other	2048

Related information

Configure download limits for media content types, 312

Configuring Integrated Windows authentication so that users can access resources on your organization's network

To permit BlackBerry device users to access resources on your organization's network using BlackBerry devices without requiring the users to type a user name and password each time they access the network resources, you can configure the BlackBerry MDS Connection Service to support Integrated Windows authentication. Users can then access network resources such as intranet sites and network shared folders on their devices using the BlackBerry Browser or Files application without typing a user name and password.

Before you configure the BlackBerry MDS Connection Service to support Integrated Windows authentication, you must create a Microsoft Active Directory account in each Microsoft Active Directory domain that includes resources that you want to turn on Integrated Windows authentication for. You must configure constrained delegation for the Microsoft Active Directory accounts so that they delegate access to each intranet site or network shared folder in the Microsoft Active Directory domain.

You must also configure two-way trust between the Microsoft Active Directory domain that the BlackBerry MDS Connection Service is running on and other Microsoft Active Directory domains in other forests that the BlackBerry MDS Connection Service must connect to. The S4U2proxy extension that the BlackBerry MDS Connection Service uses to retrieve the Kerberos service tickets for users requires a two-way trust between Microsoft Active Directory domains.

After you turn on Integrated Windows authentication and specify a Microsoft Active Directory account in the BlackBerry Administration Service, you must specify web address patterns for the network resources that you want to permit users to access, create a pull rule for the web address patterns, permit access to the web address patterns using the pull rule, and assign the pull rule to users or a group.

After you configure the BlackBerry MDS Connection Service to support Integrated Windows authentication, the BlackBerry MDS Connection Service uses the Microsoft Active Directory account to verify login information for a user and access the network resources on behalf of the user. The BlackBerry Enterprise Server then sends information from the network resources to the user's device.

Configuring the Microsoft Active Directory account to delegate access

Prerequisites: Configuring the Microsoft Active Directory account to delegate access to an intranet site

- Verify that you configured Integrated Windows authentication for the application server that hosts the intranet site.
- Verify that the application server that hosts the intranet site and the web application that runs on the application server support Kerberos authentication.
- Verify that you have permission to update the Microsoft Active Directory account in Microsoft Active Directory.
- Verify that you have access to the Windows Server setspn tool that is included with the Windows Server Support Tools. For more information about the setspn tool, visit http://technet.microsoft.com to read *Setspn Overview*.
- If you did not configure a Microsoft Active Directory account to delegate access to an intranet site or shared folder, in Microsoft Active Directory, you must create a Microsoft Active Directory account that should have the following conditions:
  - a password that meets the security requirements of your organization
  - the user is not required to change their password the next time that the user logs in
  - the user's password never expires
- If you configured a pool of application servers to host the intranet site, and the pool is running on Microsoft IIS and is located behind a load balancer, specify a user account (also known as the identity) for the pool that hosts the intranet site. For more information, see http://technet.microsoft.com/en-us/library/cc771170(WS.10).aspx.

Configure the Microsoft Active Directory account to delegate access to an intranet site

You are required to have only one Microsoft Active Directory account in each Microsoft Active Directory domain that includes the resources that you want to turn on Integrated Windows authentication for.

For more information about configuring the Microsoft Active Directory account using setspn and Microsoft Active Directory, visit www.blackberry.com/btsc to read article KB22726.

1. If a pool of application servers host a intranet site and the pool is running on Microsoft IIS and is located behind a load-balancer, use setspn or ADSI to add the SPNs of the intranet site to the user account (also known as the identity) of the pool. You must configure the SPNs using the FQDN and the name of the intranet site that users type into their browsers (for example, if users type http://intranet_site in their browsers, the name of the intranet site is intranet_site).

2. In Microsoft Active Directory, in the Microsoft Active Directory account properties, if the **Delegation** tab does not display, update the default HOST SPN registrations for the Microsoft Active Directory account.
3. In the Microsoft Active Directory account properties, on the **Delegation** tab, configure the following settings:
   - trust this user for delegation to specified services only
   - use any authentication protocol
4. Click **Add**.
5. Perform one of the following tasks:
   - If a pool of application servers hosts the intranet site and the pool is running on Microsoft IIS and is located behind a load-balancer, select the user account that runs the application pools in the Microsoft IIS servers.
   - If the intranet site is hosted by one application server, select the application server that hosts the intranet site.
6. Select the HTTP service type for the user account or application server that you specified.
7. Repeat steps 1 to 6 for each intranet site that you want to turn on integrated Windows authentication for.

After you finish:

- If required, configure BlackBerry MDS Connection Service to use a Microsoft Active Directory account when the messaging server is in a remote Microsoft Active Directory domain.
- Turn on Integrated Windows authentication when users access resources on your organization's network.

Prerequisites: Configuring the Microsoft Active Directory account to delegate access to a shared folder

- Verify that you configured Integrated Windows authentication for the file server that hosts the shared folders.
- Verify that you have permission to update the Microsoft Active Directory account in Microsoft Active Directory.
- Verify that you have access to the Windows Server setspn tool that is included with the Windows Server Support Tools. For more information about the setspn tool, visit http://technet.microsoft.com to read *Setspn Overview*.
- If you did not configure a Microsoft Active Directory account to delegate access to an intranet site or shared folder, in Microsoft Active Directory, you must create a Microsoft Active Directory account that should have the following conditions:
  - the password meets the security requirements of your organization
  - the user is not required to change their password the next time that the user logs in
  - the user's password never expires

Configure the Microsoft Active Directory account to delegate access to a shared folder

You are required to have only one Microsoft Active Directory account in each Microsoft Active Directory domain that includes the resources that you want to turn on Integrated Windows authentication for.

For more information about configuring the Microsoft Active Directory account using setspn and Microsoft Active Directory, visit www.blackberry.com/btsc to read article KB22726.

1. In Microsoft Active Directory, in the Microsoft Active Directory account properties, if the **Delegation** tab does not display, update the default HOST SPN registrations for the Microsoft Active Directory account.
2. In the Microsoft Active Directory account properties, on the **Delegation** tab, configure the following settings:
   - trust this user for delegation to specified services only
   - use any authentication protocol
3. Click **Add**.
4. Select the the file server that hosts the shared folder.
5. Select the CIFS service type for the file server that you specified.
6. Repeat steps 3 to 5 for each shared folder that you want to turn on Integrated Windows authentication for.

After you finish:

- If required, configure BlackBerry MDS Connection Service to use a Microsoft Active Directory account when the messaging server is in a remote Microsoft Active Directory domain.
- Turn on Integrated Windows authentication when users access resources on your organization's network.

Configuring the BlackBerry MDS Connection Service when the messaging server is located in a remote Microsoft Active Directory domain

If the computer that hosts the BlackBerry MDS Connection Service is not located in the same Microsoft Active Directory domain as the global catalog server or messaging server and you want to configure support for Integrated Windows authentication, you must create a Microsoft Active Directory account that the BlackBerry MDS Connection Service can use to connect to the global catalog server.

In a Microsoft Exchange environment, you must create the Microsoft Active Directory account in the Microsoft Active Directory domain that includes the messaging server.

In an IBM Lotus Domino environment, if the messaging server is located in the same Microsoft Active Directory domain as the global catalog server, you must create the Microsoft Active Directory account in that domain. If the messaging server is located in a different Microsoft Active Directory domain than the global catalog server, you must create the Microsoft Active Directory account in the Microsoft Active Directory domain that includes the global catalog server.

You do not need to configure constrained delegation for the Microsoft Active Directory account that you create in the Microsoft Active Directory domain that includes the messaging server or global catalog server.

Configure the BlackBerry MDS Connection Service when the messaging server is located in a remote Microsoft Active Directory domain

Before you begin: Create a Microsoft Active Directory account in the Microsoft Active Directory domain that the messaging server or global catalog server is located in.

1. On the computer that hosts the BlackBerry MDS Connection Service, navigate to <*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\MDS\Servers\instance\config .
2. In a text editor, open the **rimpublic.properties** file.
3. In the **rimpublic.properties** file, type **application.handler.exchange.domain**=<***domain_name***> where <*domain_name*> is the Microsoft Active Directory domain that contains the messaging server. For example, type **application.handler.exchange.domain=domain123.example.com**.
4. Save and close the **rimpublic.properties** file.
5. In the Windows Services, restart the BlackBerry MDS Connection Service service.

After you finish: Turn on Integrated Windows authentication when BlackBerry device users access resources on your organization's network.

Related information

Restarting BlackBerry Enterprise Server components, 392

Turn on Integrated Windows authentication so that users can access resources on your organization's network

Before you begin:

- Configure the Microsoft Active Directory account to access resources on your organization's network.
- If required, configure BlackBerry MDS Connection Service to use a Microsoft Active Directory account when the messaging server is in a remote Microsoft Active Directory domain.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.

4. In the **Integrated authentication turned on** drop-down list, click **Yes**.
5. For each Microsoft Active Directory account, provide the following information:
    - In the **Delegation user domain** field, type the FQDN (for example, **ldap.example.com**).
    - In the **Delegation user name** field, type the user name.
    - In the **Password** and **Confirm** fields, type the password.
6. Click **Save all**.
7. On the **HTTP** tab, click **Edit component**.
8. In the **Authentication support enabled** drop-down list, click **Yes**.
9. Click **Save all**.
10. On the **Pull URL Patterns** tab, specify web address patterns for the intranet sites or shared folders that you want to permit BlackBerry device users to access (for example, **intranet_site(:80)?(\/.*)?**). The web address patterns are based on Java regular expressions. Consider specifying the following web address patterns:
    - Specify **.*\:.*\/.*** as the web address pattern so that you can prevent users from using any other web address patterns to access intranet sites or shared network folders.
    - Specify **.*** as the web address pattern for OCSP, LDAP, and TCP to permit users to communicate with OCSP servers, LDAP servers, or TCP servers.
11. On the **Access control rules** tab, create a pull rule for each of the web address patterns that you specified. When you create the pull rule, in the **Authentication** drop-down list, click **Integrated** or **Integrated and RSA**.
12. Click **Save all**.
13. Assign the pull rules to the users or groups that you want to access intranet sites or shared network folders.
14. On the **Servers and components** menu, expand **BlackBerry solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
15. Click a BlackBerry MDS Connection Service instance.
16. Click **Edit instance**.
17. In the **Pull Authorization** drop-down list, click **Yes**.
18. Click **Save all**.
19. Repeat step 16 to 20 for each BlackBerry MDS Connection Service instance.

Related information

Specify web address patterns, 309
Create a pull rule, 309
Assign a pull rule to the members of a group, 311
Assign a pull rule to user accounts, 311
Restrict or permit web addresses and Intranet addresses using a pull rule, 310

Restricting the push application content that users can receive

By default, a BlackBerry MDS Connection Service sends push requests from server-side push applications to applications on BlackBerry devices. BlackBerry devices can receive application data and application updates without users requesting the content.

You can configure your organization's environment so that only specific server-side push applications can send push requests to BlackBerry devices. You can turn on push authentication to prevent a BlackBerry MDS Connection Service from sending push requests, and create push initiators that permit specific server-side applications to send push requests to BlackBerry devices. To permit specific users to receive push requests on BlackBerry devices, you can create push rules and assign the rules to the users.

For more information about push requests, see the *BlackBerry Java Development Environment Development Guide*.

Restrict push applications from sending data to BlackBerry devices

You can turn on push authentication to permit only authenticated push applications to send push requests to applications on BlackBerry devices.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. In the **Access control** section, in the **Push authentication** options, click **Yes**.
5. Click **Save all**.

After you finish: To authenticate and permit specific server-side push applications to send push requests to BlackBerry devices, create push initiators.

Create push initiators for push applications

Push initiators specify which server-side push applications are authenticated and permitted to send push requests to applications on BlackBerry devices. For push initiators to work, you must turn on push authentication for the BlackBerry MDS Connection Service. You can configure several server-side push applications to use the same push initiator (that is, to use the same authorization password) if your organization's development environment permits it. Verify that the authorization HTTP header in push requests from server-side push applications matches the name and password that you specify for the push initiator.

Before you begin: Turn on push authentication for the appropriate instances of the BlackBerry MDS Connection Service.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **Push initiators** tab, in the **Name** field, type the name of the server-side application that you want to permit to send push requests to BlackBerry devices.
5. In the **Credentials** field, type the password for the server-side push application.
6. Click the **Add** icon.
7. Click **Save all**.

After you finish: Create a push initiator for each server-side push application that you want to permit to send push requests to BlackBerry devices. To specify which users can receive push requests from authenticated push applications, turn on push authorization and create push rules.

Turn on push authorization

If you turned on push authentication and created push initiators to specify which push applications can send push requests, you can create push rules to specify which users are permitted to receive authenticated push requests. The BlackBerry MDS Connection Service can apply push rules only if you turn on push authorization for the BlackBerry MDS Connection Service.

Before you begin:

- Turn on push authentication.
- Create push initiators to authenticate specific push applications.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. In the **Access control** section, in the **Push authorization** drop-down list, click **Yes**.
5. Click **Save all**.

After you finish: Create a push rule.

Related information

Restrict push applications from sending data to BlackBerry devices, 320

Create a push rule

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **Access control rules** tab, in the **Rule name** field, type a name for the push rule.
5. In the **Control type** drop-down list, click **Push**.
6. Click the **Add** icon.
7. Click **Save all**.

After you finish: Assign push initiators to the push rule.

Assign push initiators to a push rule

Before you begin: Create push initiators to authenticate specific push applications.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **Access control rules** tab, click the **Edit** icon for a push rule.
5. In the **Available push initiators** list, click the push initiator that you want to assign to the push rule.
6. Click **Add**.
7. Repeat steps 5 and 6 for each push initiator that you want to assign to the push rule.
8. Click **Save all**.

After you finish: Assign the push rule to a user account or to a group.

Related information

Create push initiators for push applications, 320

Assign a push rule to the members of a group

Before you begin:

- Create a push rule.
- Assign push initiators to the push rule.

1. In the BlackBerry Administration Service, in the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Click **View more criteria**.
4. Search for a group.
5. Click **Select all results in the entire set**.
6. In the **Add to user configuration** list, click **Add push rule**.
7. In the **Available push rules** list, click a push rule.
8. Click **Add**.
9. Click **Save**.

Assign a push rule to user accounts

Before you begin:

- Create a push rule.
- Assign push initiators to the push rule.

1. In the BlackBerry Administration Service, in the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for one or more user accounts.
4. Select the user accounts that you want to assign a push rule to.
5. In the **Add to user configuration** list, click **Add push rule**.
6. In the **Available push rules** list, click a push rule.
7. Click **Add**.
8. Click **Save**.

Encrypt push requests that push applications send to BlackBerry devices

You can configure a BlackBerry MDS Connection Service to use SSL or TLS to encrypt the push requests that server-side push applications send to BlackBerry devices. By default, the BlackBerry MDS Connection Service does not encrypt the push requests that server-side push applications send.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. In the **Access control** section, in the **Push encryption** drop-down list, click **Yes**.
5. Click **Save all**.

Managing push application requests

The BlackBerry MDS Connection Service receives push application requests from server-side push applications and sends the requests to applications on BlackBerry devices. You can control how the BlackBerry MDS Connection Service processes, stores, and sends push application requests.

For more information about types of push requests, visit www.blackberry.com/developers to see the *BlackBerry Java Development Environment Development Guide*.

Specify device ports for application-reliable push requests

Application developers can create BlackBerry Java Applications to manage application-reliable push requests. When a BlackBerry Java Application receives an application-reliable push request, it sends a delivery confirmation message to the BlackBerry MDS Connection Service, which sends the message to the server-side push application. You must specify the device port numbers that the BlackBerry Java Applications listen on for application-reliable push requests.

Before you begin: Contact your organization's application developers for the unique port numbers that they defined for BlackBerry Java Applications that support application-reliable push requests.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.

2. Click the instance that you want to specify device ports for.
3. Click **Edit instance**.
4. In the **Device ports enabled for reliable pushes** field, type the device port number.
5. Click the **Add** icon.
6. Repeat steps 4 to 5 for each device port number that you want to add.
7. Click **Save all**.
8. Click **Restart instance**.

Related information
Restarting BlackBerry Enterprise Server components, 392

Store push application requests in the BlackBerry Configuration Database

To manage memory and system resources in your organization's environment, you can configure a BlackBerry MDS Connection Service to store PAP and Research In Motion push requests in the BlackBerry Configuration Database. You can also configure storage settings for the BlackBerry Configuration Database. For more information about types of push requests, visit www.blackberry.com/developers to see the *BlackBerry Java Development Environment Development Guide*.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. In the **Push access protocol** section, in the **Store push submissions** drop-down list, click **Yes**.
5. Click **Save all**.
6. Click **Restart instance**.

After you finish: Configure the settings for storing push requests in the BlackBerry Configuration Database.

Related information
Restarting BlackBerry Enterprise Server components, 392

Configure the settings for storing push requests in the BlackBerry Configuration Database

To manage your organization's system resources, you can configure storage settings for push requests that are stored in the BlackBerry Configuration Database.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. In the **Push message settings** section, in the **Maximum number of push messages stored** field, type the number of push requests that you want the BlackBerry Configuration Database to store.
5. In the **Maximum push message age** field, type the maximum length of time, in minutes, that you want the BlackBerry Configuration Database to store a push request before the BlackBerry Enterprise Server deletes it from the BlackBerry Configuration Database.
6. Click **Save all**.

Configure the maximum number of active connections that a BlackBerry MDS Connection Service can process

You can configure the maximum number of push connections that a BlackBerry MDS Connection Service can process at the same time. The BlackBerry MDS Connection Service queues the push connections that exceed this limit.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to configure active connections for.
3. Click **Edit instance**.
4. In the **Push access protocol** section, in the **Maximum number of active connections** field, type a number.
5. Click **Save all**.
6. Click **Restart instance**.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configure the maximum number of queued connections that a BlackBerry MDS Connection Service can process

The BlackBerry MDS Connection Service queues push connections when the number of connections exceeds a limit that you specify. You can configure the maximum number of push connections that a BlackBerry MDS Connection Service can queue. The BlackBerry MDS Connection Service sends a "service unavailable" message to BlackBerry devices when the number of pending push connections in the queue exceeds the limit.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click the instance that you want to configure the maximum number of queued connections for.
3. Click **Edit instance**.
4. In the **Push access protocol** section, in the **Maximum number of queued connections** field, type a number.
5. Click **Save all**.
6. Click **Restart instance**.

Related information

Restarting BlackBerry Enterprise Server components, 392

Managing organizer data synchronization

28

Managing the wireless backup and recovery of organizer data

The wireless backup feature backs up user account settings and data from BlackBerry devices to the BlackBerry Enterprise Server automatically. You can use the wireless backup feature to synchronize organizer data to BlackBerry devices without affecting the performance of your organization's messaging server. You can also use the wireless backup feature to restore data from the BlackBerry Enterprise Server to the BlackBerry device. By default, wireless backup is turned on when you activate BlackBerry devices.

Turn off the wireless backup of organizer data for a user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Organizer data synchronization** tab, in the **General** section, in the **Automatic wireless backup turned on** drop-down list, click **No**.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Delete organizer data for members of a user group from the BlackBerry Enterprise Server

If the BlackBerry Enterprise Server is not writing organizer data for members of a user group from their BlackBerry devices to the BlackBerry Configuration Database correctly, the organizer data on the BlackBerry Enterprise Server might be corrupted. You can delete the organizer data from the BlackBerry Enterprise Server. This action forces the BlackBerry devices to synchronize the current organizer data with the BlackBerry Enterprise Server over the wireless network.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Click **View more criteria**.
4. In the **Group criteria** section, in the **Specific group** drop-down list, click the appropriate group.
5. Click **Search**.
6. Select all users.
7. In the **Organizer data synchronization** list, click **Clear backed up data for organizer data synchronization**.

Delete a user's organizer data from a BlackBerry Enterprise Server

If the BlackBerry Enterprise Server writes a user’s organizer data from a BlackBerry device to the BlackBerry Configuration Database incorrectly, the organizer data on the BlackBerry Enterprise Server might become corrupt. In this case, you can delete the organizer data from the BlackBerry Enterprise Server.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for one or more user accounts.
4. Select the checkboxes beside the display names of the appropriate user accounts.
5. In the **Organizer data synchronization** list, click **Clear backed up data for organizer data synchronization**.

Turning off organizer data synchronization

Turn off organizer data synchronization for all user accounts that are associated with a BlackBerry Enterprise Server

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Synchronization**.
2. Click the instance that you want to change.
3. In the **Instance information** section, click **Synchronization**.
4. Click **Edit component**.
5. In the **Synchronization turned on** drop-down list, click **False** for each type of organizer data.
6. Click **Save all**.

Turn off organizer data synchronization for a specific user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Organizer data synchronization** tab, in the **General** section, perform one of the following actions:
   - To prevent the synchronization of organizer data, in the **General** section, in the **Turn on wireless synchronization** drop-down list, click **No**.
   - To prevent the synchronization of specific types of organizer data, in the **General** section, in the **Turn on wireless synchronization** drop-down list, click **Yes**. In the **Turn on synchronization** drop-down list, click **No** for each type of organizer data that you do not want to synchronize.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Changing how organizer data synchronizes

Change the direction of organizer data synchronization for all user accounts on a BlackBerry Enterprise Server

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Synchronization**.
2. Click the instance that you want to change.
3. In the **Instance information** section, click **Synchronization**.
4. Click **Edit component**.
5. For each type of organizer data, in the **Synchronization type** drop-down list, perform one of the following actions:
   - To synchronize data from the BlackBerry Enterprise Server to the BlackBerry device only, click **Server to Device**.
   - To synchronize data from the BlackBerry device to the BlackBerry Enterprise Server only, click **Device to Server**.
   - To synchronize data from the BlackBerry device to the BlackBerry Enterprise Server and from the BlackBerry Enterprise Server to the BlackBerry device, click **Bidirectional**.
6. Click **Save all**.

Change the direction of organizer data synchronization for a specific user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name of the user account.
5. Click **Edit user**.
6. In the **Message configuration** section, click **Default configuration**.

7. On the **Organizer data synchronization** tab, for each type of organizer data, in the **Synchronization type** drop-down list, perform one of the following actions:
    - To synchronize data from the BlackBerry Enterprise Server to the BlackBerry device only, click **Server to Device**.
    - To synchronize data from the BlackBerry device to the BlackBerry Enterprise Server only, click **Device to Server**.
    - To synchronize data from the BlackBerry device to the BlackBerry Enterprise Server and from the BlackBerry Enterprise Server to the BlackBerry device, click **Bidirectional**.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Change how the BlackBerry Administration Service resolves conflicts during organizer data synchronization for all user accounts on a BlackBerry Enterprise Server

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Synchronization**.
2. Click the instance that you want to change.
3. In the **Instance information** section, click **Synchronization**.
4. Click **Edit component**.
5. In the **Conflict resolution** drop-down list, perform one of the following actions for each type of organizer data:
    - To specify that the BlackBerry Enterprise Server data overrides the BlackBerry device data, click **Server Wins**.
    - To specify that the BlackBerry device data overrides the BlackBerry Enterprise Server data, click **Device Wins**.
6. Click **Save all**.

Change how the BlackBerry Administration Service resolves conflicts during organizer data synchronization for a specific user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.

2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Organizer data synchronization** tab, for each type of organizer data, in the **Conflict resolution drop-down** list, perform one of the following actions:
   - To specify that the BlackBerry Enterprise Server data overrides the BlackBerry device data, click **Server Wins**.
   - To specify that the BlackBerry device data overrides the BlackBerry Enterprise Server data, click **Device Wins**.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Synchronizing contact pictures

By default, the BlackBerry Synchronization Service synchronizes pictures that a user adds to contact entries in their contact list between the BlackBerry device and the email applications on their computer. A user can add, delete, and change pictures in the email applications on the computer or on the BlackBerry device.

If a picture is larger than 32 KB, the BlackBerry Synchronization Service cannot synchronize the contact picture to a BlackBerry device from an email application.

Turn off synchronization of contact pictures for a user account

Before you begin:

Verify that you turned on the mappings for organizer data synchronization for a specific user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.

6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Mappings for organizer data synchronization** tab, in the **Additional mappings** section, in the **Picture** drop-down list, click **None**.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Managing your organization's messaging environment and attachment support

Managing message forwarding

You can define the 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 users' email applications to their BlackBerry devices. You can also manage individual user accounts, provide support to users, control the size of the message queue, and control the load on the BlackBerry Messaging Agent to process forwarding requests. By default, email message forwarding is turned on when you add a user account to the BlackBerry Enterprise Server.

Users can configure message forwarding settings on their BlackBerry devices, or by using the BlackBerry Desktop Manager or the BlackBerry Web Desktop Manager. The settings that you define override the settings that users define.

Forward email messages to a BlackBerry device when no filter rules apply

You can configure a BlackBerry Enterprise Server to deliver incoming messages to a user's BlackBerry device when no email message filters apply to those messages.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of a user account.
5. In the **Messaging configuration** section, click **Default configuration**.
6. Click **Edit user**.
7. On the **Email** tab, in the **Email message filter rules** section, click **Forward email messages to the device**.

8. Click **Continue to user information edit**.
9. Click **Save all**.

Do not deliver email messages to a BlackBerry device when no filter rules apply

You can configure a BlackBerry Enterprise Server to prevent the delivery of incoming email messages to a user’s BlackBerry device when no email message filters apply to the email messages.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of a user account.
5. In the **Messaging configuration** section, click **Default configuration**.
6. Click **Edit user**.
7. On the **Email** tab, in the **Email message filter rules** section, click **Do not forward email messages to the device**.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Forward email messages from inbox subfolders to a BlackBerry device

You can specify which subfolders in a user's email application that the BlackBerry Enterprise Server can forward email messages from. By default, a BlackBerry Enterprise Server forwards messages from the inbox only.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Email** tab, in the **Redirection folders** section, perform one of the following actions:
   - To forward email messages from the user's inbox only, click **Inbox only**.

- To forward email messages from the user's inbox and sent items folder, click **Inbox and Sent Items only**.
- To select the folders that you want the BlackBerry Enterprise Server to forward messages from, click **Selected folders**. Click the folders that you want to forward messages from.

8. Click **Continue to user information edit**.
9. Click **Save all**.

Turn off email message forwarding to user accounts in a group

You can temporarily stop the BlackBerry Enterprise Server from forwarding email messages to user accounts that belong to a user group (for example, if the members of the user group are out of a wireless coverage area and do not want to receive email messages during that time). When you turn off message forwarding for user accounts, users can send email messages from their BlackBerry devices, but cannot receive email messages.

Users can turn on email message forwarding on the BlackBerry device manually.

1. In the BlackBerry Administration Service, on the **BlackBerry Solution management** menu, expand **User**.
2. Click **Manage users**.
3. Click **View more criteria**.
4. In the **Group criteria** section, in the **Specific group** drop-down list, click the group you want to turn off message forwarding for.
5. Click **Search**.
6. Select all users.
7. In the **Device services** list, click **Turn off redirection for selected devices**.

Turn off email message forwarding to a user account

You can temporarily stop the BlackBerry Enterprise Server from forwarding email messages to a BlackBerry device (for example, if a user is out of a wireless coverage area and does not want to receive email messages during that time). When you turn off message forwarding for a user account, the user can send email messages from the BlackBerry device, but cannot receive email messages.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. Click **Edit user**.

5. In the **Messaging configuration** section, click **Default configuration**.
6. In the **Email services settings** section, on the **Redirect to BlackBerry device** drop-down list, click **No**.
7. Click **Continue to user information edit**.
8. Click **Save all**.

After you finish: The user can turn on message forwarding on the BlackBerry device manually.

Turn off synchronization for email messages sent from a BlackBerry device

If you do not want a user's email application to receive a copy of email messages that the user sends from the BlackBerry device, you can turn off synchronization for email messages that the user sends from the BlackBerry device.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Services** tab, in the **Email services settings** section, in the **Save copy in sent folder** drop-down list, click **No**.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Turn off email message forwarding when a user connects a BlackBerry device to a computer

To manage network resources and control the number of email messages on a user's BlackBerry device, you can turn off email message forwarding when a user's BlackBerry device is connected to the user's computer using a USB connection.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.

6. In the **Messaging configuration** section, click **Default configuration**.
7. In the **Email services settings** section, in the **Redirect when in cradle** drop-down list, click **No**.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Managing the incoming message queue

The incoming message queue stores email messages from an organization's mail server until the BlackBerry Enterprise Server processes the email messages and sends them to BlackBerry devices.

Delete email messages for user accounts from the incoming message queue

You can delete email messages for one or more user accounts from the incoming message queue. This permits you to manage the size of the queue and to manage user accounts that have a high number of pending email messages.

When you delete pending email messages from the incoming message queue, the BlackBerry Enterprise Server does not send the email messages to the user’s BlackBerry device. The email messages remain in the email application on the user’s computer.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for one or more user accounts.
4. Select the user accounts that you want to delete incoming messages for.
5. In the **Pending data packets** list, click **Purge pending data packets for selected devices**.

If wireless calendar synchronization for a user account is turned on, the BlackBerry Enterprise Server deletes pending meeting invitations or updates from the incoming message queue and sends them at a later time. The BlackBerry Enterprise Server does not delete IT policies and IT administration commands from the incoming message queue.

Managing wireless message reconciliation

The BlackBerry Enterprise Server synchronizes email message status changes between BlackBerry devices and the email applications on users' computers. The BlackBerry Enterprise Server reconciles message moves, deletions, and indicators for read and unread messages every 30 minutes. By default, wireless message reconciliation is turned on.

To reduce high volumes of wireless network traffic, you can instruct users to limit how often they use the Reconcile Now menu item in the message list on their BlackBerry devices.

Turn off wireless message reconciliation for a BlackBerry Enterprise Server

You can turn off wireless message reconciliation to reduce wireless network traffic or to manage user accounts. If you turn off wireless message reconciliation, users can reconcile their email messages only by connecting their BlackBerry devices to the BlackBerry Desktop Manager or the BlackBerry Web Desktop Manager.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Messaging options** section, in the **Wireless message reconciliation turn on** drop down list, click **False**.
5. Click **Save all**.

Turn on reconciliation for email messages that are hard deleted

Users can hard delete email messages in Microsoft Outlook and you can configure a BlackBerry Enterprise Server to remove hard deleted messages from BlackBerry devices. If you turn on hard deletes reconciliation, the BlackBerry Messaging Agent also deletes email messages from devices when users archive or move email messages to personal folders in Microsoft Outlook. When you turn on reconciliation for hard deleted email messages, the BlackBerry Messaging Agent uses recurring message scans to detect hard deleted email messages on the messaging server, and then deletes the email messages from devices.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Messaging options** section, in the **Hard deletes reconciliation** drop-down list, click **True**.
5. Click **Save all**.
6. On the computer that hosts the BlackBerry Dispatcher, restart the BlackBerry Dispatcher.

Related information

Restarting BlackBerry Enterprise Server components, 392

Managing access to remote message data

Prevent a user from checking the availability of meeting participants on the BlackBerry device

By default, when a BlackBerry device user creates a meeting request , the BlackBerry device user can check to see if a potential participant is available. You can turn this feature off if you want to minimize the resource impact of the BlackBerry Enterprise Server on your organization's messaging server.

Before you begin: If your organization's environment includes Microsoft Exchange 2007, configure the system public folder’s Schedule + Free Busy properties. For more information, visit www.microsoft.com to read article 397221(EXCHG.80) and article 691120(EXCHG.80).

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component View** > **Email**.
2. Click the name of the BlackBerry Enterprise Server instance or BlackBerry Enterprise Server pair that you want to change.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Messaging Options** section, change **Free busy lookup turn on** to **False**.
5. Click **Save All**.
6. Restart the BlackBerry Enterprise Server using one of the following methods:
   - If you want to change a BlackBerry Enterprise Server instance, on the **Instance information** tab, click **Restart instance**.

- If you want to change a BlackBerry Enterprise Server pair, click one of the instances, and on the **Instance information** tab, click **Restart instance**. Repeat this step for the other instance in the pair.
- In the Windows Services, restart the BlackBerry Dispatcher.

7. Repeat step 2 to step 6 for each BlackBerry Enterprise Server instance that you want to turn off the feature for.

After you finish: To allow the user to check the availability of a potential meeting participant, in the **Messaging Options** section, change **Free busy lookup turn on** to **True**. Click **Save all**. Restart the BlackBerry Enterprise Server.

Related information

Restarting BlackBerry Enterprise Server components, 392

Prevent a user from searching for remote email messages using a device

You can prevent BlackBerry device users from searching with their devices for remote email messages that are located on the messaging server.

Before you begin: You must turn on wireless email reconciliation.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the name of the BlackBerry Messaging Agent instance that you want to prevent a device user from searching for remote email messages.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Messaging options** section, in the **Remote search turned on** drop-down list, click **False**.
5. Click **Save all**.
6. On the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **BlackBerry Enterprise Server**.
7. Click the name of the BlackBerry Enterprise Server instance or BlackBerry Enterprise Server pair that is associated with the email instance that you want to prevent a device user from searching for remote email messages.
8. Restart the BlackBerry Enterprise Server using one of the following methods:
    - If you are changing a BlackBerry Enterprise Server instance, in the **Status** list, click **Restart instance**.
    - If you are changing a BlackBerry Enterprise Server pair, in the **Status** list for one of the instances in the pair, click **Restart instance**. Repeat this step for the other instance in the pair.
    - In the Windows Services, restart the BlackBerry Dispatcher.
9. Repeat step 2 to step 8 for each BlackBerry Messaging Agent instance that you want to turn off remote searching for.

After you finish: To turn on the ability to search for remote messages, in the **Messaging Options** section, change **Remote search turn on** to **True**. Click **Save all**. Restart the BlackBerry Enterprise Server.

Related information

Restarting BlackBerry Enterprise Server components, 392

Managing email messages that contain HTML and rich content

The BlackBerry Enterprise Server supports email messages that contain HTML and rich content on BlackBerry devices that are running BlackBerry Device Software version 4.5 or later. You can turn off support for rich content and inline images in email messages. Users can configure the message settings on the BlackBerry devices. The settings that you define override the settings that users define.

View whether a user turned on support for email messages that contain HTML and rich content for a BlackBerry device

You can view whether a user turned on support for email messages with HTML and rich content and whether a user can download images to a BlackBerry device automatically. A user can choose whether to turn off support on the BlackBerry device.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for the user account that you assigned the BlackBerry device to.
4. In the search results, click the user name.
5. In the **Messaging configuration** section, click the device configuration name.
6. In the **Email Services Settings** section, check if **Rich content turned on** and **Automatic downloading of inline images turned on** are configured to **Yes**.

Turn off support for rich text formatting and inline images in email messages for users on a BlackBerry Enterprise Server

You can prevent the BlackBerry Enterprise Server from sending email messages that contain HTML and rich content to BlackBerry devices. When you turn off rich text formatting, the BlackBerry Enterprise Server sends all email messages in plain text format. You can also prevent the BlackBerry Enterprise Server from sending email messages that contain inline images to BlackBerry devices.

If you turn off support for rich content and inline images, you reduce the resource consumption on the computers that are running the messaging server, BlackBerry Attachment Service, and BlackBerry MDS Connection Service.

1. In the BlackBerry Administration Service, in the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component View** > **Email**.
2. Click the name of the BlackBerry Enterprise Server instance or BlackBerry Enterprise Server pair that you want turn off rich text formatting or inline images for.
3. Click **Edit instance**.
4. On the **Messaging** tab, perform one or both of the following options:
   - To turn off rich text formatting, in the **Messaging options** section, in the **Rich content turned on** drop-down list, click **False**.
   - To prevent sending inline images, in the **Messaging options** section, in the **Automatic downloading of inline images turned on** drop-down list, click **False**.
5. Click **Save All**.
6. Restart the BlackBerry Enterprise Server using one of the following methods:
   - If you want to change a BlackBerry Enterprise Server instance, on the **Instance information** tab, click **Restart instance**.
   - If you want to change a BlackBerry Enterprise Server pair, click one of the instances, and on the **Instance information** tab, click **Restart instance**. Repeat this step for the other instance in the pair.
   - In the Windows Services, restart the BlackBerry Dispatcher.
7. Repeat step 2 through step 6 for each BlackBerry Enterprise Server instance that you want to turn off rich text formatting or inline images for.

Turn off support for rich text formatting and inline images in email messages using an IT policy rule

You can change an IT policy rule to prevent the BlackBerry Enterprise Server from sending email messages that contain HTML and rich content or inline images to users. If you turn off support for rich text formatting, the BlackBerry Enterprise Server sends all email messages in plain text format.

If you turn off rich content formatting and inline images, you reduce resource consumption on the computers that host the messaging server, BlackBerry Attachment Service, and BlackBerry MDS Connection Service.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. Click the name of the IT policy that you want to change.
4. Click **Edit IT policy**.
5. On the **Email Messaging** tab, perform one or both of the following actions:
   - To turn off rich content formatting, in the **Disable Rich Content Email** drop-down list, click **Yes**.
   - To turn off inline images, in the **Inline Content Requests** drop-down list, click **Disabled**.
6. Click **Save all**.
7. Resend the updated IT policy to the BlackBerry devices.

Related information

Restarting BlackBerry Enterprise Server components, 392

Synchronizing folders on the BlackBerry device

Control which published public contact folders a user can synchronize to a BlackBerry device

By default, a user can synchronize contacts from all of the published public contact folders on the messaging server with the contact lists on a BlackBerry device. To help manage network resources, you can select the published public contact folders that a user can synchronize.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click the device configuration name.
7. On the **Email** tab, in the **Published public contact folders** section, select the check box beside each public address book that you want to permit the user to synchronize with the contact lists on the BlackBerry device.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Control which personal contact subfolders a user can synchronize to a BlackBerry device

By default, a user can synchronize all of the personal contact subfolders on the messaging server with the contact lists on the BlackBerry device. To help manage network resources, you can select the personal contact subfolders that a user can synchronize.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.

3. Search for a user account.
4. Click the display name for the user account.
5. Click **Edit User**.
6. In the **Messaging configuration** section, click **Device configuration**.
7. On the **Email** tab, in the **Private contact folders** section, select the private contact subfolders that you want to permit the user to synchronize with the contact lists on the BlackBerry device.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Control which personal mail folders a user can synchronize with a BlackBerry device

To help manage network resources, you can select the personal mail folders that a user can synchronize with a BlackBerry device.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for the user account.
4. In the search results, click the display name for a user account.
5. Click **Edit User**.
6. In the **Messaging configuration** section, click **Device configuration**.
7. On the **Email** tab, in the **Redirection settings** section, click **Selected Folders**.
8. Select the folders that you want to permit the user to synchronize with the contact lists on the BlackBerry device.
9. Click **Continue to user information edit**.
10. Click **Save all**.

After you finish: To permit the user to select which folders that the user can synchronize, instruct the user to select folders using the BlackBerry Desktop Manager or BlackBerry Web Desktop Manager.

Configuring access to documents on remote file systems

By default, the BlackBerry MDS Connection Service can search your organization's Windows network for any documents that users might want to access from the BlackBerry devices.

In BlackBerry Enterprise Server version 5.0 or later and BlackBerry Device Software version 5.0 or later, if you want to permit users to access specific documents that are not located on the Windows network (for example, documents that are located on a Linux network) from the BlackBerry devices, you must configure the BlackBerry MDS Connection Service to search the remote file system where the documents are located and provide the authentication credentials to users or the BlackBerry MDS Connection Service. For remote file systems that require authentication, you can provide the credentials to the BlackBerry MDS Connection Service so that users do not need to provide the credentials when they access the documents.

To configure the BlackBerry MDS Connection Service to search the remote file system, you must define how the BlackBerry MDS Connection Service communicates with the remote file system, add the communication information to a BlackBerry MDS Connection Service configuration set, and assign the configuration set to one or more BlackBerry MDS Connection Service instances.

Configure the BlackBerry MDS Connection Service to communicate with a remote file system

To permit the BlackBerry MDS Connection Service to communicate with a remote file system, you specify the URL for the remote file system and the type of access (Linux or Windows) that the domain of the remote file system supports. You can also provide credentials for the domain so that BlackBerry device users do not need to provide the credentials when they access the documents.

Before you begin: If the file system requires the BlackBerry MDS Connection Service to authenticate to the remote file system, create an account on the remote file system that the BlackBerry MDS Connection Service can use to authenticate when the BlackBerry MDS Connection Service receives requests for documents.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **File** tab, in the **Name** field, type a name for the communication method that you want to configure.
5. In the **Service URL** field, type the UNC path to the remote file system using the following format: /*<computer_name>* *<fs_path>*, where *<computer_name>* is the FQDN or IP address of a computer or the virtual view of the shared folders

(for example, the DFS Namespace in Windows Server) and <*fs_path*> is the optional directory path that can include a specific filename. When you type the UNC path, you can use an asterisk (*) to represent a sequence of arbitrary characters (including blank spaces), a question mark (?) to represent a single arbitrary character, and a backslash (\) to represent an escape character. You cannot type a URL that can search all of the computers in a Windows domain.

6. If the file system requires the BlackBerry MDS Connection Service to authenticate with the remote file system, perform the following actions:
   - In the **User name** field, type the name of the account that you want the BlackBerry MDS Connection Service to use to authenticate to the remote file system.
   - In the **Authentication domain** field, type the domain for the user account.
   - In the **Password** and **Confirm password** fields, type the password for the user account.
   - In the **Network provider** drop-down list, click the network provider that BlackBerry MDS Connection Service should use to access the file system.
7. Click **Save all**.

Examples for step 5

To access a specific file on a computer, you can type **/test.company.net/docs/presentation.ppt**. To access the shared folders on a specific computer, you can type **/10.10.10.10**. To access all of the content on the computers in a specific domain, you can type ***.test.company.net/***.

After you finish: Add communication information to a BlackBerry MDS Connection Service configuration set.

Add communication information to a BlackBerry MDS Connection Service configuration set

A BlackBerry MDS Connection Service configuration set is a set of service configurations that the BlackBerry MDS Connection Service instances in your organization can use to communicate with a remote file system, an LDAP server, a DSML server, a CRL server, an OCSP server, or a certification authority. You must add the communication information that the BlackBerry MDS Connection Service requires to communicate with servers to a configuration set so that a BlackBerry MDS Connection Service instance can communicate with the servers after you assign the configuration set to the instance.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click **Edit component**.
4. On the **Configuration Sets** tab, perform one of the following actions:
   - To create a configuration set, in the **Configuration set name** section, type a name and description for the configuration set.

- To change an existing configuration set, click the **Edit** icon.

5. In the **Priority Service group** drop-down list, click the name of the service that you want to configure the communication method for.
6. In the **Service (Name : Description)** drop-down list, click the name of the communication method that you want to configure.
7. Click the **Add** icon.
8. To specify the communication method that the BlackBerry MDS Connection Service should try to connect to the server with first , click the **Up** and **Down** arrows. The BlackBerry MDS Connection Service resolves conflicts by applying communication methods in the order that you specify. The order of that you specify for LDAP, DSML, or file communication applies to each communication method separately. The order permits the BlackBerry MDS Connection Service to resolve conflicts between domains if you created multiple communication methods for a specific URL.
9. Perform one of the following actions:
   - To add a new configuration set, click the **Add** icon.
   - To update an existing configuration set, click the **Update** icon.
10. Click **Save all**.

After you finish:

- To confirm your changes, click the **View** icon.
- Assign the configuration set to a BlackBerry MDS Connection Service.

Assign a BlackBerry MDS Connection Service configuration set to a BlackBerry MDS Connection Service instance

You can assign a BlackBerry MDS Connection Service configuration set to a BlackBerry MDS Connection Service instance so that BlackBerry device users can access documents on remote file systems from devices, the BlackBerry MDS Connection Service can search for certificates and check for the status of the certificates from LDAP servers, DSML servers, CRL servers, or OCSP servers, and the BlackBerry MDS Connection Service can send certificate requests to a certificate authority.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **MDS Connection Service**.
3. Click the instance that you want to change.

4. Click **Edit instance**.
5. On the **Component Configuration Sets** tab, in the **Available component configuration sets** section, in the **Service configuration sets** drop-down list, click the configuration set that you want to assign to the BlackBerry MDS Connection Service instance.
6. Click **Save all**.
7. To restart the BlackBerry MDS Connection Service instance, on the **Instance information** tab, in the **Status** list, click **Restart instance**.
8. To assign the BlackBerry MDS Connection Service configuration set to another BlackBerry MDS Connection Service instance, repeat steps 3 to 7.

Related information

Restarting BlackBerry Enterprise Server components, 392

Managing signatures and disclaimers in email messages

Add a signature to email messages that a user sends from a BlackBerry device

To enforce a signature format policy in your organization, you can add a standard signature to the email messages that users send from their BlackBerry devices.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Email** tab, in the **Mail options** section, in the **Auto signature** field, type the signature that you want to appear in the email messages that the user sends from the BlackBerry device.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Add a disclaimer to email messages that users send from BlackBerry devices

You can add a disclaimer to email messages that users send from their BlackBerry devices. Users cannot change the disclaimers that you define.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Messaging options** section, perform one of the following actions:
    - To add a disclaimer before the body of the message, in the **Prepended disclaimer text** field, type the disclaimer.
    - To add a disclaimer after the user signature, in the **Appended disclaimer text** field, type the disclaimer.
5. Repeat steps 2 to 4 for each instance that you want to create a disclaimer for.
6. Click **Save all**.

Add a disclaimer to email messages that a user sends from a BlackBerry device

You can add a disclaimer to all email messages that are sent by a user that is different from the disclaimer that you added for all users on a BlackBerry Enterprise Server. A user cannot change the disclaimer that you define.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for the user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Email** tab, in the **Mail options** section, perform one of the following actions:
    - To add a disclaimer before the body of the message, in the **Prepended disclaimer text** field, type the disclaimer.
    - To add a disclaimer after the user signature, in the **Appended disclaimer text** field, type the disclaimer.

8. Click **Continue to user information edit**.
9. Click **Save all**.

Specify conflict rules for disclaimers

If you associate multiple disclaimers with a user account, you can specify conflict rules for the disclaimer to define the order in which the BlackBerry Enterprise Server applies the disclaimers. For example, you can configure the BlackBerry Enterprise Server to display the user disclaimer first in the email message, followed by the BlackBerry Enterprise Server disclaimer.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Messaging options** section, perform one of the following actions:
   - To specify the conflict rules for disclaimers that appear before the body of a message, in the **Messaging options** section, in the **Prepended disclaimer conflict rule** drop-down list, click a conflict rule.
   - To specify the conflict rules for disclaimers that appear after the user signature, in the **Messaging options** section, in the **Appended disclaimer conflict rule** drop-down list, click a conflict rule.
5. Click **Save all**.

Turn off disclaimers for email messages

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Messaging tab**, in the **Messaging options** section, perform any of the following actions:
   - To turn off disclaimers that appear before the body of the message, in the **Prepended disclaimer conflict rule** field, in the drop-down list, click **Disable all disclaimer text**.
   - To turn off disclaimers that appear after the user signature, in the **Appended disclaimer conflict rule** field, in the drop-down list, click **Disable all disclaimer text**.
5. Click **Save all**.

Monitor email messages that users send from BlackBerry devices

To monitor the content of email messages that users send from their BlackBerry devices, you can BCC specific email addresses on the email messages. You can BCC the email addresses of all of the users that you assign to a BlackBerry Messaging Agent. When you automatically BCC email addresses on messages, the BCC field of the original message is populated, so the message sender is aware that the message is BCCed.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Auto BCC email address** section, perform one of the following tasks:

Task	Steps
Add email addresses manually.	In the **Auto BCC email address** field, type the email addresses.
Add email addresses from the address book.	1. Click **Select from mail address list**. 2. Search for one or more users. 3. In the search results, select one or more user accounts. 4. Click **Continue**.

5. Click the **Add** icon.
6. Repeat steps 4 and 5 for each email address that you want to add.
7. Click **Save all**.

Sending notification messages to users

You can send a notification message to a user, to all of the users associated with a BlackBerry Enterprise Server, or to all of the users in the BlackBerry Domain. You can send notifications as email messages or PIN messages. PIN messages are appropriate for informing users about messaging server outages because BlackBerry devices send and receive PIN messages directly, without using the messaging server. BlackBerry devices do not apply filters to PIN messages.

When users reply to a notification email message, their BlackBerry devices send the replies to the Windows account that you used to install the BlackBerry Enterprise Server (for example, besadmin).

Send a notification message to all users in a BlackBerry Domain

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry solution topology**.
2. Click **BlackBerry Domain**.
3. On the **Domain information** tab, click **Send message to users**.
4. Type the message that you want to send.
5. Click **Send message**.

Send a notification message to all users on a BlackBerry Enterprise Server

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **BlackBerry Enterprise Server**.
2. Click an instance.
3. Under **Manage BlackBerry Enterprise Server users**, click **Send message to users**.
4. Type the message that you want to send.
5. Click **Send message**.

Send a notification message to group members

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. Click a group.
4. Click **Send message to users in group**.
5. Type the message that you want to send.

6. Click **Send message**.

Send a notification message to a user

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of a user account.
5. Click **Send message to user**.
6. Type the message that you want to send.
7. Click **Send message**.

Change the size of the message state database

The BlackBerry Messaging Agent uses a message state database to manage the mapping between email messages on BlackBerry devices and email messages on the Microsoft Exchange Server. The size of the message state database defines how many recent email messages are kept in this mapping for each user. Increasing the size of the message state database might decrease the message load on the Microsoft Exchange Server because the BlackBerry Messaging Agent can use the local message state database to search for messages instead of communicating with the Microsoft Exchange Server. Increasing the size of the message state database also increases how much memory the BlackBerry Messaging Agent uses.

If you change the size of the message state database, your organization's environment might experience a serious performance impact.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Performance** section, in the **Message state database size** field, type a value between 0 and 1000, that specifies the number of messages that the BlackBerry Enterprise Server keeps in the mapping for each user.
   The default value is 100 messages.
5. Click **Save all**.

How the BlackBerry Attachment Connector communicates with BlackBerry Attachment Service instances

When a user sends a request to view an email message attachment on a BlackBerry device, the BlackBerry device sends a request to the BlackBerry Enterprise Server to convert the attachment. The BlackBerry Enterprise Server uses a BlackBerry Attachment Connector to send the attachment data to a BlackBerry Attachment Service, which processes the request and returns the attachment data to the BlackBerry Attachment Connector. The BlackBerry Enterprise Server requests the attachment data from the BlackBerry Attachment Connector and sends the attachment data to the user's BlackBerry device.

By associating multiple BlackBerry Attachment Service instances with a single BlackBerry Attachment Connector, you can create a BlackBerry Attachment Service pool. You can configure different BlackBerry Attachment Service instances as dedicated servers for processing specific file formats. For example, you can create a BlackBerry Attachment Service pool that contains three BlackBerry Attachment Service instances, where one instance processes email message attachments that are in audio file formats, one instance processes email message attachments that are in image file formats, and one instance processes email message attachments that are in all other file formats. For more information about configuring high availability for the BlackBerry Attachment Service, see the *BlackBerry Enterprise Server Planning Guide*.

You can change how a BlackBerry Attachment Connector processes attachment requests that it cannot deliver to a BlackBerry Attachment Service, and you can change how a BlackBerry Attachment Connector restores a lost connection to a BlackBerry Attachment Service.

Related information

Create a BlackBerry Attachment Service pool for high availability, 114

Change how a BlackBerry Attachment Connector retries sending requests to a BlackBerry Attachment Service

The BlackBerry Attachment Connector sends requests to view attachments from users' BlackBerry devices to a BlackBerry Attachment Service. You can change how a BlackBerry Attachment Connector processes attachment requests that it cannot deliver to a BlackBerry Attachment Service.

Depending on the number of users in your organization's environment, if you change the BlackBerry Attachment Connector settings, your organization's environment might experience a performance impact.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Attachment** > **Connector**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. In the **General** section, in the **Minimum wait for retry per request** field, type the amount of time, in milliseconds, that the BlackBerry Attachment Connector waits before it resends a request that is not delivered to a BlackBerry Attachment Service.

   The default value is 1000 milliseconds.
5. In the **Maximum retries per request** field, type the maximum number of times that the BlackBerry Attachment Connector tries to resend a request that is not delivered to a BlackBerry Attachment Service.

   The default value is 10.
6. Click **Save all**.

Change how a BlackBerry Attachment Connector restores a lost connection to a BlackBerry Attachment Service

Based on the number of users in your organization's environment, if you change the BlackBerry Attachment Connector settings, your organization's environment might experience a performance impact.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Attachment** > **Connector**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. In the **General** section, in the **Minimum wait to attempt restore of lost connection** field, type the amount of time, in milliseconds, that the BlackBerry Attachment Connector waits before it tries to restore a lost connection to a BlackBerry Attachment Service.

   The default value is 1000 milliseconds.
5. Click **Save all**.

Attachment file formats that the BlackBerry Attachment Service supports

Format	Extension
Adobe Acrobat	.pdf
ASCII text	.txt
audio	.amr, .mp3, .wav, .wma
Corel WordPerfect 7-10	.wpd
HTML	.htm, .html
images	.bmp, .gif, .jpeg, .jpg, .png, .ppm, .tif, .tiff, .wmf
Microsoft Excel 97-2003, 2007, and XP	.xls, .xlsx
Microsoft PowerPoint 97-2003, 2007, and XP	.pps, .ppsx, .ppt, .pptx
Microsoft Word 97-2003, 2007, and XP	.doc, .dot, .dotx, .docx
OpenOffice Format version 1.1	.odp, .ods, .odt, .ott
RTF	.rtf
ZIP archives	.zip

Limitations for supported attachment file formats

Format and extension	Limitations
audio	You must install the software update for KB22953 on Windows Server 2008 if you want the BlackBerry Attachment Service to support .mp3 audio files on BlackBerry devices and all audio formats on BlackBerry 7100 Series devices that support CDMA networks. To download the software update for KB22953, visit www.blackberry.com/support/downloads/.

Format and extension	Limitations
OpenOffice Format version 1.1 — .odp files	The BlackBerry Attachment Service supports .odp files that users create using IBM Lotus Symphony only. The fonts that can be displayed in slides are dependent on the font types that are available on the BlackBerry Attachment Service. If a specific font is not available, the BlackBerry Attachment Service uses the most similar font type that is available. The BlackBerry Attachment Service does not support the following features in .odp files: • some text effects and style options • line spacing: proportional, at least, leading • text with position functionality • animation • transitions • tables • .svm images • crop and clip image effects • specific types of text object spacing • table of contents • portrait page orientation • color gradient, hatching, and bitmap fill effects • some shapes • shape, image, and text rotation • connector shape route that connects to shapes
OpenOffice Format version 1.1 — .ods files	The BlackBerry Attachment Service supports .ods files that users create using IBM Lotus Symphony only. Cell dimensions might change when they are displayed on devices. The BlackBerry Attachment Service does not support the following features in .ods files: • some text effects: specific underline styles, specific strikethrough styles, emphasis, outline, shadow, embossed, engrayed • text alignment

Format and extension	Limitations
	• charts • style effects for cells: shadow, borders • headers and footers • drawing objects and Fontwork objects

Changing how a BlackBerry Attachment Service converts attachments

If the BlackBerry Enterprise Server receives requests from BlackBerry device users to view email message attachments, the BlackBerry Attachment Service converts the attachments into a DOM and caches the DOM locally. The BlackBerry Attachment Service accesses the DOM to process the requests. If users send requests to view the same message attachment again, the BlackBerry Attachment Service accesses the same DOM to process the requests. The BlackBerry Attachment Service keeps all of the cached data in memory only and never caches the original documents.

Each attachment conversion process allocates memory when it starts, uses memory on conversion, and caches the attachment DOM locally on the computer that hosts the BlackBerry Attachment Service. A larger cache size means that more memory is allocated to each running conversion process. The maximum file size of attachments impacts the amount of cached memory that the BlackBerry Attachment Service uses.

By default, the BlackBerry Attachment Service does not limit the file size of an attachment that is embedded in an email message or retrieved using a link. The BlackBerry Enterprise Server sends data to BlackBerry devices over the wireless network in packets that are no larger than 64 KB, and it can send an unlimited number of packets to BlackBerry devices.

You can change how the BlackBerry Attachment Service converts attachments by specifying a maximum file size for attachments that users can receive and controlling how the BlackBerry Attachment Service retrieves, distills, and converts attachment data.

Change how a BlackBerry Attachment Service converts attachments

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Attachment** > **Server**.
2. Click the instance that you want to change.
3. Click **Edit instance**.

4. In the **General** section, configure the BlackBerry Attachment Service optimization settings.
5. Click **Save**.

BlackBerry Attachment Service optimization settings

Setting	Description	Range
Submit port	This setting specifies the TCP/IP port number that a BlackBerry Attachment Service uses to listen for and receive attachment conversion requests in a predefined XML/binary protocol. The default value is 1900.	—
Result port	This setting specifies the TCP/IP port number that a BlackBerry Attachment Service returns attachment conversion results to in a predefined XML/binary protocol. The default value is 2000.	—
Configuration port	This setting specifies the TCP/IP port number that you can use with an XML protocol to configure or obtain configuration information for a BlackBerry Attachment Service, including version information, the number of conversion processes, and the number of cached documents. The default value is 1999.	—
Document cache size	This setting specifies the maximum number of converted documents that can be located in the document cache (as DOM) for a single conversion process. The default value is 32.	1 through 128
Maximum number of processes	This setting specifies the number of conversion requests that the BlackBerry Attachment Service can process at the same time. When you specify this value, consider the amount of available memory and the competing services on the computer that hosts the BlackBerry Attachment Service. The default value is 4.	1 through 64
Process recycle time (minutes)	This setting specifies the length of time that an application conversion process can reuse system resources to reclaim space and prevent failed processes from occupying memory resources. The default value is 25 minutes.	5 to 60 minutes
Maximum conversion threads	This setting specifies the number of documents that the BlackBerry Attachment Service can convert at the same time in a single conversion process. You can use this setting with the Server busy time setting to control thread saturation and manage the BlackBerry Attachment Service workload.	2 to 32

Setting	Description	Range
	The default value is 4.	
Server busy time (seconds)	This setting specifies the threshold at which the BlackBerry Attachment Service does not accept new conversion requests. The default value is 120 seconds.	60 to 270 seconds
Allow remote services	This setting specifies whether you prevent or permit remote TCP/IP connections to the BlackBerry Attachment Service. The default value is Yes.	—
Maximum archive (ZIP) level	This setting specifies how many levels of zipped files that the BlackBerry Attachment Service can process. For example, if you set this field to 2, the BlackBerry Attachment Service processes the .zip files within a .zip file. If you set this field to 1, the BlackBerry Attachment Service only lists the contents of a .zip file. The default value is 1.	1 to 9

Change the maximum file size for attachments that users can receive

The BlackBerry Attachment Service uses memory during the attachment conversion process. If users try to open large or complex attachments (for example, .pdf files or ASCII text files that are larger than 2 MB) or multiple attachments at the same time, you might want to limit the file size for attachments.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Attachment** > **Server**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. In the **Distiller display name** section, in the **Attachment size (KB)** column, type a value, in KB, for the distillers that you want to change. If necessary, configure the settings in the **Additional data** column.
5. Click **Save**.

After you finish: Restart the BlackBerry Attachment Service.

Suggested file sizes for attachments

File format	Suggested size
Adobe Acrobat versions 1.1, 1.2, 1.3, and 1.4	less than 2000 KB
ASCII text	less than 100 KB
audio	less than 2000 KB
Corel WordPerfect versions 6.0, 7.0, 8.0, 9.0 (2000), and 10.0	less than 2000 KB
HTML	less than 100 KB
images	less than 2000 KB
Microsoft Excel versions 97, 2000, 2003, 2007, and XP	less than 2000 KB
Microsoft PowerPoint versions 97, 2000, 2003, 2007, and XP	less than 2000 KB
Microsoft Word versions 97, 2000, 2003, 2007, and XP	less than 2000 KB
MP3	less than 2000 KB
OpenOffice Format version 1.1 - ODP, ODS, ODT	less than 2000 KB
RTF	less than 2000 KB
ZIP archives	less than 2000 KB

Turn off support for an attachment file format for a BlackBerry Attachment Service

The BlackBerry Attachment Service uses distillers to convert attachments that are in supported file formats so that users can view the attachments on their BlackBerry devices. By default, all supported distillers are turned on. You can turn off a distiller to prevent users from viewing attachments that are in a specific file format. For example, if you turn off the .pdf distiller, users cannot view .pdf attachments on their BlackBerry devices.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Attachment** > **Server**.
2. Click the instance that you want to change.

3. Click **Edit instance**.
4. In the **Distiller display name** section, in the **Allowed** column, specify which distillers are supported for the instance.
5. Click **Save**.

After you finish: Restart the BlackBerry Attachment Service.

Related information

Restarting BlackBerry Enterprise Server components, 392

Add support for an additional attachment file format to a BlackBerry Attachment Service

You can configure a BlackBerry Attachment Service to support additional file formats. If your organization's messaging server connects to a document management system that renames file format extensions, you must add the necessary extensions to the list of supported file formats for all BlackBerry Attachment Service instances.

If your organization uses new common extensions for a file format that there is a distiller available for on a BlackBerry Attachment Service, you must add those extensions to the BlackBerry Attachment Connector. For example, if users send .rtf files as .wav files, you must verify that the BlackBerry Attachment Connector supports .wav files and that the appropriate distiller is turned on for the BlackBerry Attachment Service instances.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Attachment** > **Connector**.
2. Click the BlackBerry Attachment Connector instance that is associated with the BlackBerry Attachment Service that you want to change.
3. Click **Edit instance**.
4. On the **Supported Attachment Server instances** tab, click the **Edit** icon for the BlackBerry Attachment Service that you want to support additional file formats.
5. In the field at the bottom of the **Extensions** list, type the extension of the file format that you want to add.
6. Click the **Add** icon.
7. Repeat steps 4 to 6 for each BlackBerry Attachment Service that you want to add additional file formats to.
8. Click **Save all**.

Changing how the BlackBerry Messaging Agent reconciles attachments to the messaging server

The BlackBerry Messaging Agent receives message attachments from supported BlackBerry devices and reconciles the attachments to the messaging server. The BlackBerry Attachment Service does not convert the attachments.

The entries in the CMIME service book on BlackBerry devices indicate whether the BlackBerry Enterprise Server supports attachments that users send from their BlackBerry devices. Users must have BlackBerry Desktop Software version 4.2 or later installed on their computers to make sure that these service book entries remain on their BlackBerry devices during service book updates over a physical connection to a computer that is running the BlackBerry Desktop Software.

By default, the BlackBerry Messaging Agent limits the file size of attachments that it can receive from a BlackBerry device to a maximum of 3 MB. If the BlackBerry Messaging Agent receives more than one attachment at a time, it limits the total file size of all of the attachments to a maximum of 5 MB.

Data that a BlackBerry device and the messaging server send each other over the wireless network must be in packets that are no larger than 64 KB. If a BlackBerry device sends an attachment that is larger than a single packet, the BlackBerry device divides the attachment into multiple packets. The BlackBerry Messaging Agent caches all of the packets and sends the attachment to the messaging server after it receives the last packet.

You can optimize the amount of memory and the number of transactions that the BlackBerry Messaging Agent uses when it receives attachments by changing the maximum file size of attachments or preventing users from sending large attachments.

Users with BlackBerry devices that are running BlackBerry Device Software version 4.5 or later can download attachments in any native format to their BlackBerry devices. Users can open and make changes to native file formats using an appropriate third-party application on their BlackBerry devices. Users might be able to open specific file formats using the media application on their BlackBerry devices.

To manage network resources in your organization's environment, you can change the maximum file size of attachments that users can download to their BlackBerry devices.

Change the maximum file size for attachments that users can send

By default, the maximum file size of a single attachment that users can send is 3072 KB, and the maximum file size of multiple attachments that BlackBerry devices can send in a single email message is 5120 KB.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Messaging options** section, perform any of the following actions:
   - To change the maximum file size for a single attachment that BlackBerry devices can send, in the **Maximum single attachment upload size (KB)** field, type a number that is between 1 and 3072 KB.
   - To change the maximum file size of multiple attachments that BlackBerry devices can send at one time, in the **Maximum multiple attachment upload size (KB)** field, type a number that is between 1 and 5120 KB that is greater than the value in the **Maximum single attachment upload size (KB)** field.
5. Click **Save all**.

Related information

Restarting BlackBerry Enterprise Server components, 392

Prevent users from sending large attachments

If you prevent users from sending large attachments, they can only send specific attachments, such as certificates and contact list entries, that are less than a single packet.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Messaging options** section, in the **Maximum single attachment upload size (KB)** field, type **0**.
5. Click **Save all**.

Change the maximum file size of attachments that users can download

On BlackBerry devices that are running specific versions of the BlackBerry Device Software, users can download attachments in native formats (for example, .txt for a text file) to their BlackBerry devices. Users can open and make changes to the files that they download using an appropriate third-party application on their BlackBerry devices. A user might be able to open specific file formats using the media application on the BlackBerry device.

The default maximum file size of attachments that users can download to their BlackBerry devices is 3072 KB (3 MB).

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Email**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. On the **Messaging** tab, in the **Messaging options** section, in the **Maximum single attachment download size (KB)** field, type a number, in KB, that is between 0 and 10240 (10 MB). If you type **0**, users cannot download attachments in a native format to their BlackBerry devices.
5. Click **Save all**.

Managing calendars

30

Configuring the BlackBerry Enterprise Server to use Microsoft Exchange Web Services or MAPI and CDO libraries

By default, the BlackBerry Enterprise Server uses Microsoft Exchange Web Services to manage calendars on BlackBerry devices. The BlackBerry Enterprise Server monitors periodically whether a user account can use Microsoft Exchange Web Services. If a user account cannot use Microsoft Exchange Web Services, for example, because of a configuration error in Microsoft Exchange, the BlackBerry Enterprise Server uses MAPI and CDO libraries to manage calendars on devices. A BlackBerry Messaging Agent on the BlackBerry Enterprise Server can include a dynamic mix of user accounts that use Microsoft Exchange Web Services and user accounts that use MAPI and CDO libraries.

You can use the BlackBerry Enterprise Trait Tool to configure the BlackBerry Enterprise Server to use only Microsoft Exchange Web Services or only MAPI and CDO libraries to manage calendars on devices. You can configure a specific BlackBerry Messaging Agent instance, a specific BlackBerry Enterprise Server, or all BlackBerry Enterprise Server instances that share one BlackBerry Configuration Database.

To use Microsoft Exchange Web Services, your organization's environment must include Microsoft Exchange 2007 SP1 or later.

For more information about Microsoft Exchange Web Services, visit http://msdn.microsoft.com/en-us/library/bb204119.aspx.

Prerequisites: Configuring the BlackBerry Enterprise Server to use Microsoft Exchange Web Services

- Install an SSL certificate on a BlackBerry Enterprise Server so that the BlackBerry Enterprise Server can communicate with Microsoft Exchange Web Services. You must export the SSL certificate from the client access server for Microsoft Exchange and import the SSL certificate to the BlackBerry Enterprise Server. The BlackBerry Enterprise Server supports a self-signed security certificate or a certificate that a certificate authority issues. For more information about installing an SSL certificate, visit support.microsoft.com to read article KB 962624.

- Configure Microsoft Exchange Impersonation for a BlackBerry Enterprise Server administrator account. For more information about configuring Microsoft Exchange Impersonation, visit msdn.microsoft.com/en-us/library/bb204095.aspx and select the appropriate tab for Microsoft Exchange 2007 or Microsoft Exchange 2010.
- Assign IIS permissions to a BlackBerry Enterprise Server administrator account on the Microsoft Exchange Server that hosts the client access server role. For more information about assigning IIS permissions, visit support.microsoft.com to read article KB 816117.

Turn off client throttling in Microsoft Exchange 2010

By default, Microsoft Exchange 2010 uses client throttling policies to track the bandwidth that each Microsoft Exchange user consumes and enforce bandwidth limits as necessary. The policies affect the performance of the BlackBerry Enterprise Server, so you should turn off client throttling for the Windows account that has a Microsoft Exchange mailbox.

1. On a computer that hosts the Microsoft Exchange Management Shell, open the Microsoft Exchange Management Shell.
2. Type **New-ThrottlingPolicy BESPolicy**.
3. Type the following command:

   Set-ThrottlingPolicy BESPolicy -RCAMaxConcurrency $null -RCAPercentTimeInAD $null -RCAPercentTimeInCAS $null -RCAPercentTimeInMailboxRPC $null -EWSMaxConcurrency $null -EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null -EWSPercentTimeInMailboxRPC $null -EWSMaxSubscriptions $null -EWSFastSearchTimeoutInSeconds $null -EWSFindCountLimit $null
4. Type **Set-Mailbox "BESAdmin" -ThrottlingPolicy BESPolicy**.

Configure the BlackBerry Enterprise Server to use Microsoft Exchange Web Services

You can configure the BlackBerry Enterprise Server to use only Microsoft Exchange Web Services to manage calendars on BlackBerry devices.

1. Copy the BlackBerry Enterprise Server installation files to the computer that hosts the primary BlackBerry Enterprise Server.
2. Extract the contents to a folder on the computer.
3. At a command prompt, navigate to <*extracted_folder*>\tools.
4. Perform one of the following actions:
   - To configure a specific BlackBerry Messaging Agent on a specific BlackBerry Enterprise Server to use Microsoft Exchange Web Services, type **traittool -server** ***<server_name>*** **-agent** ***<agent_id>*** **-trait EWSEnable -set true**, where <*server_name*> is the name of the BlackBerry Enterprise Server and <*agent_id*> is the ID for the

BlackBerry Messaging Agent. If you configured high availability, configure only the primary BlackBerry Enterprise Server.

- To configure all BlackBerry Messaging Agent instances on a specific BlackBerry Enterprise Server to use Microsoft Exchange Web Services, type **traittool -server *<server_name>* -trait EWSEnable -set true**, where *<server_name>* is the name of the BlackBerry Enterprise Server. If you configured high availability, configure only the primary BlackBerry Enterprise Server.
- To configure all BlackBerry Messaging Agent instances on all BlackBerry Enterprise Server instances to use Microsoft Exchange Web Services, type **traittool -global -trait EWSEnable -set true**.

5. Restart the BlackBerry Messaging Agent instances that you made changes to.

After you finish:

In the logs folder verify that the file named *<server_name>*_CALH_*<agent_id>*_*<date>*.txt appears. In the file name, *<server_name>* is the name of the BlackBerry Enterprise Server, *<agent_id>* is the ID of the BlackBerry Messaging Agent, and *<date>* is the date that you configured the BlackBerry Enterprise Server to use Microsoft Exchange Web Services.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configure the BlackBerry Enterprise Server to use MAPI and CDO libraries

You can configure the BlackBerry Enterprise Server to use only MAPI and CDO libraries to manage calendars on BlackBerry devices.

1. Copy the BlackBerry Enterprise Server installation files to the computer that hosts the primary BlackBerry Enterprise Server.
2. Extract the contents to a folder on the computer.
3. At a command prompt, navigate to *<extracted_folder>*\tools.
4. Perform one of the following actions:

   - To configure a specific BlackBerry Messaging Agent on a specific BlackBerry Enterprise Server to use MAPI and CDO libraries, type **traittool -server *<server_name>* -agent *<agent_id>* -trait EWSEnable -set false**, where *<server_name>* is the name of the BlackBerry Enterprise Server and *<agent_id>* is the ID for the BlackBerry Messaging Agent. If you configured high availability, configure only the primary BlackBerry Enterprise Server.
   - To configure all BlackBerry Messaging Agent instances on a specific BlackBerry Enterprise Server to use MAPI and CDP libraries, type **traittool -server *<server_name>* -trait EWSEnable -set false**, where *<server_name>* is the name of the BlackBerry Enterprise Server. If you configured high availability, configure only the primary BlackBerry Enterprise Server.

- To configure all BlackBerry Messaging Agent instances on all BlackBerry Enterprise Server instances to use MAPI and CDO libraries, type **traittool -global -trait EWSEnable -set false**.

5. Restart the BlackBerry Messaging Agent instances that you made changes to.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configure the BlackBerry Messaging Agent instances to use a web address for a specific Microsoft Autodiscover service

You can configure the BlackBerry Messaging Agent instances to use a specific Microsoft Autodiscover service to search for a client access server for Microsoft Exchange by specifying the web address for the service. You can use the web address of the service if the default Microsoft Autodiscover service does not find an appropriate client access server for Microsoft Exchange or if you want to use a different client access server for Microsoft Exchange.

1. Copy the BlackBerry Enterprise Server installation files to the computer that hosts the primary BlackBerry Enterprise Server.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to <*extracted_folder*>\tools.
4. Perform one of the following actions:
    - To configure all BlackBerry Messaging Agent instances on a specific BlackBerry Enterprise Server to use a web address for a specific Microsoft Autodiscover service, type **traittool -server <*server_name*> -trait EWSSCPURL -set <*web_address*>** , where <*server_name*> is the name of the BlackBerry Enterprise Server and <*web_address*> is the web address of the Microsoft Autodiscover service. If you configured high availability, configure only the primary BlackBerry Enterprise Server.
    - To configure all BlackBerry Messaging Agent instances on all BlackBerry Enterprise Server instances to use a web address for a specific Microsoft Autodiscover service, type **traittool -global -trait EWSSCPURL -set <*web_address*>** , where <*web_address*> is the web address of the Microsoft Autodiscover service.

5. Restart the BlackBerry Messaging Agent instances that you made changes to.

Example:

To specify a web address for a specific Microsoft Autodiscover service that all BlackBerry Messaging Agent instances on all BlackBerry Enterprise Server instances will use, type **traittool -global -trait EWSSCPURL -set https://server.company.com/Autodiscover/Autodiscover.xml**

Related information

Restarting BlackBerry Enterprise Server components, 392

Configure the BlackBerry Messaging Agent instances to use a specific web address for a client access server for Microsoft Exchange

You can configure the BlackBerry Messaging Agent instances to use a specific client access server for Microsoft Exchange to connect to Microsoft Exchange Web Services. You can use the specific web address for the client access server if you do not have access to the Microsoft Autodiscover service or if you do not want to use the client access server for Microsoft Exchange that the Microsoft Autodiscover service selects. If you configure the BlackBerry Messaging Agent instances to use the web address for the client access server, the BlackBerry Messaging Agent instances do not use the Microsoft Autodiscover service to search for a client access server for Microsoft Exchange.

1. Copy the BlackBerry Enterprise Server installation files to the computer that hosts the primary BlackBerry Enterprise Server.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to <*extracted_folder*>\tools.
4. Perform one of the following actions:
   - To configure a specific BlackBerry Enterprise Server to use a specific web address for a client access server for Microsoft Exchange, type **traittool -server** <***server_name***> **-trait EWSCASURL -set** <***web_address***> , where <*server_name*> is the name of the BlackBerry Enterprise Server and <*web_address*> is the web address for the Microsoft Exchange client access server. If you configured high availability, configure only the primary BlackBerry Enterprise Server.
   - To configure all BlackBerry Messaging Agent instances on all BlackBerry Enterprise Server instances to use a specific web address for a client access server for Microsoft Exchange, type **traittool -global -trait EWSCASURL -set** <***web_address***> , where <*web_address*> is the web address for the Microsoft Exchange client access server.
5. Restart the BlackBerry Messaging Agent instances that you made changes to.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configuring the BlackBerry Messaging Agent instances to look up the user's status using only Microsoft Exchange Web Services

You can configure the BlackBerry Messaging Agent instances to use only Microsoft Exchange Web Services to determine the user's status, for example, whether a user is available, busy, or offline. By default, the BlackBerry Messaging Agent instances can determine the user's status using Microsoft Exchange Web Services unless the user is an external user or the user's email address is a distribution list. If the BlackBerry Messaging Agent instances cannot determine the user's status using Microsoft Exchange Web Services and Microsoft Exchange public folders that are in your organization's environment, the BlackBerry Messaging Agent instances can search the Microsoft Exchange public folders for the user's status. If your organization's environment is running Microsoft Exchange 2007, it does not include public folders and the BlackBerry Messaging Agent instances write error messages to the log files because they cannot find the public folders.

You can configure the BlackBerry Messaging Agent instances to look up the user's status using only Microsoft Exchange Web Services to avoid the BlackBerry Messaging Agent instances writing error messages to their log files.

Configure the BlackBerry Messaging Agent instances to look up a user's status using only Microsoft Exchange Web Services

1. Copy the BlackBerry Enterprise Server installation files to the computer that hosts the primary BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to <*extracted_folder*>\tools.
4. Perform one of the following actions:
   - To configure a BlackBerry Messaging Agent on a BlackBerry Enterprise Server to look up the user's status using only Microsoft Exchange Web Services, type **traittool -server <server_name> -agent <agent_id> -trait EWSUserAvailabilityAccess -set EWS**, where <*server_name*> is the name of the BlackBerry Enterprise Server and <*agent_id*> is the ID for the BlackBerry Messaging Agent.
   - To configure all BlackBerry Messaging Agent instances on a specific BlackBerry Enterprise Server to look up the user's status using only Microsoft Exchange Web Services, type **traittool -server <server_name> -trait EWSUserAvailabilityAccess -set EWS**, where <*server_name*> is the name of the BlackBerry Enterprise Server.
   - To configure all BlackBerry Messaging Agent instances on all BlackBerry Enterprise Server instances to look up the user's status using only Microsoft Exchange Web Services, type **traittool -global -trait EWSUserAvailabilityAccess -set EWS**.
5. Press ENTER.

Correcting calendar synchronization errors on devices

If you run corrective calendar synchronization on a BlackBerry Enterprise Server instance, you can find and correct differences between the calendar entries on BlackBerry devices and the calendar entries on users' computers. You can specify a recurring day and time when the process can run and specific days when the process should check for calendar synchronization errors.

You configure corrective calendar synchronization using the BlackBerry Enterprise Trait Tool, which is located in the Tools folder of the BlackBerry Enterprise Server installation files.

If corrective calendar synchronization finds differences between the calendar entries on a device and the calendar entries on a computer, the process writes information about the differences to the BlackBerry Messaging Agent log file and, optionally, automatically corrects the calendar synchronization errors that it finds.

It is a best practice to schedule corrective calendar synchronization to occur during low-use periods. For example, you can schedule the process to begin in the early evening, before devices are scheduled to turn off automatically.

Configuration levels using the BlackBerry Enterprise Trait Tool

You can use the BlackBerry Enterprise Trait Tool to specify whether corrective calendar synchronization checks calendar entries for a specific user, users on a specific BlackBerry Enterprise Server, or all users. The tool uses a hierarchy to determine what calendar entries to check. Settings at the user level override settings at the server level, settings at the server level override settings at the global level, and settings at the global level override the default settings.

Level	Description
-global	The setting that you specify applies to all users.
-server <*server_name*>	The setting that you specify applies to all users on a specific BlackBerry Enterprise Server.
-user <*smtp_address*>	The setting that you specify applies to a specific user.

Turn off corrective calendar synchronization

By default, corrective calendar synchronization is turned on. If you do not want the BlackBerry Enterprise Server to check for differences between calendar entries on BlackBerry devices and calendar entries on users' computers, you can turn off corrective calendar synchronization.

1. Copy the BlackBerry Enterprise Server installation files to a computer that hosts a BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to the folder that contains the TraitTool.exe file.
4. Perform one of the following actions:
   - To turn off corrective calendar synchronization for a specific user account, type **traittool -user *<smtp_address>* -trait ExchangeSmartSyncEnable -set false**.
   - To turn off corrective calendar synchronization for all user accounts that are associated with a BlackBerry Enterprise Server, type **traittool -server *<server_name>* -trait ExchangeSmartSyncEnable -set false**.
   - To turn off corrective calendar synchronization for all user accounts, type **traittool -global -trait ExchangeSmartSyncEnable -set false**.
5. Press ENTER.

Example: Turning off the process for all users

```
traittool -global -trait ExchangeSmartSyncEnable -set false
```

Example: Turning off the process for a specific user

```
traittool -user ian.dundas@blackberry.com -trait ExchangeSmartSyncEnable -set false
```

After you finish: To turn on corrective calendar synchronization process, type **traittool -*<level>* -trait ExchangeSmartSyncEnable -set true**, where *<level>* is the SMTP address of a specific user account, the server name of a specific BlackBerry Enterprise Server for all user accounts that are associated with the specific BlackBerry Enterprise Server, or global for all user accounts.

View the current settings for corrective calendar synchronization

1. Copy the BlackBerry Enterprise Server installation files to a computer that hosts a BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to the folder that the TraitTool.exe file is located in.
4. Perform one of the following actions:
   - To view the calendar synchronization settings for a specific user account, type **traittool -user** *<smtp_address>* **-list**.
   - To view the calendar synchronization settings for all user accounts that are associated with a BlackBerry Enterprise Server, type **traittool -server** *<server_name>* **-list**.
   - To view the calendar synchronization settings for all user accounts, type **traittool -global -list**.
5. Press ENTER.

Example: Viewing the global calendar synchronization settings

```
traittool -global -list
```

Turn off automatic error correction in corrective calendar synchronization

By default, corrective calendar synchronization process finds calendar synchronization errors, add the errors to the BlackBerry Messaging Agent log file, and automatically corrects the errors. If you do not want corrective calendar synchronization to automatically correct calendar synchronization errors, you can turn off this function.

1. Copy the BlackBerry Enterprise Server installation files to a computer that hosts a BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to <*extracted_folder*>\tools.
4. Perform one of the following actions:

- To turn off automatic correction of calendar synchronization errors for a specific user account, type **traittool -user *<smtp_address>* -trait ExchangeSmartSyncSendUpdate -set false**.
- To turn off automatic correction of calendar synchronization errors for all user accounts that are associated with a BlackBerry Enterprise Server, type **traittool -server *<server_name>* -trait ExchangeSmartSyncSendUpdate -set false**.
- To turn off automatic correction of calendar synchronization errors for all user accounts, type **traittool -global -trait ExchangeSmartSyncSendUpdate -set false**.

5. Press ENTER.

Example: Turn off automatic error correction for a specific user

```
 traittool -user ian.dundas@blackberry.com -trait ExchangeSmartSyncSendUpdate -set
false
```

After you finish: To turn on calendar synchronization error correction, type **traittool -*<level>* -trait ExchangeSmartSyncSendUpdate -set true**, where *<level>* is the SMTP address of a specific user account, the server name of a specific BlackBerry Enterprise Server for all user accounts that are associated with the specific BlackBerry Enterprise Server, or global for all user accounts.

Configure the range of days to check for calendar synchronization errors

You can configure corrective calendar synchronization to check for calendar synchronization errors during a specific range of days in the calendar after the current date.

1. Copy the BlackBerry Enterprise Server installation files to a computer that hosts a BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to the folder that the TraitTool.exe file is located in.
4. Perform one of the following actions:
    - To check for calendar synchronization errors during a specific range of days in the calendar for a user account, type **traittool -user *<smtp_address>* -trait ExchangeSmartSyncDays -set *<value>*** , where *<value>* is a number from 1 to 365.
    - To check for calendar synchronization errors during a specific range of days in the calendar for all user accounts that are associated with a BlackBerry Enterprise Server, type **traittool -server *<server_name>* -trait ExchangeSmartSyncDays -set *<value>*** , where *<value>* is a number from 1 to 365.

- To check for calendar synchronization errors during a specific range of days in the calendar for all user accounts, type **traittool -global -trait ExchangeSmartSyncDays -set *<value>*** , where <*value*> is a number from 1 to 365.

5. Press ENTER.

Example: To configure corrective calendar synchronization to check calendar entries for the period of three days from the current date for all users, type:

```
traittool -global -trait ExchangeSmartSyncDays -set 3
```

Configure when corrective calendar synchronization runs

You can configure corrective calendar synchronization to start running at a specific hour, on recurring days, or on only one recurring day. To specify more than one value for when corrective calendar synchronization runs, after you extract the BlackBerry Enterprise Server installation files to the computer, you can create a list of values that are separated by commas (,) at the command prompt.

1. Copy the BlackBerry Enterprise Server installation files to a computer that hosts a BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to the folder that the TraitTool.exe file is located in.
4. Perform one of the following actions:

   - To configure calendar synchronization to occur at a specific hour for a specific user account, type **traittool -user *<smtp_address>* -trait ExchangeSmartSyncTriggerHour -set *<value>*** , where <*value*> is a number from 0 to 23, 0 is 12:00 AM, and 23 is 11:00 PM. The default value is 0, which is 12:00 AM.
   - To configure calendar synchronization to occur at a specific hour for all user accounts that are associated with a BlackBerry Enterprise Server, type **traittool -server *<server_name>* -trait ExchangeSmartSyncTriggerHour -set *<value>*** , where <*value*> is a number from 0 to 23, 0 is 12:00 AM, and 23 is 11:00 PM. The default value is 0, which is 12:00 AM.
   - To configure calendar synchronization to occur at a specific hour for all user accounts, type **traittool -global -trait ExchangeSmartSyncTriggerHour -set *<value>*** , where <*value*> is a number from 0 to 23, 0 is 12:00 AM, and 23 is 11:00 PM. The default value is 0, which is 12:00 AM.

5. Press ENTER.
6. Perform one of the following actions:

   - To configure calendar synchronization to recur on specific days for all user accounts, type **traittool -global -trait ExchangeSmartSyncSchedule -set *<value>*** , where <*value*> is one or more of the following options: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Weekdays, Weekends, or Daily. The default value is Daily.

- To configure calendar synchronization to recur on specific days for all user accounts that are associated with a BlackBerry Enterprise Server, type **traittool -server *<server_name>* -trait ExchangeSmartSyncSchedule -set *<value>*** , where <*value*> is one or more of the following options: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Weekdays, Weekends, or Daily. The default value is Daily.
- To configure calendar synchronization to recur on specific days for a user account, type **traittool -user *<smtp_address>* -trait ExchangeSmartSyncSchedule -set *<value>*** , where <*value*> is one or more of the following options: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Weekdays, Weekends, or Daily. The default value is Daily.

7. Press ENTER.

Example: Configuring corrective calendar synchronization to run at 10:00 PM for all users on the BlackBerry Enterprise Server that is named SERVER01

```
 traittool -server SERVER01 -trait ExchangeSmartSyncTriggerHour -set 22
```

Example: Corrective calendar synchronization that runs at 11:00 PM for all users on the BlackBerry Enterprise Server that is named SERVER02

```
 traittool -server SERVER02 -trait ExchangeSmartSyncTriggerHour -set 23
```

Example: Corrective calendar synchronization that runs on weekdays for all users

```
 traittool -global -trait ExchangeSmartSyncSchedule -set Weekdays
```

Example: Corrective calendar synchronization that runs on Monday, Wednesday, and Friday for a specific user

```
 traittool -user greg.stark@blackberry.com -trait ExchangeSmartSyncSchedule -set
Monday,Wednesday,Friday
```

Logging information for corrective calendar synchronization

Corrective calendar synchronization writes the following information to the BlackBerry Messaging Agent log file:

Item	Description
DIF	specifies that a calendar item is different on the BlackBerry device than it is in the email application

Item	Description
MOD	specifies that a calendar item is missing on the device
MOO	specifies that a calendar item is missing in the email application
SAM	specifies that a calendar item is the same on the device and in the email application
SmartSyncFireOff	specifies that the calendar synchronization process was initiated using the BlackBerry Enterprise Trait Tool instead of the standard calendar synchronization process

Delete a setting for corrective calendar synchronization

If you delete a setting for corrective calendar synchronization, the calendar synchronization process uses the setting that you specified at the next highest level of the hierarchy. For example, if you delete a setting at the user level, the process uses the setting that is specified at the server level because the server level is the next highest level. If you do not specify any values, the default value is used.

1. Copy the BlackBerry Enterprise Server installation files to a computer that hosts a BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to the folder that the TraitTool.exe file is located in.
4. Perform one of the following actions:
   - To delete a setting for a specific user account, type **traittool -user** <***smtp_address***> **-trait** <***name***> **-erase**, where <*name*> is the setting you want to delete.
   - To delete a setting for all user accounts that are associated with a BlackBerry Enterprise Server, type **traittool -server** <***server_name***> **-trait** <***name***> **-erase**, where <*name*> is the setting you want to delete.
   - To delete a setting for all user accounts, type **traittool –global -trait** <***name***> **-erase**, where <*name*> is the setting you want to delete.
5. Press ENTER.

Example: To delete the setting for the hour that corrective calendar synchronization begins on the BlackBerry Enterprise Server that is named SERVER01, type:

```
traittool -server SERVER01 -trait ExchangeSmartSyncTriggerHour -erase
```

Start corrective calendar synchronization manually for a user account

By default, the BlackBerry Enterprise Server synchronizes the calendar on each BlackBerry device user's computer with the calendar on each user's BlackBerry device at a regular interval. You can use the BlackBerry Administration Service to start corrective calendar synchronization manually for a user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the PIN for the user account.
5. In the **Communications** list, click **Synchronize calendar**.

Improving the flow of email messages and calendar synchronization when the BlackBerry Enterprise Server runs on Windows Server 2008

The BlackBerry Messaging Agent uses the CalHelper application to connect to the Microsoft Exchange Server so that the BlackBerry Messaging Agent can synchronize calendars on BlackBerry devices with Microsoft Outlook calendars. In BlackBerry Enterprise Server 4.1 SP6 and earlier and in BlackBerry Enterprise Server 5.0, the BlackBerry Messaging Agent uses the CDO.dll library to create temporary MAPI profiles that the CalHelper application can use to connect to the Microsoft Exchange Server to access users’ calendars.

In BlackBerry Enterprise Server 4.1 SP7 and BlackBerry Enterprise Server 5.0 SP1 and later, to improve performance, the BlackBerry Messaging Agent uses the MAPI32.dll library to create the temporary MAPI profiles.

After you install BlackBerry Enterprise Server 4.1 SP7 or BlackBerry Enterprise Server 5.0 SP1 or later, if you are running Windows Server 2008 and notice that the limit that Windows Server 2008 places on NSPI connections is impacting MAPI performance and the flow of email messages, you can change how the BlackBerry Messaging Agent creates temporary MAPI profiles for the CalHelper application.

For more information, visit www.blackberry.com/support to read KB 21413.

Change how the BlackBerry Enterprise Server creates temporary MAPI profiles for the CalHelper application

1. On the computer that hosts the BlackBerry Enterprise Server, on the taskbar, click **Start** > **Run**.
2. Type **regedit.**
3. Click **OK**.
4. Perform one of the following actions:
   - If you are running a 32-bit version of Windows, go to HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion \BlackBerry Enterprise Server\Agents.
   - If you are running a 64-bit version of Windows, go to HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node \Research In Motion\BlackBerry Enterprise Server\Agents.
5. Create a DWORD value that is named **CreateCDOProfile**.
6. Double-click the new DWORD value.
7. In the **Value data** field, perform one of the following actions:
   - To use the CDO.dll library to create temporary MAPI profiles for the CalHelper application, type **0**.
   - To use the MAPI32.dll library to create temporary MAPI profiles for the CalHelper application, type **1**.
8. In the Windows Services, restart the BlackBerry Dispatcher.

Managing instant messaging

31

The BlackBerry Collaboration Service is designed to provide a connection between your organization's instant messaging server and the collaboration client on BlackBerry devices. In some instant messaging environments, you can use TLS or HTTPS to encrypt the connection between specific instant messaging components.

The BlackBerry Collaboration Service supports up to 2000 connections for instant messaging sessions on the following instant messaging servers:

- Microsoft Office Live Communications Server 2005
- Microsoft Office Communications Server 2007
- Microsoft Office Communications Server 2007 R2
- Microsoft Lync Server 2010
- IBM Lotus Sametime

The number of connections that the BlackBerry Collaboration Service supports for instant messaging sessions on the Novell GroupWise instant messaging server is limited to the number of Windows sockets that are available.

Installing a collaboration client on BlackBerry devices

For detailed information about the methods that you can use to install a collaboration client on BlackBerry devices, see the "Add a collaboration client to the application repository" and "Alternative methods for installing BlackBerry Java Applications on devices" sections of the *BlackBerry Enterprise Server Administration Guide*.

To download the .zip file for the appropriate collaboration client, visit www.blackberry.com/support/downloads. For information about the compatibility of collaboration clients and versions of the BlackBerry Enterprise Server, visit na.blackberry.com/eng/support/downloads/im_server_compatibility.jsp.

Change the instant messaging server or pool that a BlackBerry Collaboration Service connects to

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Collaboration**.
2. Expand the instant messaging environment.
3. Click the instance that you want to change.
4. Click **Edit instance**.
5. In the **Connection settings** section, perform one of the following actions:
   - For Microsoft Office Communications Server 2007 R2 or Microsoft Lync Server 2010, in the **Instant messaging server pool name** field, type the FQDN of the pool of instant messaging servers.
   - For all other types of instant messaging server, in the **Host Server for instant messaging** field, type the host name of the instant messaging server.
6. In the **Port** field, type the port number of the instant messaging server or the port number of the pool of instant messaging servers.
7. If necessary, in the **Transport protocol** drop-down list, click the appropriate transport protocol.
8. Click **Save all**.

Change the transport protocol for a Microsoft instant messaging environment

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Collaboration**.
2. Expand the instant messaging environment.
3. Click the instance that you want to change.

4. Click **Edit instance**.
5. In the **Connection settings** section, perform one of the following actions:

Option	Description
For Microsoft Office Communications Server 2007 R2	In the **Transport protocol** drop-down list, perform one of the following actions: • click **TLS** if you want the BlackBerry Collaboration Service to encrypt the data that it sends to the instant messaging servers • click **TCP** if you do not want the BlackBerry Collaboration Service to encrypt the data that it sends to the instant messaging servers
For Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007	In the **Transport protocol** drop-down list, perform one of the following actions: • click **HTTPS** if you want the BlackBerry Collaboration Service to encrypt the data that it sends to the Microsoft Office Communicator Web Access server. The computer that hosts the BlackBerry Collaboration Service must trust the TLS certificate on the Microsoft Office Communicator Web Access server. • click **HTTP** if you do not want the BlackBerry Collaboration Service to encrypt the data that it sends to the Microsoft Office Communicator Web Access server

6. Click **Save all**.

Specify the Windows domain name for users who log in to a collaboration client

You can specify your organization's Windows domain name so that users do not have to type their user names when they log in to a collaboration client on their BlackBerry devices.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Collaboration**.
2. Expand the instant messaging environment.
3. Click the instance that you want to change.
4. Click **Edit instance**.
5. In the **General** section, in the **Default domain name** field, type the Windows domain name.
6. Click **Save all**.

Managing instant messaging sessions

Specify the maximum number of instant messaging sessions that can be open at the same time

To control bandwidth and resource consumption in your organization's environment, you can specify the number of instant messaging sessions that can be open between the BlackBerry Collaboration Service and the instant messaging server at the same time.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Collaboration**.
2. Expand the instant messaging environment.
3. Click the instance that you want to change.
4. Click **Edit instance**.
5. In the **General** section, in the **Maximum simultaneous sessions** field, type the maximum number of instant messaging sessions that can be open at the same time.
6. Click **Save all**.

Specify the inactivity timeout limit for instant messaging sessions

The BlackBerry Collaboration Service closes instant messaging sessions that exceed the inactivity timeout limit.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Collaboration**.
2. Expand the instant messaging environment.
3. Click the instance that you want to change.
4. Click **Edit instance**.
5. In the **General** section, in the **Inactivity timeout (milliseconds)** field, type a value, in milliseconds.
6. Click **Save all**.

Managing instant messaging features

Prevent users from sending specific file types to instant messaging contacts using the BlackBerry Client for IBM Lotus Sametime

On BlackBerry devices that are running BlackBerry Device Software version 4.2 or later and the latest version of the BlackBerry Client for IBM Lotus Sametime, users can send files to their instant messaging contacts. To help manage network resources in your organization's environment, you can specify the types of files that users cannot send from their BlackBerry devices.

In the IT policy for a group or a specific user account, in the Instant Messaging policy group, in the Disallow File Transfer Types IT policy rule, perform one of the following actions:

- To prevent users from sending specific file types, type the file extensions and separate them using commas. For example, type bat, exe, mp3 to prevent users from sending batch, executable, and mp3 files.
- To prevent users from sending all file types, type an asterisk (*).

Related information

Change the value for an IT policy rule, 46

Specifying the maximum size of file types that users can send using the BlackBerry Client for IBM Lotus Sametime

To control the use of network resources in your organization's environment, you can use the media content management feature to specify the maximum size of specific file types that BlackBerry device users can send to each other using the BlackBerry Client for IBM Lotus Sametime. The maximum file size that you specify for a file type must not exceed the maximum file size that you specified on the IBM Lotus Sametime server.

Related information

Configure download limits for media content types, 312

Prevent users from sending instant messaging conversations in email messages

Using the latest version of the BlackBerry Client for use with Microsoft Office Live Communications Server 2005, BlackBerry Client for use with Microsoft Office Communications Server 2007, or BlackBerry Client for IBM Lotus Sametime, BlackBerry device users can send their instant messaging conversations to contacts in email messages. You can turn off this feature if you do not want BlackBerry device users to send their instant messaging conversations to other users.

In the IT policy for a group or user account, in the Instant Messaging policy group, change the Disable Emailing Conversation IT policy rule to Yes.

Related information

Change the value for an IT policy rule, 46

Prevent users from saving instant messaging conversations

On BlackBerry devices that are running BlackBerry Device Software version 4.2 or later and the latest version of a collaboration client, users can save their instant messaging conversations as .txt files in the internal memory of their BlackBerry devices or on an external memory device. You can turn off this feature if you do not want users to save their instant messaging conversations on their BlackBerry devices.

In the IT policy for a group or user account, in the Instant Messaging policy group, change the Disable Saving Conversation IT policy rule to Yes.

Related information

Change the value for an IT policy rule, 46

Hide the icon that appears on BlackBerry devices for mobile contacts

If users are using the BlackBerry Client for IBM Lotus Sametime or BlackBerry Client for Novell GroupWise Messenger, you can control whether an icon appears on BlackBerry devices beside the names of contacts who are using the same collaboration client. By default, the icon appears.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry solution topology** > **BlackBerry Domain** > **Component view** > **Collaboration**.
2. Expand the instant messaging environment.

3. Click the instance that you want to change.
4. Click **Edit instance**.
5. In the **General** section, in the **Show Mobile Icon** drop-down list, click **False**.
6. Click **Save all**.

Make additional contact information and phone numbers available for the BlackBerry Client for IBM Lotus Sametime users

In the latest version of the BlackBerry Client for IBM Lotus Sametime, users can make calls to contacts directly from their contact lists. You can make additional phone numbers available to users from their contact lists, and you can make more contact information available in the contact list on BlackBerry devices by adding new fields to each user's contact information.

1. On the computer that hosts the IBM Lotus Domino server, navigate to <*drive*>:\Program Files\Lotus\Domino .
2. Back up the **UserInfoConfig.xml** file.
3. In a text editor, open the **UserInfoConfig.xml** file.
4. Copy the following text into the **Details** section of the **UserInfoConfig.xml** file:

```
<Detail id="_doneOfficePhone1323895037773" FieldName="OfficePhoneNumber" Type="text/plain"/>
<Detail id="_doneHomePhone13238950376382" FieldName="PhoneNumber" Type="text/plain"/>
<Detail id="_doneCellPhone13238950372283" FieldName="CellPhoneNumber" Type="text/plain"/>
<Detail id="_doneManager13238950374224" FieldName="Manager" Type="text/plain"/>
<Detail id="_doneDepartment1323895037989" FieldName="Department" Type="text/plain"/>
<Detail id="_doneWorkAddress13238950373371" FieldName="OfficeStreetAddress" Type="text/plain"/>
<Detail id="_doneWorkZip13238950371864" FieldName="OfficeZip" Type="text/plain"/>
<Detail id="_doneWorkState13238950373463" FieldName="OfficeState" Type="text/plain"/>
<Detail id="_doneWorkCity1323895037436" FieldName="OfficeCity" Type="text/plain"/>
<Detail id="_doneHomeAddress1323895037196" FieldName="StreetAddress" Type="text/plain"/>
<Detail id="_doneHomeZip13238950375909" FieldName="Zip" Type="text/plain"/>
<Detail id="_doneHomeState13238950377713" FieldName="State" Type="text/plain"/>
<Detail id="_doneHomeCity13238950378707" FieldName="City" Type="text/plain"/>
<Detail id="_doneLoginId13238950371796" FieldName="ShortName" Type="text/plain"/>
```

5. Copy the following text into the **ParamsSets** section of the **UserInfoConfig.xml** file:

```
<Set Set id="_done2132389503733320"
params="MailAddress,Name,Title,Location,Telephone,Photo,Company,OfficePhone,HomePhone,CellPhone,Manag
er,Department,HomeAddress,HomeZip,HomeState,HomeCity,WorkAddress,WorkZip,WorkCity,WorkState,LoginId"/>
```

6. Save the **UserInfoConfig.xml** file.
7. Restart the IBM Lotus Domino server.
8. To verify that the new fields were added to each user's contact information, perform the following actions:
   1. Create a test user account in the IBM Lotus Domino Directory.
   2. Using the IBM Lotus Sametime administration web page, change the test user account by typing values for the contact information fields.
   3. In a browser, type **http://*<Sametime_Server_Name>*/servlet/UserInfoServlet?operation=3&setid=2&userid=*<Test_Account_Name>*** .
   4. Verify that the output includes the fields that you added.

After you finish: Using the IBM Lotus Sametime administration web page, change each user's contact information to include information for the fields that you added.

Managing a BlackBerry Domain 32

Restarting BlackBerry Enterprise Server components

When you complete certain tasks, you need to restart one or more BlackBerry Enterprise Server components. You restart the BlackBerry Enterprise Server components using the BlackBerry Administration Service or Windows services.

BlackBerry Enterprise Server component	Component name in the BlackBerry Administration Service	Associated service in Windows Services
BlackBerry Messaging Agent, BlackBerry Controller, and BlackBerry Dispatcher	BlackBerry Enterprise Server	BlackBerry Controller and BlackBerry Dispatcher
BlackBerry Collaboration Service	Collaboration	BlackBerry Collaboration Service
BlackBerry Synchronization Service	Synchronization	BlackBerry Synchronization Service
BlackBerry Attachment Service	Attachment Service	BlackBerry Attachment Service
BlackBerry MDS Connection Service	MDS Connection Service	BlackBerry MDS Connection Service
BlackBerry Monitoring Service	–	• BlackBerry Monitoring Service - Application Core • BlackBerry Monitoring Service - Data Collection Subsystem • BlackBerry Monitoring Service - Polling Engine
BlackBerry Router	–	BlackBerry Router
BlackBerry Policy Service	Policy	BlackBerry Policy Service

BlackBerry Enterprise Server component	Component name in the BlackBerry Administration Service	Associated service in Windows Services
BlackBerry Administration Service	BlackBerry Administration Service	• BlackBerry Administration Service - Application Server • BlackBerry Administration Service - Native Code Container
BlackBerry Web Desktop Manager	BlackBerry Administration Service	• BlackBerry Administration Service - Application Server • BlackBerry Administration Service - Native Code Container

Restart a BlackBerry Enterprise Server component using the BlackBerry Administration Service

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Expand the component that you want to restart.
3. Click an instance.
4. Click **Restart instance**.

Restart a BlackBerry Enterprise Server component using Windows Services

1. On each computer that hosts the BlackBerry Enterprise Server component, in the Windows Services, restart the services for the component.
2. If you want to restart all of the BlackBerry Enterprise Server components, you must restart the Windows Services in the following order:
   - BlackBerry Administration Service - Application Server
   - BlackBerry Administration Service - Native Code Container
   - BlackBerry Mail Store Service
   - BlackBerry Instant Messaging Connector
   - BlackBerry MDS Connection Service

- BlackBerry Dispatcher
- BlackBerry Attachment Service
- BlackBerry Controller
- All of the remaining services for BlackBerry Enterprise Server components

Best practice: Restarting more than one BlackBerry Administration Service instance

To restart all BlackBerry Administration Service instances without issues, the best practice is to stop all instances before you begin restarting the instances.

If you must keep at least one BlackBerry Administration Service instance running while you restart all instances, you should restart the instances one at a time and verify that each instance that you restart is running before you restart the next instance.

Using the BlackBerry Enterprise Trait Tool

The BlackBerry Enterprise Trait Tool is a stand-alone command line tool that you can use to configure specific BlackBerry Enterprise Server traits. You can configure most BlackBerry Enterprise Server settings using the BlackBerry Administration Service, but you must use the BlackBerry Enterprise Trait Tool to configure specific settings that are not available in the BlackBerry Administration Service.

The BlackBerry Enterprise Trait Tool file is located in the installation files for the BlackBerry Enterprise Server and is named TraitTool.exe. You must launch the TraitTool.exe file using a Windows command prompt.

Use the BlackBerry Enterprise Trait Tool

1. Copy the BlackBerry Enterprise Server installation files to a computer that hosts a BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to <*extracted_folder*>\tools.
4. Perform one of the following actions:

Task	Steps
Display the current version of the trait tool and a summary of valid commands.	Type **traittool**.
Display all possible traits, the expected data types, and any value restrictions.	Type **traittool -show**.
Display a list of traits that were configured in the BlackBerry Domain.	Type **traittool** {*} **-list**.
Configure the value of a trait in the BlackBerry Domain specified.	Type **traittool** {*} **-trait** <*trait name*> **-set** <*value*>.
Erase the value of a trait.	Type **traittool** {*} **-trait** <*trait name*> **-erase**.

Replace the braces and asterisk {*} with one or more of the following command line options:

- **-global** to specify all BlackBerry Enterprise Server instances in the BlackBerry Domain
- **-agent** <*agent id*> to specify the ID for the BlackBerry Messaging Agent
- **-group** <*groups_name*> to specify a group of BlackBerry device users
- **-host** <*host_name*> to specify a pair of high availability BlackBerry Enterprise Server instances
- **-user** <*smtp_address*> to specify one user
- **-server** <*server_name*> to specify a BlackBerry Enterprise Server instance
- **-basserver** <*name*> to specify the computer that hosts the BlackBerry Administration Service

5. Press ENTER.
6. Restart the BlackBerry Enterprise Server component that is associated with the trait that you configured.

BlackBerry Enterprise Trait Tool traits

The BlackBerry Enterprise Trait Tool includes the following traits that you can change to meet the requirements of your organization's environment:

Trait	Description
ACPByteSizeDeviceVersion	This trait specifies the minimum version of the BlackBerry Device Software that can receive 8 bytes of ACP data. The typical amount of

Trait	Description
	ACP data that BlackBerry devices can receive is 4 bytes. The BlackBerry Enterprise Server check-s the value of this trait to find out how many bytes of ACP data to send to devices. If the version of the BlackBerry Device Software that the device is running is earlier than the version that this trait specifies, the BlackBerry Enterprise Server sends the device 4 bytes of ACP data instead of 8 bytes. If you do not configure this trait, the BlackBerry Enterprise Server sends 8 bytes of ACP data to the device.
ActiveDirectoryLDAPConnectTimeout	This trait specifies the number of seconds that the BlackBerry Administration Service waits for the BlackBerry Administration Service and the Microsoft Active Directory to connect over LDAP before the connection times out. The default value is 5.
BASIsProxyWPADOptionEnabled	This trait specifies whether the BlackBerry Administration Service uses the Web Proxy Autodiscovery protocol to discover proxy servers automatically. If you want to enable the Web Proxy Autodiscovery protocol, change the value to 1. If you want to disable the Web Proxy Autodiscovery protocol, change the value to 0. If you do not change the value to 1, the Web Proxy Autodiscovery protocol is not enabled. For more information, see Configure the BlackBerry Administration Service to use Web Proxy Autodiscovery Protocol to discover a proxy server .
BASNumberOfAdditionalWiredApplicationsToIncludeInACP	This trait specifies the number of additional wired applications to include in the application control policy when reconciling applications.
BASPASBundleRequestVersionSupport	This trait specifies the version of the BundleRequest.xml file that the BlackBerry Infrastructure supports. The default version is 1.0.
BASProxyBasicAuthPassword and BASProxyBasicAuthUID	If the BlackBerry Administration Service uses HTTP basic authentication to authenticate with a proxy server, these traits specify the password and user name that the BlackBerry Administration Service can use. You can specify the password and user name for a BlackBerry Administration Service instance, or for all the BlackBerry Administration Service instances in the BlackBerry Domain. If you do

Trait	Description
	not configure these traits, you cannot use HTTP basic authentication for proxy authentication. For more information, see Configure the BlackBerry Administration Service to use HTTP basic authentication .
CalendarRescanInterval	This trait specifies the amount of time, in minutes, that can occur between the scans that the BlackBerry Enterprise Server performs on the calendar contents on the device. When the amount of time between scans expires, the BlackBerry Enterprise Server synchronizes the calendar contents on the device with the calendar contents in the user's email application. If the BlackBerry Enterprise Server detects any differences between the calendar contents, the BlackBerry Enterprise Server synchronizes the differences. The default value is 15.
EnableLegacyProfileConfig	This trait specifies how the BlackBerry Messaging Agent modifies MAPI profile settings when you install the BlackBerry Enterprise Server. If you want the BlackBerry Messaging Agent to modify the MAPI profile settings that the BlackBerry Enterprise Server requires for BlackBerry Enterprise Server version 4.1 SP6 and earlier, set the trait to true (1). The default value is false (0), the BlackBerry Messaging Agent modifies the MAPI profile settings by configuring the reconnect settings for the global catalog server that are required for global catalog referrals for Microsoft Exchange Server 2007.
EWSCASURL	This trait specifies whether the BlackBerry Messaging Agent uses a specific web address to access the client access server for Microsoft Exchange. You can configure this trait for all BlackBerry Messaging Agent instances on a specific BlackBerry Enterprise Server, or all BlackBerry Messaging Agent instances on all BlackBerry Enterprise Server instances. If you do not configure this trait, the BlackBerry Messaging Agent uses the service to find the client access server for Microsoft Exchange. For more information, see Configure the BlackBerry Messaging Agent instances to use a specific web address for a client access server for Microsoft Exchange .
EWSDomain	This trait specifies the domain name to use with the Service Account if you configure the EWSServiceAccount trait.

Trait	Description
EWSEnable	This trait specifies how the BlackBerry Enterprise Server manages calendars on devices. You can configure this trait for a specific BlackBerry Messaging Agent, all BlackBerry Messaging Agent instances on a specific BlackBerry Enterprise Server, or all BlackBerry Messaging Agent instances on all BlackBerry Enterprise Server instances. If you want the BlackBerry Enterprise Server to use only Microsoft Exchange Web Services to manage calendars on devices, change the value to true (1). If you want the BlackBerry Enterprise Server to use only MAPI and CDO libraries to manage calendars on devices, change the value to false (0). If you want the BlackBerry Enterprise Server to use Microsoft Exchange Web Services whenever possible and MAPI and CDO libraries when using Microsoft Exchange Web Services is not possible, delete the trait value which restores the default setting. For more information, see Configure the BlackBerry Enterprise Server to use Microsoft Exchange Web Services , and Configure the BlackBerry Enterprise Server to use MAPI and CDO libraries.
EWSMaxWorkerThreads	This trait specifies how many worker threads Microsoft Exchange Web Services uses. This trait is valid for BlackBerry Enterprise Server 5.0 SP1. The default value is 27.
EWSPassword	This trait specifies the password to use with the Service Account if you configure the EWSServiceAccount trait.
EWSSCPURL	This trait specifies whether the BlackBerry Messaging Agent uses a specific web address to access the service. You can configure this trait for all BlackBerry Messaging Agent instances on a specific BlackBerry Enterprise Server, or all BlackBerry Messaging Agent instances on all BlackBerry Enterprise Server instances. If you do not configure this trait, the BlackBerry Messaging Agent uses a web address to access the service that the record lookup for the Microsoft Active Directory Service Connection Point provides. For more information, see Configure the BlackBerry Messaging Agent instances to use a web address for a specific service.

Trait	Description
EWSServiceAccount	Service account name that you can use to connect to Microsoft Exchange Web Services to impersonate all other BlackBerry Enterprise Server users.
EWSUserAvailabilityAccess	This trait specifies whether the BlackBerry Messaging Agent receives the user's status using Microsoft Exchange Web Services or by searching for the information in the Microsoft Exchange public folders. You can configure this trait for a specific BlackBerry Messaging Agent, all BlackBerry Messaging Agent instances on a specific BlackBerry Enterprise Server, or all BlackBerry Messaging Agent instances on all BlackBerry Enterprise Server instances. If you want the BlackBerry Messaging Agent to receive the user's status using Microsoft Exchange Web Services, change the value to EWS. The default value is PF, the BlackBerry Messaging Agent receives the user's status using Microsoft Exchange public folders. For more information, see Configure the BlackBerry Messaging Agent instances to look up a user's status using only Microsoft Exchange Web Services .
ExchangeDisableConfirmEmailDelivery	This trait specifies whether a user can append the word "confirm" to the subject of email messages to receive an automatic confirmation that the email message is delivered to the intended recipient. If you want to permit the BlackBerry Messaging Agent to send confirmations automatically when the BlackBerry Messaging Agent delivers email messages, change the value to false (0). If you want to prevent the BlackBerry Messaging Agent from sending confirmations automatically when the BlackBerry Messaging Agent delivers email messages, change the value to true (1). The default value is false (0), the BlackBerry Messaging Agent sends confirmations automatically when the BlackBerry Messaging Agent delivers email messages.
ExchangeEnableMLangConversion	This trait specifies whether the BlackBerry Messaging Agent uses the Microsoft Multi Language Support DLL to perform character set conversions. If you want the BlackBerry Messaging Agent to use Microsoft Multi Language Support DLL, change the value to true (1). The default value is false (0).
ExchangeEnableWriteUserStatsToMailbox	This trait specifies whether the BlackBerry Messaging Agent writes statistics to each user's Microsoft Exchange mailbox when it processes email messages for users. By default, to reduce the

Trait	Description
	workload on the Microsoft Exchange Server, BlackBerry Messaging Agent 5.0 SP2 or later does not write statistics to user mailboxes when it processes email messages. If you want the BlackBerry Messaging Agent to write statistics to users' Microsoft Exchange mailboxes, change the value to true (1). By default, the value is false (0). If you change this value, the result might be an impact on the performance of your organization's BlackBerry Enterprise Server environment and the Microsoft Exchange Server. For more information, see Permit the BlackBerry Messaging Agent to write statistics to Microsoft Exchange mailboxes.
ExchangeSmartSyncDays	This trait specifies how many days in the calendar, after the current date, that the BlackBerry Enterprise Server checks for calendar errors on devices. You can configure the BlackBerry Enterprise Server to check for calendar errors for a user account, all user accounts that you associate with a BlackBerry Enterprise Server, or all user accounts. The default value is 7. For more information, see Configure the period of days to check for calendar synchronization errors.
ExchangeSmartSyncEnable	This trait specifies whether the BlackBerry Enterprise Server checks for calendar errors on devices. The BlackBerry Enterprise Server checks for calendar errors on devices for all user accounts. If you don't want the BlackBerry Enterprise Server to check for calendar errors on devices, change the value to false (0) for a specific user account, all user accounts that are associated with a BlackBerry Enterprise Server, or all user accounts. The default value is true (1), the BlackBerry Enterprise Server checks for calendar errors on devices. For more information, see Turn off corrective calendar synchronization process.
ExchangeSmartSyncSchedule	This trait specifies when the calendar synchronization process runs. You can configure the calendar synchronization process to start running on multiple recurring days or on only one recurring day for a user account, all user accounts that you associate with a BlackBerry Enterprise Server, or all user accounts.

Trait	Description
	The default value is Daily. For more information, see Configure when corrective calendar synchronization runs.
ExchangeSmartSyncSendUpdate	This trait specifies whether the calendar synchronization process writes calendar synchronization errors to the BlackBerry Messaging Agent log file, or writes the errors to the log file and corrects the calendar synchronization errors on devices. If you don't want the BlackBerry Messaging Agent to correct calendar synchronization errors automatically, change the value to false (0) for a specific user account, all user accounts that you associate with a BlackBerry Enterprise Server, or all user accounts. The default value is true (1), the BlackBerry Messaging Agent corrects calendar synchronization errors automatically. For more information, see Turn off automatic error correction in corrective calendar synchronization.
ExchangeSmartSyncTriggerHour	This trait specifies when the BlackBerry Enterprise Server checks for calendar synchronization errors on devices. You can configure the BlackBerry Enterprise Server to check for calendar synchronization errors on devices at a specific hour for a specific user account, all user accounts that you associate with a BlackBerry Enterprise Server, or all user accounts. The default value is 0, the BlackBerry Enterprise Server checks for calendar synchronization errors on devices at 12:00 AM. For more information, see Configure when corrective calendar synchronization runs.
ExchangeSuppressBodyOfSentItems	This trait specifies whether the body of an email message is included in an email message sent to a device when the BlackBerry Enterprise Server synchronizes email messages sent by an email application. The default value is false (0), the body of an email message is sent to a device.
MailstoreAddressRefreshEnabled	This trait specifies whether you want the BlackBerry Mail Store Service to update the user directory in the BlackBerry Configuration Database. If you want the BlackBerry Mail Store Service to update the user directory in the BlackBerry Configuration Database, change the value to true (1). If you do not want the BlackBerry Mail Store Service

Trait	Description
	to update the user directory in the BlackBerry Configuration Database, change the value to false (0). The default value is true (1), the BlackBerry Mail Store Service updates the user directory in the BlackBerry Configuration Database. For more information, see Configure the BlackBerry Mail Store Service instance that updates the contact list.
MailstorePublicFolderLookupEnabled	This trait specifies whether the BlackBerry Administration Service looks up public folders and displays them in the list of public contact folders. When an organization has a large number of public folders available, it can take longer than expected for the BlackBerry Messaging Agent to display the folders and the BlackBerry Administration Service might time out. If you want to turn off the look up function, change the value to false (0). If you turn off the look up function, you can access the BlackBerry Messaging Agent in the BlackBerry Administration Service but you cannot see the list of available public folders in the Email component page in the BlackBerry Administration Service. The default value is true (1), the BlackBerry Administration Service looks up public folders.
MaxDomainSlowSyncsPerMin	This trait specifies the maximum number of full synchronization events that the BlackBerry Synchronization Service can process each minute, in a BlackBerry Domain. The default value is 300.
MaxPollCycleCountForHungSlowSync	This trait specifies the maximum number of times that the BlackBerry Synchronization Service polls a device to determine if there is a hung synchronization event. The default value of 10.
MaxPollCycleCountForNoResponseToSlowSync	This trait specifies the maximum number of times that the BlackBerry Synchronization Service polls a device to determine if the device is out of a wireless coverage area or if wireless synchronization is disabled on the device. The default value is 2.
MaxSyncServerSlowSyncsInProcess	This trait specifies the maximum number of full synchronization events that a BlackBerry Synchronization Service can start before it schedules more full synchronization events.

Trait	Description
	The default value is 10.
MaxSyncServerSlowSyncsPerMin	This trait specifies the maximum number of pending full synchronization events that the BlackBerry Synchronization Service can process each minute. The default value is 30.
MonitorJunkEmailFolderForETP	This trait specifies whether the BlackBerry Messaging Agent monitors the Junk folder and the Inbox for email messages that include an etp.dat attachment. When the activation process over the wireless network begins, the BlackBerry Enterprise Server sends an email message that includes an etp.dat attachment from the blackberry.net domain to the email account of the user. In some scenarios, anti-spam software applications that the messaging server or gateway uses filters the email messages and places them in the Junk folder. If you do not want the BlackBerry Enterprise Server to monitor the Junk folder for activation messages, change the value to false (0) and restart the BlackBerry Controller. The default value is true (1), the BlackBerry Enterprise Server monitors the Junk folder for activation messages.
NumberOfUserTargetTypeForSlowSyncInParallel	This trait specifies how many different types of organizer data, such as tasks, memos, and contacts, the BlackBerry Synchronization Service can synchronize at the same time during a full synchronization event. The default value is 10.
PolicySRPWhitelist	This trait specifies a list of calendar services, messaging services, and browser services that a device can connect to when you turn off the Allow Other Browser Services IT policy rule. To specify a list of services that the device can connect to, type the SRP IDs of the services. Separate the SRP IDs with a comma (,). The default value is empty, a device cannot connect to calendar services, messaging services, and browser services that your organization does not provide.
PolicyEnterpriseWipeCommandOrderTraitType	This trait specifies the order for commands that run when the BlackBerry Policy Service sends the "Delete only the organization data and remove device" IT administration command to a device. The value is a string that contains the command IDs separated by a colon (:), for example, commandId1:commandId2.

Trait	Description
	The default value is 3:18. Contact a BlackBerry Technical Support representative before you change the default value of this trait.
PolicyThrottlingAppPush	This trait specifies whether the BlackBerry Policy Service uses throttling to send applications the same way that it throttles IT policies and service books. If you want the BlackBerry Policy Service to send applications using throttling in the same way that it throttles IT policies and service books, change the value to true (1). If you do not want the BlackBerry Policy Service to send applications using throttling in the same way that it throttles IT policies and service books, change the value to false (0). The default value is false (0), the BlackBerry Policy Service does not use throttling to send applications the same way that it throttles IT policies and service books. For more information, see Configure BlackBerry Policy Service throttling for application polling.
PolicyThrottlingInProcessJobs	This trait specifies the maximum number of processes for IT policies or processes for service books that a BlackBerry Policy Service can run at one time before the BlackBerry Policy Service schedules additional processes for IT policies or service books. The default value is 30. For more information, see Configure BlackBerry Policy Service throttling for IT policies and service books.
PolicyThrottlingMaxBESJobs	This trait specifies the maximum number of IT policies and service books that a BlackBerry Policy Service can send to devices each minute. The default value is 100. For more information, see Configure BlackBerry Policy Service throttling for IT policies and service books.
PolicyThrottlingMaxDomainJobs	This trait specifies the maximum number of IT policies and service books that all BlackBerry Policy Service instances can send to devices each minute. The default value is 300. For more information, see Configure BlackBerry Policy Service throttling for IT policies and service books.

Trait	Description
PolicyThrottlingP2PKeyRate	This trait specifies the maximum number of processes for PIN encryption keys that a BlackBerry Policy Service can process at one time before the BlackBerry Policy Service schedules additional processes for PIN encryption keys. The default value is 60. For more information, see Configuring BlackBerry Policy Service throttling for PIN encryption keys.
RouterAutoDiscoveryMethod	This trait specifies the method that the BlackBerry Enterprise Server uses to update the list of BlackBerry Router instances in the BlackBerry Configuration Database. If you want the BlackBerry Enterprise Server to compile the list of BlackBerry Router instances automatically, change the value to true (1). If you want the BlackBerry Router instances to provide the BlackBerry Enterprise Server with the list of BlackBerry Router instances, change the value to false (0). The default value is true (1), the BlackBerry Enterprise Server compiles the list of BlackBerry Router instances automatically.
SlowSyncPollCycleInterval	This trait specifies the interval (in minutes) between the times that the BlackBerry Synchronization Service reviews the list of users, to determine how many pending full synchronization events can be scheduled based on the throttling parameters. The default value is 2.
ServerHealthPercentage	This trait specifies the percentage of messaging servers that are healthy. The BlackBerry Dispatcher uses this trait to change the Connection to the messaging server(s) health parameter. If this health parameter indicates that the primary BlackBerry Enterprise Server is unhealthy and you turn on automatic failover, the BlackBerry Enterprise Server starts the failover process. You can change the percentage for this trait to customize the percentage of messaging servers that must be unhealthy before an automatic failover occurs in your organization's environment. The default value is 75%. For more information, see Change when automatic failover occurs by customizing the health parameters for user accounts and messaging servers.

Trait	Description
UserHealthPercentage	This trait specifies the percentage of user accounts that are healthy. The BlackBerry Dispatcher uses this trait to change the User accounts health parameter. If either of the health parameters indicate that the primary BlackBerry Enterprise Server is unhealthy and you turn on automatic failover, the BlackBerry Enterprise Server starts the failover process. You can change the percentage for this trait to customize the percentage of user accounts that must be unhealthy before an automatic failover occurs in your organization's environment. The default value is 75%. For more information, see Change when automatic failover occurs by customizing the health parameters for user accounts and messaging servers.

Related information

Using the BlackBerry Enterprise Trait Tool, 394

Permit the BlackBerry Messaging Agent to write statistics to Microsoft Exchange mailboxes

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. If you want the BlackBerry Messaging Agent to function as it did in previous versions, you can permit the BlackBerry Messaging Agent to write statistics to each user's Microsoft Exchange mailbox. Permitting the BlackBerry Messaging Agent to write statistics might have an impact on the performance of your organization's BlackBerry Enterprise Server environment and the Microsoft Exchange Server.

1. Copy the BlackBerry Enterprise Server installation files to a computer that hosts a BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to the folder that contains the TraitTool.exe file.
4. Perform one of the following actions:

- To permit all BlackBerry Messaging Agent instances to write statistics to users' Microsoft Exchange mailboxes, type **TraitTool -global -trait ExchangeEnableWriteUserStatsToMailbox -set true**.
- To permit all BlackBerry Messaging Agent instances that are associated with a specific BlackBerry Enterprise Server to write statistics to users' Microsoft Exchange mailboxes, type **TraitTool -server** <***server_name***> **-trait ExchangeEnableWriteUserStatsToMailbox -set true**.

5. Press ENTER.

After you finish: If you do not want BlackBerry Messaging Agent instances to write statistics to each user's Microsoft Exchange mailbox, type **TraitTool -<level> -trait ExchangeEnableWriteUserStatsToMailbox -set false**, where <*level*> is the server name of a specific BlackBerry Enterprise Server, or global for all BlackBerry Messaging Agent instances.

Managing BlackBerry CAL keys

BlackBerry CAL keys control how many user accounts can exist on a BlackBerry Enterprise Server at the same time. If you exceed the number of user accounts that can exist on a BlackBerry Enterprise Server, the BlackBerry Administration Service informs you that you require more BlackBerry CAL keys.

If you use a temporary evaluation version of a BlackBerry CAL key and the BlackBerry CAL key expires, the BlackBerry Dispatcher stops all synchronization between the BlackBerry Enterprise Server and BlackBerry devices. You must purchase a new BlackBerry CAL key before you can restart the BlackBerry Dispatcher. If you use a temporary evaluation version of a CAL key, you cannot reuse the temporary BlackBerry CAL key after you purchase a permanent BlackBerry CAL key.

To help you transfer BlackBerry CAL keys to computers in other BlackBerry Domain instances or troubleshoot BlackBerry CAL key issues, copy the BlackBerry CAL keys from the BlackBerry Administration Service to a text file.

Add or delete a BlackBerry CAL key

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service**.
3. Click **Edit component**.
4. In the **License key** section, perform one of the following actions:
    - To add a BlackBerry CAL key, type the information for the BlackBerry CAL key. Click the **Add** icon.
    - To delete a BlackBerry CAL key, click the **Delete** icon.
5. Click **Save all**.

Copy a BlackBerry CAL key to a text file

You can copy a BlackBerry CAL key to a text file and save it on a computer for reference if you want to transfer CAL keys to a different BlackBerry Enterprise Server or troubleshoot BlackBerry CAL key issues.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **BlackBerry Administration Service**.
3. Click **Edit component**.
4. In the **License key** section, highlight and right-click the BlackBerry CAL key.
5. Click **Copy**.
6. Open a text editor.
7. Paste the BlackBerry CAL key into the file.
8. Save the file.

Configuring the BlackBerry Mail Store Service instance that updates the contact list

The BlackBerry Configuration Database contains your organization's contact list and a list of BlackBerry Enterprise Server instances. By default, the BlackBerry Mail Store Service instance that you installed with the first BlackBerry Enterprise Server instance that appears in the list updates the contact list. If you prevent the BlackBerry Mail Store Service that you installed with the first BlackBerry Enterprise Server instance from updating the contact list, the next available BlackBerry Mail Store Service instance in the list updates the contact list.

By default, if you install multiple BlackBerry Mail Store Service instances, each instance can update the contact list in the BlackBerry Configuration Database. The first BlackBerry Mail Store Service instance that updates the contact list prevents the other instances from also updating the contact list. Each BlackBerry Mail Store Service instance searches for time stamp information in the BlackBerry Configuration Database to determine if another BlackBerry Mail Store Service instance is updating the contact list already before it starts to update the contact list.

You must verify that at least one BlackBerry Mail Store Service instance can update the contact list in the BlackBerry Configuration Database so that the BlackBerry Administration Service can access the latest contact list information when you create and manage user accounts. If you prevent all of the BlackBerry Mail Store Service instances from updating the contact list, the BlackBerry Configuration Database might not contain the contact information for all user accounts on your organization's messaging server.

If the BlackBerry Configuration Database does not contain contact information for a user account, you cannot create the user account by searching for the contact information in the BlackBerry Administration Service. You can only create the user account if you use the Add from company directory option in the BlackBerry Administration Service. The Add from company directory option permits the BlackBerry Mail Store Service to search the contact information that is stored in the messaging environment so that you can create the user account even if the BlackBerry Configuration Database does not contain the contact information for the user account.

Configure the BlackBerry Mail Store Service instance that updates the contact list

1. Copy the BlackBerry Enterprise Server installation media to a computer that hosts a BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to <*extracted_folder*>\tools.
4. Perform one of the following actions:
    - To permit a BlackBerry Mail Store Service instance to update the contact list, type **Traittool -host *<instance_name>* -trait MailstoreAddressRefreshEnabled -set true**, where <*instance_name*> is the name of the BlackBerry Enterprise Server instance that you installed the BlackBerry Mail Store Service with.
    - To prevent a BlackBerry Mail Store Service instance from updating the contact list, type **Traittool -host *<instance_name>* -trait MailstoreAddressRefreshEnabled -set false**, where <*instance_name*> is the name of the BlackBerry Enterprise Server instance that you installed the BlackBerry Mail Store Service with.
5. Repeat step 4 for each BlackBerry Mail Store Service instance.

Configuring a Hosted BlackBerry services environment

Hosted BlackBerry services permit you to make the BlackBerry Enterprise Server that is in your organization's environment available to other organizations (for example, SMBs). When you include Hosted BlackBerry services in your organization's environment, one or more organizations can subscribe to your organization's BlackBerry Enterprise Server.

If your organization hosts a BlackBerry Enterprise Server and multiple organizations subscribe to Hosted BlackBerry services, you must customize the BlackBerry Enterprise Server so that BlackBerry device users can access only their organization’s contact list and restrict users from accessing the contact information of other organizations that also subscribe to the Hosted BlackBerry services.

If your organization permits customers to have limited access or read-only access to the Microsoft Active Directory, you can configure the BlackBerry Enterprise Server to use MAPI, LDAP, or both to retrieve recipients’ email addresses. If your organization permits customers to have full control of subtrees in Microsoft Active Directory and you configured Microsoft Active Directory for multi-tenancy, you can configure the BlackBerry Enterprise Server to limit the scope of the LDAP search.

To configure Hosted BlackBerry services, you must use a licensing model for the BlackBerry Enterprise Server that is specific for Hosted BlackBerry services.

For more information about Hosted BlackBerry services, see the *BlackBerry Enterprise Server Planning Guide*.

Related information

Configuring the BlackBerry Enterprise Server to use LDAP to retrieve email addresses and organizer data, 412

Configuring Hosted BlackBerry services when you permit your organization’s customers limited access to Microsoft Active Directory

If you configure Hosted BlackBerry services, you must make sure that the name of the organization that each BlackBerry device user belongs to is listed accurately and consistently in the entry for each user in Microsoft Active Directory. For example, if the organization’s name appears as an acronym in some entries but in expanded form in others, the BlackBerry Enterprise Server might return inaccurate search results. If a user tries to search for another user's contact information but you did not specify the name of the organization that the other user belongs to in Microsoft Active Directory, the BlackBerry Enterprise Server does not return any search results.

You can specify the organization name in the entry for each user in an LDAP field such as the Company Name field. If you specify the organization’s name in a field other than the Company Name field, you must specify the name of the LDAP field when you configure Hosted BlackBerry services. If you do not specify an LDAP field, the BlackBerry Enterprise Server uses the Company Name field to search for contact information.

Configure Hosted BlackBerry services when you permit your organization’s customers limited access to Microsoft Active Directory

Before you begin: Configure the BlackBerry Enterprise Server to retrieve email addresses using LDAP.

1. On the computer that hosts the BlackBerry Enterprise Server, click **Start** > **Run**.
2. Type **regedit**. Click **OK**.
3. Perform one of the following actions:
    - If you are running a 32-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\Research In Motion \BlackBerry Enterprise Server\Agents.

- If you are running a 64-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\WOW6432Node\Research In Motion\BlackBerry Enterprise Server\Agents.

4. Create a DWORD value named **HostedServer**.
5. Change the value to **1**.
6. In the Windows Services, restart the BlackBerry Controller.

Related information

Configuring the BlackBerry Enterprise Server to use LDAP to retrieve email addresses and organizer data, 412

Restarting BlackBerry Enterprise Server components, 392

Configure the BlackBerry Enterprise Server to resolve email addresses using an LDAP field that is not the Company Name field

1. On the computer that hosts the BlackBerry Enterprise Server, click **Start** > **Run**.
2. Type **regedit**. Click **OK**.
3. Perform one of the following actions:
   - If you are running a 32-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\Research In Motion\BlackBerry Enterprise Server\Agents.
   - If you are running a 64-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\WOW6432Node\Research In Motion\BlackBerry Enterprise Server\Agents.
4. Create a String value named **LDAPCompanyField**.
5. Specify the name of the LDAP field that contains the name of your organization's customers as the value.
6. In the Windows Services, restart the BlackBerry Controller.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configure Hosted BlackBerry services when your organization’s customers have full control of their subtree in Microsoft Active Directory

You can configure the BlackBerry Enterprise Server to search for contact information or calendar availability within subtrees in a Microsoft Active Directory that you configured for multi-tenancy. When you configure the BlackBerry Enterprise Server to search within subtrees, the BlackBerry Enterprise Server searches the Microsoft Active Directory using the organizational unit information that is included in the distinguished name of the BlackBerry device users.

Before you begin:

- Configure the BlackBerry Enterprise Server to retrieve email addresses using LDAP.
- Verify that the BlackBerry Enterprise Server version is version 5.0 SP2 or later.

1. On the computer that hosts the BlackBerry Enterprise Server, click **Start** > **Run**.
2. Type **regedit**. Click **OK**.
3. Perform one of the following actions:
    - If you are running a 32-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\Research In Motion \BlackBerry Enterprise Server\Agents.
    - If you are running a 64-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\WOW6432Node \Research In Motion\BlackBerry Enterprise Server\Agents.
4. Create a DWORD value named **LDAPUseScopedSearch**.
5. Change the value to **1**.
6. In the Windows Services, restart the BlackBerry Controller.

Related information

Configuring the BlackBerry Enterprise Server to use LDAP to retrieve email addresses and organizer data, 412
Restarting BlackBerry Enterprise Server components, 392

Configuring the BlackBerry Enterprise Server to use LDAP to retrieve email addresses and organizer data

By default, when BlackBerry device users search for recipients' email addresses or organizer data, the BlackBerry Enterprise Server uses MAPI to connect to the Microsoft Exchange Server and retrieve the email addresses or organizer data that is stored in Microsoft Active Directory. You can configure the BlackBerry Enterprise Server to use LDAP to connect to Microsoft Active Directory directly to retrieve email addresses, organizer data, or both.

When you configure the BlackBerry Enterprise Server to use LDAP to retrieve email addresses and organizer data, you help reduce the MAPI connections that the BlackBerry Enterprise Server requires which helps improve the performance of the BlackBerry Enterprise Server and Microsoft Exchange Server. In a Microsoft Exchange 2010 environment, if you configure the BlackBerry Enterprise Server to use LDAP, you cannot migrate users to different forests.

If you configure Hosted BlackBerry services, you must configure the BlackBerry Enterprise Server to use LDAP to retrieve email addresses.

You can configure the following options when you configure the BlackBerry Enterprise Server to use LDAP to retrieve email addresses and organizer data:

- Windows domain that the Microsoft Active Directory uses
- whether to use LDAPS to connect to Microsoft Active Directory
- timeout value for the connection to Microsoft Active Directory
- which contacts the BlackBerry Enterprise Server cannot retrieve, if required
- whether to support a Microsoft Active Directory that you configured for multi-tenancy, if required
- custom field to use to resolve email addresses for Hosted BlackBerry services, if required
- baseDN of the Microsoft Active Directory tree, if required

Related information

Configuring a Hosted BlackBerry services environment, 409

Configure the BlackBerry Enterprise Server to connect to Microsoft Active Directory

1. On the computer that hosts the BlackBerry Enterprise Server, click **Start** > **Run**.
2. Type **regedit**. Click **OK**.
3. Perform one of the following actions:
   - If you are running a 32-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\Research In Motion \BlackBerry Enterprise Server\Agents.
   - If you are running a 64-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\WOW6432Node \Research In Motion\BlackBerry Enterprise Server\Agents.
4. If your organization’s environment includes multiple Windows domains, perform the following actions:
   a. Create a String value named **LDAPDomain**.
   b. Change the value to the FQDN of the global catalog server and the port number that the BlackBerry Enterprise Server can use to resolve the DNS name of Microsoft Active Directory, using the following format: <*FQDN_of_GC*>:<*port*>. If the BlackBerry Enterprise Server must connect to multiple global catalog servers for DNS name resolution, specify all of them as the value, using the following format: <*FQDN_of_GC1*>:<*port*> <*FQDN_of_GC2*>:<*Port*> <*FQDN_of_GC3*>:<*port*>. Separate multiple entries using spaces.

      Optionally, if you do not want to configure a limited list of global catalog servers, set the value to a domain name, and the port number to the global catalog server (for example, example.com:3268).
5. If the BlackBerry Enterprise Server must use a specific port to connect to Microsoft Active Directory and you did not specify the port number in the LDAPDomain string, perform the following actions:
   a. Create a DWORD value named **LDAPport**.

   b. Change the value to the port number. To limit the number of LDAP queries that the BlackBerry Enterprise Server needs, use the port number of the global catalog server (port 3268).

6. If the BlackBerry Enterprise Server must use LDAPS to connect to the Microsoft Active Directory, perform the following actions:
   a. Create a DWORD value named **LDAPssl**.
   b. Change the value to **1**.

7. To change the amount of time that the BlackBerry Enterprise Server waits for a response from Microsoft Active Directory before the connection times out (by default, 10 seconds), perform the following actions:
   a. Create a DWORD value named **LDAPTimeout**.
   b. Change the value to the timeout period, in seconds, that your organization requires.

8. In the Windows Services, restart the BlackBerry Controller.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configure the BlackBerry Enterprise Server to retrieve email addresses and organizer data using LDAP

1. On the computer that hosts the BlackBerry Enterprise Server, click **Start** > **Run**.
2. Type **regedit**. Click **OK**.
3. Perform one of the following actions:
   - If you are running a 32-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\Research In Motion \BlackBerry Enterprise Server\Agents.
   - If you are running a 64-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\WOW6432Node \Research In Motion\BlackBerry Enterprise Server\Agents.
4. Create a DWORD value named **LDAPSearch**.
5. Change the value to **1**.
6. To configure the BlackBerry Enterprise Server to resolve email addresses using LDAP, perform the following actions:
   a. Create a DWORD value named **LDAPALPSearch**.
   b. Change the value to **1**.

7. To configure the BlackBerry Enterprise Server to resolve organizer data using LDAP, perform the following actions:
   a. Create a DWORD value named **LDAPPIMSearch**.

b. Change the value to **1**.

8. In the Windows Services, restart the BlackBerry Controller.

Related information

Restarting BlackBerry Enterprise Server components, 392

Prevent the BlackBerry Enterprise Server from retrieving contact information for specific users

If you are required by your organization to prevent BlackBerry device users from finding contact information for specific users, you can specify a list of users that you want to prevent BlackBerry device users from finding contact information for or you can filter users using an attribute in Microsoft Active Directory.

Before you begin:

- Configure the BlackBerry Enterprise Server to resolve email addresses and organizer data information using LDAP.
- If you want to filter users using an attribute, choose an attribute in Microsoft Active Directory such as Mail or any of the extensionAttributes (extensionAttribute1 through extensionAttribute15). You can use the Active Directory Users and Computers console to change the value for the attribute to HideFromBlackBerry for all users that you do not want BlackBerry device users to find.

1. On the computer that hosts the BlackBerry Enterprise Server, click **Start** > **Run**.
2. Type **regedit**. Click **OK**.
3. Perform one of the following actions:
   - If you are running a 32-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\Research In Motion \BlackBerry Enterprise Server\Agents.
   - If you are running a 64-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\WOW6432Node \Research In Motion\BlackBerry Enterprise Server\Agents.
4. Create a String value named **LDAPALPObjectCategory**.
5. Change the value to one of the following options:
   - If your organization uses Microsoft Exchange 2007 or Microsoft Exchange 2010, use **msExchDynamicDistributionList,Group,Person))(!(<*attribute*>=HideFromBlackBerry**, where <*attribute*> is the name of the attribute that you want to filter (for example, extensionAttribute1).
   - If your organization uses earlier versions of Microsoft Exchange, use **Group,Person))(!(<*attribute*>=HideFromBlackBerry**, where <*attribute*> is the name of the attribute that you want to filter (for example, extensionAttribute1).

   You can use an asterisk (*) as a wildcard.

6. In the Windows Services, restart the BlackBerry Controller.

Related information

Restarting BlackBerry Enterprise Server components, 392

Restrict the location in Microsoft Active Directory that the BlackBerry Enterprise Server can retrieve email addresses and organizer data from

You can configure a BlackBerry Enterprise Server instance so that it searches for email addresses and organizer data only in a specified BaseDN in Microsoft Active Directory.

1. On the computer that hosts the BlackBerry Enterprise Server, click **Start** > **Run**.
2. Type **regedit**. Click **OK**.
3. Perform one of the following actions:
   - If you are running a 32-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\Research In Motion\BlackBerry Enterprise Server\Agents.
   - If you are running a 64-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\WOW6432Node\Research In Motion\BlackBerry Enterprise Server\Agents.
4. Create a String value named **LDAPBaseDN**.
5. Change the value to the BaseDN that you want the BlackBerry Enterprise Server to use (for example, ou=Waterloo,o=example,c=CA).
6. In the Windows Services, restart the BlackBerry Controller.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configuring BlackBerry Policy Service throttling

You can configure BlackBerry Policy Service throttling on a BlackBerry Enterprise Server instance to limit the database usage of the BlackBerry Policy Service when it performs the following actions:

- sends IT policies and service books that you update to all BlackBerry devices that are associated with the BlackBerry Enterprise Server instance that the BlackBerry Policy Service runs on
- sends updated PIN encryption keys to all devices that are associated with the BlackBerry Enterprise Server instance that the BlackBerry Policy Service runs on
- performs an application poll to verify whether the BlackBerry Policy Service must send applications to all devices that are associated with the BlackBerry Enterprise Server instance that the BlackBerry Policy Service runs on

You can configure BlackBerry Policy Service throttling using the BlackBerry Enterprise Trait Tool. You can access the BlackBerry Enterprise Trait Tool in the Tools folder of the BlackBerry Enterprise Server installation files.

View the current settings for BlackBerry Policy Service throttling

1. Copy the BlackBerry Enterprise Server installation files to a computer that hosts the primary BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to <*extracted_folder*>\tools.
4. Type **traittool -global -list**
5. Press ENTER.

   If the BlackBerry Enterprise Trait Tool does not list any BlackBerry Policy Service throttling traits, no BlackBerry Policy Service throttling traits have been changed from their default values.

Configuring BlackBerry Policy Service throttling for IT policies and service books

If the BlackBerry Policy Service detects that you updated an IT policy or service book in the BlackBerry Configuration Database, it schedules a task to create and deliver the IT policy or service book to BlackBerry device users that must receive the update. The BlackBerry Policy Service tries to process tasks as fast as the server permits, which can result in an unexpected increase in CPU usage and database usage.

Because you cannot synchronize multiple BlackBerry Policy Service instances on multiple BlackBerry Enterprise Server instances, an update to an IT policy or service book that affects many users on multiple BlackBerry Enterprise Server instances can increase the CPU usage and database usage significantly for a long period of time. The increased CPU usage and database usage can lead to unexpected behavior such as database updates not completing.

To avoid this scenario, you can throttle the processing of IT policies and service books. You can specify the maximum number of processes for IT policies and service books that a BlackBerry Policy Service can run at one time before the BlackBerry Policy Service schedules additional processes for IT policies and service books. You can also specify the maximum number of IT policies and service books that a BlackBerry Policy Service can send to devices each minute and the maximum number of IT policies and service books that all BlackBerry Policy Service instances can send to devices each minute.

If you configure throttling, the BlackBerry Policy Service determines which users that are associated with the BlackBerry Enterprise Server instance that the BlackBerry Policy Service runs on require a new IT policy or service book. The BlackBerry Policy Service also determines how many users to schedule for processing in the next 60 seconds. The BlackBerry Policy Service then schedules the same number of users for processing at equal intervals over the next 60 seconds to distribute the usage on the BlackBerry Configuration Database.

The BlackBerry Policy Service only applies throttling when it automatically detects updates to IT policies or service books. The BlackBerry database notification system starts automatic detection. If you configure the BlackBerry database notification system to be turned off, a five-minute timer starts automatic detection. The BlackBerry Policy Service does not apply throttling when the BlackBerry Enterprise Server requests IT policies or service books during device activation or when you request that the BlackBerry Enterprise Server send IT policies or service books to users.

Configure BlackBerry Policy Service throttling for IT policies and service books

1. Copy the BlackBerry Enterprise Server installation files to a computer that hosts the primary BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to <*extracted_folder*>\tools.
4. Perform one of the following actions:
   - To configure the maximum number of processes that a BlackBerry Policy Service can run for IT policies and services books at one time before the BlackBerry Policy Service schedules additional processes, type **traittool -global -trait PolicyThrottlingInProcessJobs -set** <***value***> , where <*value*> is 0 or greater. The default value is 30.
   - To configure the maximum number of IT policies and service books that a BlackBerry Policy Service can send to BlackBerry devices each minute, type **traittool -global -trait PolicyThrottlingMaxBESJobs -set** <***value***> , where <*value*> is 1 or greater. The default value is 100.
   - To configure the maximum number of IT policies and service books that all BlackBerry Policy Service instances can send to devices each minute, type **traittool -global -trait PolicyThrottlingMaxDomainJobs -set** <***value***> , where <*value*> is 1 or greater. The default value is 300.
5. Press ENTER.

Example: Configuring the maximum number of IT policies or service books that a BlackBerry Policy Service can send

If you want to configure the maximum number of IT policies or service books that a BlackBerry Policy Service can send to 500, type **traittool -global -trait PolicyThrottlingMaxDomainJobs -set 500.**

Configuring BlackBerry Policy Service throttling for PIN encryption keys

If the BlackBerry Policy Service detects that you updated the PIN encryption keys in the BlackBerry Configuration Database, the BlackBerry Policy Service verifies which BlackBerry device users require a new key and then schedules a certain number of users at equal intervals over the next 60 second period. The default setting is 60, or one process per second. You can adjust the number of users that the BlackBerry Policy Service schedules over the 60 second interval using throttling.

The BlackBerry Policy Service only applies throttling when it automatically detects updates to the PIN encryption keys. The BlackBerry database notification system starts automatic detection. If you turn off the BlackBerry database notification system, a five-minute timer starts automatic detection.

Configure BlackBerry Policy Service throttling for PIN encryption keys

1. Copy the BlackBerry Enterprise Server installation files to a computer that hosts the primary BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to <*extracted_folder*>\tools.
4. To configure the maximum number of processes for PIN encryption keys that a BlackBerry Policy Service can process at one time before it schedules additional processes, type **traittool -global -trait PolicyThrottlingP2PKeyRate -set *<value>*** , where <*value*> is 0 or greater. The default value is 60. If you configure a value of 0, theBlackBerry Policy Service will not throttle the processes to update PIN encryption keys.
5. Press ENTER.

Example: Configuring the maximum number of processes for PIN encryption keys

If you want to configure the maximum number of processes for PIN encryption keys to 30, you can type **traittool -global -trait PolicyThrottlingP2PKeyRate -set 30.**

Configuring BlackBerry Policy Service throttling for application polling

The BlackBerry Policy Service performs application polling to verify when it must send applications to all BlackBerry devices that are associated with the BlackBerry Enterprise Server instance that the BlackBerry Policy Service runs on. You can configure BlackBerry Policy Service throttling on a BlackBerry Enterprise Server instance to limit the database usage of the BlackBerry Policy Service when it sends applications to devices.

If you do not configure throttling, the BlackBerry Policy Service tries to process tasks as fast as the server permits, which might result in an unexpected increase in CPU usage and database usage. If you configure throttling, the BlackBerry Policy Service sends applications to devices using the same method that it uses to throttle IT policies and service books.

Configure BlackBerry Policy Service throttling for application polling

1. Copy the BlackBerry Enterprise Server installation file to a computer that hosts the primary BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to <*extracted_folder*>\tools.
4. Perform one of the following actions:
   - To configure the BlackBerry Policy Service to send applications using the same method that it uses to throttle IT policies and service books, type **traittool -global -trait PolicyThrottlingAppPush -set true.**
   - To configure the BlackBerry Policy Service to not send applications using throttling, and to process the requests as quickly as possible, type **traittool -global -trait PolicyThrottlingAppPush -set false.**

   The default value is false.
5. Press ENTER.

Delete a BlackBerry Policy Service throttling setting

1. Copy the BlackBerry Enterprise Server installation files to a computer that hosts a BlackBerry Enterprise Server instance.
2. Extract the contents to a folder on the computer.
3. At the command prompt, navigate to the Tools folder where the TraitTool.exe file is located.
4. Type **traittool -global -trait** ***<trait_name>*** **-erase**, where <*trait_name*> is the configuration that you want to delete.
5. Press ENTER.

Example: Deleting a BlackBerry Policy Service throttling setting

If you want to delete the maximum number of IT policies and service books that all BlackBerry Policy Service instances can send to BlackBerry devices each minute, type **traittool -global -trait PolicyThrottlingMaxDomainJobs -erase.**

Change the port number that BlackBerry Enterprise Server components use to connect to the BlackBerry Configuration Database

You can change the static port number that BlackBerry Enterprise Server components use if you changed the port number that the BlackBerry Configuration Database uses after you install the BlackBerry Enterprise Server.

By default, the BlackBerry Configuration Database accepts TCP/IP connections to port 1433 on a Microsoft SQL Server. The BlackBerry Configuration Database accepts connections through ports 1024 to 65535.

1. On the computer that hosts the BlackBerry Enterprise Server component, open the BlackBerry Configuration Panel.
2. In the **Database Connectivity** tab, in the **Use dynamic ports or specify SQL port** field, type the port number.
3. Click **Apply.**
4. Click **OK.**
5. In the Windows Services, restart the appropriate service for the BlackBerry Enterprise Server component.
6. Repeat steps 1 to 5 on each computer that hosts a BlackBerry Enterprise Server component that connects to the BlackBerry Configuration Database.

Related information

Restarting BlackBerry Enterprise Server components, 392

BlackBerry Configuration Database connection types and port numbers, 452

Change the port number that the syslog tools use to monitor BlackBerry Enterprise Server events

You can change the port number that the syslog tools listen on to monitor BlackBerry Enterprise Server events. By default, the syslog tools listen to events for the BlackBerry Enterprise Server on port 514.

1. On the computer that hosts the BlackBerry Enterprise Server component, open the Windows Registry Editor.
2. Perform one of the following actions:
   - If you are running a 32-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\Research In Motion \BlackBerry Enterprise Server.
   - If you are running a 64-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\WOW6432Node \Research In Motion\BlackBerry Enterprise Server.
3. In the **Logging Info** registry key, click a BlackBerry Enterprise Server component.
4. If the DWORD value does not exist, create a DWORD value that you name **(Default)**.
5. Change the DWORD value to the port number that the syslog tools listen on.
6. Click **OK**.
7. In the Windows Services, restart the service for the BlackBerry Enterprise Server component.

Related information

Restarting BlackBerry Enterprise Server components, 392
Syslog connection type and port number, 469

BlackBerry Controller and BlackBerry Enterprise Server Component Monitoring

33

How the BlackBerry Controller monitors the BlackBerry Enterprise Server components

The BlackBerry Controller enables the BlackBerry Enterprise Server to continue running if nonresponsive threads occur or BlackBerry Enterprise Server services become inactive. The BlackBerry Controller monitors the BlackBerry Messaging Agent, the extension plug-ins for the BlackBerry Messaging Agent, and the BlackBerry Dispatcher so that the BlackBerry Controller can detect when to start, restart, or stop the services. The BlackBerry Controller can also restart other BlackBerry Enterprise Server services if they stop responding.

Services that require database access are installed in manual start mode and the BlackBerry Controller starts the services when the BlackBerry Dispatcher verifies the connection to the database. Other services are installed in automatic start mode, and by default, the BlackBerry Controller restarts the services if the BlackBerry Controller detects that the services are inactive. By default, the BlackBerry Controller also restarts services if the BlackBerry Controller detects nonresponsive threads or that a service is inactive for a long period of time.

Registry keys determine how the BlackBerry Controller monitors the BlackBerry Enterprise Server components and restarts the services that are associated with the components. You can change the default behavior of the BlackBerry Controller by creating new registry keys and changing the default values of the registry keys.

Change how the BlackBerry Controller restarts the BlackBerry Messaging Agent

Before you begin: To create a user.dmp file, or to use a user.dmp file as a data collection option, you must download and install the User Mode Process Dumper application that is included as a part of the Microsoft OEM Support Tools.

1. On the computer that hosts the BlackBerry Enterprise Server, open the Registry Editor.
2. In the left pane, perform one of the following actions:

- If you are running a 32-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\Research In Motion \BlackBerry Enterprise Server.
- If you are running a 64-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\ WOW6432Node \Research In Motion\BlackBerry Enterprise Server.

3. Click **Controller**.
4. Perform any of the following tasks:

Task	Steps
Change how the BlackBerry Controller restarts the BlackBerry Messaging Agent.	1. Create a DWORD value that is named **RestartAgentsOnCrash**. 2. Double-click the new DWORD value. 3. In the **Value data** field, perform one of the following actions: • To prevent the BlackBerry Controller from restarting the BlackBerry Messaging Agent if the BlackBerry Messaging Agent stops responding, type **0**. • To permit the BlackBerry Controller to restart the BlackBerry Messaging Agent if the BlackBerry Messaging Agent stops responding, type **1**.
Change the maximum number of times that the BlackBerry Messaging Agent restarts daily.	1. Create a DWORD value that is named **MaxAgentRestartPerDay**. 2. Double-click the new DWORD value. 3. In the **Value data** field, type a value. The default maximum number of restarts that can occur daily is ten.
Change the maximum number of missed health checks that can occur before the BlackBerry Messaging Agent restarts.	1. Create a DWORD value that is named **WaitToRestartAgentOnHung**. 2. Double-click the new DWORD value. 3. In the **Value data** field, type a value that is greater than four, which provides the BlackBerry Controller with sufficient time to monitor thread health checks before the BlackBerry Controller restarts the BlackBerry Messaging Agent. The default value is 6. Health checks occur every ten minutes. If a health check does not receive a response from the thread that that the BlackBerry Controller monitors, the BlackBerry Enterprise Server tracks the missed health check in the BlackBerry Messaging Agent log file as the wait count. Example: [20148] (05/12 12:21:00):{0xC28} Thread: *** No Response *** Thread Id=0xB00, Handle=0x558, WaitCount=2

Task	Steps
Prevent the BlackBerry Controller from restarting the BlackBerry Messaging Agent when a nonresponsive thread occurs.	1. Create a DWORD value that is named **WaitToRestartAgentOnHung**. 2. Double-click the new DWORD value. 3. In the **Value data** field, type **0**. The default value is 6.
Prevent the BlackBerry Controller from restarting the BlackBerry Messaging Agent for a specific time range if the BlackBerry Controller detects a nonresponsive thread.	1. Create a DWORD value that is named **RestartAgentOnHungBlackoutFrom**. 2. Double-click the new DWORD value. 3. In the **Base** section, select the **Decimal** option. 4. In the **Value data** field, type the lowest value of the time range. The values range from 0 to 23, where 0 is 12:00 AM and 23 is 11:00 PM. 5. Create a DWORD value that is named **RestartAgentOnHungBlackoutTo**. 6. Double-click the new DWORD value. 7. In the **Base** section, select the **Decimal** option. 8. In the **Value data** field, type the highest value of the time range. For example, if you configure the RestartAgentOnHungBlackoutFrom value to eight and the RestartAgentOnHungBlackoutTo value to 17, the BlackBerry Controller does not restart the BlackBerry Messaging Agent between 8:00 AM and 5:00 PM if it detects a nonresponsive thread. To turn off the time range, in the **RestartAgentOnHungBlackoutFrom** and **RestartAgentOnHungBlackoutTo** value fields, type **0**.
Change the maximum number of user.dmp files that each BlackBerry Enterprise Server creates daily before the BlackBerry Controller restarts the BlackBerry Messaging Agent.	1. Create a DWORD value that is named **MaxUserDumpPerDay**. 2. Double-click the new DWORD value. 3. In the **Value data** field, type a value. The default value is 3. To turn off the daily creation of user.dmp files, change the **MaxUserDumpPerDay** value field to **0**.
Change the number of ten-minute intervals that the BlackBerry Controller waits for a successful health check before it restarts the BlackBerry Messaging Agent.	1. Create a DWORD value that is named **MissedHeartbeatThreshold**. 2. Double-click the new DWORD value. 3. In the **Value data** field, type a value. The default value is 2. If you configure the MissedHeartbeatThreshold value to be three, the BlackBerry Controller waits for 30 minutes before it restarts the BlackBerry Messaging Agent.

Task	Steps
Prevent the BlackBerry Messaging Agent from restarting if the BlackBerry Controller does not receive health checks from it.	1. Create a DWORD value that is named **MissedHeartbeatThreshold**. 2. Double-click the new DWORD value. 3. In the **Value data** field, type **0**.

5. Click **OK**.

Change how the BlackBerry Controller restarts a BlackBerry Enterprise Server service

By default, the BlackBerry Controller restarts a BlackBerry Enterprise Server service if it stops responding.

1. On the computer that hosts the BlackBerry Enterprise Server component that you want to change, open the Registry Editor.
2. In the left pane, perform one of the following actions:
   - If you are running a 32-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\Research In Motion.
   - If you are running a 64-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\WOW6432Node \Research In Motion.
3. Perform any of the following tasks:

Task	Steps
Change how the BlackBerry Controller restarts the BlackBerry Attachment Service.	1. Click **BBAttachServer**. 2. Double-click the DWORD value that is named **RestartOnCrash**. 3. In the **Value data** field, perform one of the following actions: • To prevent the BlackBerry Controller from restarting the BlackBerry Attachment Service if the service stops responding, type **0**. • To permit the BlackBerry Controller to restart the BlackBerry Attachment Service if the service stops responding, type **1**.
Change how the BlackBerry Controller restarts the BlackBerry Collaboration Service.	1. Click **BlackBerry Collaboration Service**. 2. Double-click the DWORD value that is named **RestartOnCrash**. 3. In the **Value data** field, perform one of the following actions:

Task	Steps
	• To prevent the BlackBerry Controller from restarting the BlackBerry Collaboration Service if the service stops responding, type **0**. • To permit the BlackBerry Controller to restart the BlackBerry Collaboration Service if the service stops responding, type **1**.
Change how the BlackBerry Controller restarts the BlackBerry MDS Connection Service.	1. Click **BlackBerry Mobile Data Server**. 2. Double-click the DWORD value that is named **RestartOnCrash**. 3. In the **Value data** field, perform one of the following actions: • To prevent the BlackBerry Controller from restarting the BlackBerry MDS Connection Service if the service stops responding, type **0**. • To permit the BlackBerry Controller to restart the BlackBerry MDS Connection Service if the service stops responding, type **1**.
Change how the BlackBerry Controller restarts the BlackBerry Router.	1. Click **BlackBerryRouter**. 2. Double-click the DWORD value that is named **RestartOnCrash**. 3. In the **Value data** field, perform one of the following actions: • To prevent the BlackBerry Controller from restarting the BlackBerry Router if the service stops responding, type **0**. • To permit the BlackBerry Controller to restart the BlackBerry Router if the service stops responding, type **1**.
Change how the BlackBerry Controller restarts the BlackBerry Mail Store Service.	1. Navigate to BlackBerry Enterprise Server. 2. Click **MailStore**. 3. Double-click the DWORD value that is named **RestartOnCrash**. 4. In the **Value data** field, perform one of the following actions: • To prevent the BlackBerry Controller from restarting the BlackBerry Mail Store Service if the service stops responding, type **0**. • To permit the BlackBerry Controller to restart the BlackBerry Mail Store Service if the service stops responding, type **1**.
Change how the BlackBerry Controller restarts the BlackBerry Policy Service.	1. Navigate to BlackBerry Enterprise Server. 2. Click **PolicyServer**. 3. Double-click the DWORD value that is named **RestartOnCrash**. 4. In the **Value data** field, perform one of the following actions:

Task	Steps
	- To prevent the BlackBerry Controller from restarting the BlackBerry Policy Service if the service stops responding, type **0**. - To permit the BlackBerry Controller to restart the BlackBerry Policy Service if the service stops responding, type **1**.
Change how the BlackBerry Controller restarts the BlackBerry Synchronization Service.	1. Navigate to BlackBerry Enterprise Server. 2. Click **SyncServer**. 3. Double-click the DWORD value that is named **RestartOnCrash**. 4. In the **Value data** field, perform one of the following actions: - To prevent the BlackBerry Controller from restarting the BlackBerry Synchronization Service if the service stops responding, type **0**. - To permit the BlackBerry Controller to restart the BlackBerry Synchronization Service if the service stops responding, type **1**.

4. Click **OK**.

BlackBerry Enterprise Server Alert Tool

Configuring notifications using the BlackBerry Enterprise Server Alert Tool

You can use the BlackBerry Enterprise Server Alert Tool to monitor the Windows Event Log and send users that you define as notification recipients a notification message when the tool records a critical, error, warning, or informational event. You must configure notification settings for each BlackBerry Enterprise Server in your organization's BlackBerry Domain.

Change the default event monitoring level

By default, the BlackBerry Enterprise Server Alert Tool monitors critical events only.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Alert**.
2. Click the instance that you want to change.

3. Click **Edit instance**.
4. In the **SMTP host name** field, type the SMTP host name of your organization's gateway in DNS format (for example, smtp.CompanyName.com).
5. In the **SMTP account name** field, type the name of the SMTP account that you want to send notifications from.
6. In the **SMTP from address** field, type the SMTP address that you want to send notifications and receive replies to notifications.
7. In the **Event level** drop-down list, click one of the following menu items:
    - To monitor level 0 events (critical), click **Critical**.
    - To monitor all events up to and including level 1 (critical and error), click **Error**.
    - To monitor all events up to and including level 2 (critical, error, and warning), click **Warning**.
    - To monitor all events up to and including level 3 (critical, error, warning, and informational), click **Informational**.
8. Click **OK**.

Related information

Restarting BlackBerry Enterprise Server components, 392

Define a notification recipient

You can specify a notification recipient for the BlackBerry Enterprise Server Alert Tool so that the contact receives notification messages in email or popup messages that appear on the screen. You can send popup messages to the contact if the Messenger service for Windows is running on the computer that you installed the BlackBerry Enterprise Server Alert Tool on, and if the computer is not running Windows Server 2008. The contact receives popup messages only if the Messenger service is running on the contact's computer.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Alert**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. In the **User name** field, type the name of the contact.
5. In the **Event level** drop-down list, click one of the following menu items:
    - To send notification messages for the default event monitoring level, click **Default**.
    - To send notification messages for all events up to and including level 1 (critical and error), click **Error**.
    - To send notification messages for all events up to and including level 2 (critical, error, and warning), click **Warning**.
    - To send notification messages for all events up to and including level 3 (critical, error, warning, and informational), click **Info**.

6. In the **Email address** field, type the recipient's email address.
7. To send notification messages as popup messages on the contact's computer, in the **Console** field, type the name of the contact's computer.
8. Click **OK**.

Related information

Restarting BlackBerry Enterprise Server components, 392

BlackBerry Enterprise Server log files

34

Monitoring PIN messages, SMS text messages, and calls

Change the default location for the log files for PIN messages, SMS text messages, and calls

Note: The log files for PIN messages, SMS text messages, and calls store confidential information in plain-text format. To protect the information, you must restrict access to the location of the log files.

By default, the log files are stored in C:\Program Files\Research In Motion\BlackBerry Enterprise Server\Logs. This is the same location that the BlackBerry Enterprise Server component log files are stored in.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Synchronization**.
2. Click the instance that you want to change.
3. Click **Edit instance**.
4. In the **General** section, in the **Audit root directory** field, type the path to the location where you want to save the log files.
5. Click **Save all**.

Monitor PIN messages

You can use the log files for PIN messages to monitor the time and frequency when users send PIN messages from BlackBerry devices. The log files are named using the format PINLog_<*yyyymmdd*>. By default, logging for PIN messages is turned off.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.

2. Click **Manage IT policies**.
3. In the list of IT policies, click an IT policy.
4. Click **Edit IT policy**.
5. On the **PIM Synchronization** tab, in the **Disable PIN Messages Wireless Synchronization** drop-down list, click **No**.
6. Click **Save all**.

Monitor SMS text messages

You can use the log files for SMS text messages to monitor the time and the frequency when users send SMS text messages from BlackBerry devices. The log files are named using the format SMSLog_*yyyymmdd*. By default, logging for SMS text messages is turned off.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. In the list of IT policies, click an IT policy.
4. Click **Edit IT policy**.
5. On the **PIM Synchronization** tab, in the **Disable SMS Messages Wireless Synchronization** drop-down list, click **No**.
6. Click **Save all**.

Turn off call logging

You can use the log files for calls to monitor the time and frequency when users make calls from BlackBerry devices. The log files are named using the format PhoneCallLog_<*yyyymmdd*>. By default, logging for calls is turned on.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. In the list of IT policies, click the appropriate IT policy.
4. Click **Edit IT policy**.
5. On the **PIM Synchronization** tab, in the **Disable Phone Call Log Wireless Synchronization** drop-down list, click **Yes**.
6. Click **Save all**.

Log files for BlackBerry Enterprise Server components

You can use log files to record the activity of BlackBerry Enterprise Server components and troubleshoot issues with the components. The BlackBerry Enterprise Server creates a log file for each BlackBerry Enterprise Server component and saves the log files on the computer that hosts the BlackBerry Enterprise Server. By default, the BlackBerry Enterprise Server saves the log files in C:\Program Files\Research In Motion\BlackBerry Enterprise Server\Logs . Each BlackBerry Enterprise Server instance saves the log files in folders that it creates daily and organizes by date. To prevent the BlackBerry Enterprise Server log files from taking up too much disk space, you can change how BlackBerry Enterprise Server components create and delete log files.

By default, the BlackBerry Enterprise Server names log files <*server_name*>_<*component_identifier*>_<*instance*>_<*yyyymmdd*>_<*log_number*>.txt (for example, BBServer01_MAGT_01_20070120_0001.txt). An event that the BlackBerry Enterprise Server writes to a log file begins with a five-digit number, where the first digit represents the logging level. For example, the following log file entry logs level 3, which are informational level events: [30000] (03/12 14:03:42.315):{0x18CC} [ENV] Computer Host Name: *host_name*.

Changing the location where BlackBerry Enterprise Server components save log files

Change the location where BlackBerry Enterprise Server components save log files

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Logging**.
2. Click the instance that contains the logging settings that you want to change.
3. Click **Edit instance**.
4. In the **General** section, in the **Log file path** field, type the path where you want to save the log files.
5. Click **Save all**.
6. On each computer that hosts a BlackBerry Enterprise Server component or BlackBerry Enterprise Server service, in the Windows Services, restart the BlackBerry Enterprise Server services.

Related information

Restarting BlackBerry Enterprise Server components, 392

Store the log files for BlackBerry Enterprise Server components in one folder

You can store the log files for BlackBerry Enterprise Server components in one folder instead of permitting the BlackBerry Enterprise Server to save the log files in folders that it creates daily and organizes by date.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Logging**.
2. Click the instance that contains the logging settings that you want to change.
3. Click **Edit instance**.
4. In the **General** section, in the **Create folder for daily logs** drop-down list, click **False**.
5. Click **Save all**.
6. On each computer that hosts a BlackBerry Enterprise Server component or BlackBerry Enterprise Server service, in the Windows Services, restart the BlackBerry Enterprise Server services.

Changing how BlackBerry Enterprise Server components create log files

Add a prefix to the file names of the log files for BlackBerry Enterprise Server components

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Logging**.
2. Click the instance that contains the logging settings that you want to change.
3. Click **Edit instance**.
4. In the **General** section, in the **Log file prefix** field, type the prefix that you want to add to the log files.
5. Click **Save all**.
6. On each computer that hosts a BlackBerry Enterprise Server component or BlackBerry Enterprise Server service, in the Windows Services, restart the BlackBerry Enterprise Server services.

Related information

Restarting BlackBerry Enterprise Server components, 392

Change the maximum size of the log file for a BlackBerry Enterprise Server component

When the log file for a BlackBerry Enterprise Server component reaches its maximum size, the BlackBerry Enterprise Server either creates an additional log file for the component or overwrites the current one, depending on whether you turn on log auto-roll.

By default, log auto-roll is turned on for all BlackBerry Enterprise Server components, which means that the BlackBerry Enterprise Server creates an additional log file when the current log file reaches its maximum size.

You can specify a different maximum size for each log file.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Logging**.
2. Click the instance that contains the logging settings that you want to change.
3. On the **Logging details** tab, click **Edit instance**.
4. In each section, in the **Maximum size of daily log files (MB)** field, type the file size.
5. Click **Save all**.
6. On the **Servers and components** menu, locate and restart the components that contain the logging settings that you changed.

Related information

Create an additional log file for a BlackBerry Enterprise Server component when the current log file reaches its maximum size, 436
Restarting BlackBerry Enterprise Server components, 392

Change the logging level for a BlackBerry Enterprise Server component

You can select whether the information that you save to the log files is detailed or limited by changing the logging level for a BlackBerry Enterprise Server component. A more detailed logging level can help you troubleshoot issues with a BlackBerry Enterprise Server component.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Logging**.
2. Click the instance that contains the logging settings that you want to change.
3. On the **Logging details** tab, click **Edit instance**.
4. In each section, in the **Log level** drop-down list, click one of the following menu items:
   - To write error messages to the log files, click **Error**.
   - To write warning messages to the log files, click **Warning**.
   - To write daily activities to the log files, click **Informational**.

- To write additional information to the log files that can help you troubleshoot issues with your organization's environment, click **Debug**.

5. Click **Save all**.
6. On the **Servers and components** menu, locate and restart the components that contain the logging settings that you changed.

Related information

Restarting BlackBerry Enterprise Server components, 392

Create an additional log file for a BlackBerry Enterprise Server component when the current log file reaches its maximum size

If you turn on log auto-roll for a BlackBerry Enterprise Server component, the BlackBerry Enterprise Server creates a new log file for the component when the current log file reaches the maximum size. If you turn off log auto-roll for a BlackBerry Enterprise Server component, the BlackBerry Enterprise Server overwrites the current log file for the component when the log file reaches the maximum size. By default, log auto-roll is turned on for all BlackBerry Enterprise Server components.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Logging**.
2. Click the instance that contains the logging settings that you want to change.
3. On the **Logging details** tab, click **Edit instance**.
4. In each section, in the **Log auto-roll** drop-down list, click **True**.
5. Click **Save all**.
6. On the **Servers and components** menu, locate and restart the components that contain the logging settings that you changed.

Related information

Restarting BlackBerry Enterprise Server components, 392

Change the identifier of the log file for a BlackBerry Enterprise Server component

You can identify the log file for a BlackBerry Enterprise Server component by the identifier that is included in the file name. For example, a log file that is named BBServer01_SYNC_01_20080120_001.txt uses the default component identifier SYNC to identify the BlackBerry Synchronization Service component.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Logging**.
2. Click the instance that contains the logging settings that you want to change.
3. On the **Logging details** tab, click **Edit instance**.
4. In each section, in the **Log identifier** field, type a new identifier name.

5. Click **Save all**.
6. On the **Servers and components** menu, locate and restart the components that contain the logging settings that you changed.

Related information

Restarting BlackBerry Enterprise Server components, 392

Prevent a BlackBerry Enterprise Server component from creating a daily log file

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Logging**.
2. Click the instance that contains the logging settings that you want to change.
3. On the **Logging details** tab, click **Edit instance**.
4. In each section, in the **Daily file creation** drop-down list, click **False**.
5. Click **Save all**.
6. On the **Servers and components** menu, locate and restart the components that contain the logging settings that you changed.

Related information

Restarting BlackBerry Enterprise Server components, 392

Configure when the BlackBerry Enterprise Server deletes a log file

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Logging**.
2. Click the instance that contains the logging settings that you want to change.
3. On the **Logging details** tab, click **Edit instance**.
4. In each section, in the **Maximum age of daily log files** field, type the number of days that you want the BlackBerry Enterprise Server to delete the log files after.
5. Click **Save all**.
6. On the **Servers and components** menu, locate and restart the components that contain the logging settings that you changed.

Related information

Restarting BlackBerry Enterprise Server components, 392

Change the character encoding of the log file for a BlackBerry Enterprise Server component

You can change the character encoding of the log files of a BlackBerry Enterprise Server component so that the encoding supports the tools that you use to parse and examine the log files. You can specify a different character encoding for each BlackBerry Enterprise Server component. You can use the ANSI, UTF-8, and UTF-16LE character encoding methods.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Logging**.
2. Click the instance that contains the logging settings that you want to change.
3. On the **Logging details** tab, click **Edit instance**.
4. In each section, in the **Log encoding** drop-down list, click one of the following character encodings:
   - **ANSI**
   - **UTF-8**
   - **UTF-16LE**
5. Click **Save all**.
6. On the **Servers and components** menu, locate and restart the components that contain the logging settings that you changed.

Related information

Restarting BlackBerry Enterprise Server components, 392

Restore logging settings to default values for all components

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Logging**.
2. Click the instance that you want to restore to default values.
3. On the **Logging details** tab, click **Edit instance**.
4. Click **Reset logging defaults**.
5. Click **Save all**.
6. For the changes to take effect, perform any of the following actions to restart the BlackBerry Enterprise Server services:
   - To restart services other than the BlackBerry Administration Service, on the **Servers and components** menu, locate and restart the services that you restored to default values.
   - To restart the BlackBerry Administration Service, on the computer that hosts the BlackBerry Administration Service, in the Windows Services, restart the **BlackBerry Administration Service - Native Code Container** service.

Related information

Restarting BlackBerry Enterprise Server components, 392

Component identifiers for log files

You can identify the names for the BlackBerry Enterprise Server log files using the following component identifiers:

Component identifier	Logging component
ACNV	BlackBerry Attachment Service attachment conversion
ALRT	BlackBerry Enterprise Server Alert Tool
APP	BlackBerry Monitoring Service Application Core
ASCL	BlackBerry Attachment Service client
ASMN	BlackBerry Attachment Service attachment monitor
ASRV	BlackBerry Attachment Service component
BBAS-AS	BlackBerry Administration Service – Application Server
BBAS-NCC	BlackBerry Administration Service – Native Code Container
BBIM	BlackBerry Instant Messaging
BBMS	BlackBerry Monitoring Service console
BBMS-APP	BlackBerry Monitoring Service Application Core
BBMS-DCS	BlackBerry Monitoring Service Data Collection Subsystem
BBMS-ENG	BlackBerry Monitoring Service Polling Engine
CBCK	backup connector
CEXC	Microsoft Exchange connector
CMNG	management connector
ConfigTool	BlackBerry Enterprise Server configuration tool
CONN	BlackBerry Synchronization Connector
CTRL	BlackBerry Controller
DBNS	BlackBerry database notification service

Component identifier	Logging component
DCS	BlackBerry Monitoring Service Data Collection Subsystem
DISP	BlackBerry Dispatcher
EXTS	extension connector
HHCG	BlackBerry Configuration Panel
MAGT	BlackBerry Messaging Agent
MAST	BlackBerry Mail Store Service
MDAT	BlackBerry MDS Connection Service
POLC	BlackBerry Policy Service
ROUT	BlackBerry Router
SYNC	BlackBerry Synchronization Service
TAT	BlackBerry Threshold Analysis Tool

BlackBerry MDS Connection Service log files

Changing how the BlackBerry MDS Connection Service creates a log file

Change the logging level for BlackBerry MDS Connection Service log files

You can change the logging level for the BlackBerry MDS Connection Service log file, which includes the event log, UDP log files, and TCP log files.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click an instance of the BlackBerry MDS Connection Service.
3. On the **Logging** tab, click **Edit instance**.

4. In the **File logging destination**, **UDP logging destination**, **TCP logging destination**, or **EventLog logging destination** sections, select one of the following logging levels from the **Log level** drop-down list:

   - To write events to the log files, click **Event**.
   - To write error messages to the log files, click **Error**.
   - To write warning messages to the log files, click **Warning**.
   - To write daily activities to the log files, click **Informational**.
   - To write additional information to the log files that can help you troubleshoot issues with the BlackBerry MDS Connection Service, click **Debug**.

5. Click **Save all**.

Related information

Restarting BlackBerry Enterprise Server components, 392

Change the interval that the BlackBerry MDS Connection Service writes information to a log file

The interval that the BlackBerry MDS Connection Service writes information to a log file applies to all BlackBerry MDS Connection Service log files, including the event log, UDP log files, and TCP log files.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click an instance of the BlackBerry MDS Connection Service.
3. On the **Logging** tab, click **Edit instance**.
4. In the **File logging destination** section, in the **Log timer interval** field, type the interval in milliseconds.

   The default value is 30000.

5. Click **Save all**.

Related information

Restarting BlackBerry Enterprise Server components, 392

Change the host and port number that the BlackBerry MDS Connection Service connects to when it sends UDP log file messages

The SNMP agent for the BlackBerry Enterprise Server receives UDP log file messages from the same host and port number that the BlackBerry MDS Connection Service connects to when it sends UDP log messages.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click an instance of the BlackBerry MDS Connection Service.

3. On the **Logging** tab, click **Edit instance**.
4. In the **UDP logging destination** section, in the **Location** field, type the host name and port number using the format <*host_name*>:<*port_number*>.
5. Click **Save all**.

Related information
Restarting BlackBerry Enterprise Server components, 392

Change the host and port number that the BlackBerry MDS Connection Service connects to when it sends TCP log file messages

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click an instance of the BlackBerry MDS Connection Service.
3. On the **Logging** tab, click **Edit instance**.
4. In the **TCP logging destination** section, in the **Location** field, type the host name and port number using the format <*host_name*>:<*port_number*>.
5. Click **Save all**.

Related information
Restarting BlackBerry Enterprise Server components, 392

Configure BlackBerry MDS Connection Service to log DSML information

1. On the computer that hosts the BlackBerry MDS Connection Service, navigate to <*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\MDS\Servers\instance\config .
2. In any text editor, open the rimpublic.properties file.
3. In the rimpublic.properties file, type **application.handler.dsml.logging**=**Yes**.
4. Save and close the rimpublic.properties file.
5. In the Windows Services, restart the BlackBerry MDS Connection Service service.

Related information
Restarting BlackBerry Enterprise Server components, 392

Change the activities that the BlackBerry MDS Connection Service writes to a log file

The settings for the activities that the BlackBerry MDS Connection Service writes to a log file apply to all log files, including the event log, UDP log files, and TCP log files.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **MDS Connection Service**.
2. Click a BlackBerry MDS Connection Service instance.
3. On the **Logging** tab, click **Edit instance**.
4. In the **Logging** section, perform any of the following tasks:

Task	Steps
Do not trace how data packets travel inside the SRP network layer from the BlackBerry MDS Connection Service to the BlackBerry Dispatcher.	In the **SRP logging turned on** drop-down list, click **No**.
Do not trace how data packets travel inside the IPPP network layer from the BlackBerry MDS Connection Service to the BlackBerry Dispatcher.	In the **IPPP logging turned on** drop-down list, click **No**.
Send logging information using UDP to a UDP server.	In the **UDP logging turned on** drop-down list, click **Yes**.
Trace how data packets travel inside the gateway message envelope network layer from the BlackBerry MDS Connection Service to the BlackBerry Dispatcher.	In the **GME logging turned on** drop-down list, click **Yes**.
Monitor HTTP headers for request and response messages that the web server sends or receives when users retrieve content from the Internet and intranet on BlackBerry devices.	In the **HTTP logging turned on** drop-down list, click **Yes**.
Monitor HTTP headers and the body of response messages that the web server sends when users retrieve content from the Internet and intranet on BlackBerry devices.	In the **Verbose HTTP logging turned on** drop-down list, click **Yes**.
Monitor activity that occurs between the BlackBerry MDS Connection Service and the target server when the BlackBerry MDS Connection Service uses a TLS connection.	In the **TLS logging turned on** drop-down list, click **Yes**.
Monitor the certificate revocation status that the BlackBerry device retrieves from the OCSP server.	In the **OCSP logging turned on** drop-down list, click **Yes**.
Monitor BlackBerry device requests to access a user profile or certificate from the LDAP directory.	In the **LDAP logging turned on** drop-down list, click **Yes**.
Monitor CRLs that the BlackBerry device retrieves from the CRL server.	In the **CRL logging turned on** drop-down list, click **Yes**.
Monitor PGP key status and revocation information that the BlackBerry device retrieves from the PGP server.	In the **PGP logging turned on** drop-down list, click **Yes**.

5. Click **Save all**.

Related information

Restarting BlackBerry Enterprise Server components, 392

Using BlackBerry MDS Connection Service log files to view information for proxied connections to BlackBerry devices

The BlackBerry Enterprise Server writes data for each BlackBerry device connection that the BlackBerry MDS Connection Service proxies in the BlackBerry MDS Connection Service log files.

You can find the BlackBerry MDS Connection Service log files on the computer that hosts the BlackBerry Enterprise Server. You can identify BlackBerry MDS Connection Service log files by the component identifier MDAT in the log file name.

Log file example: BlackBerry device user initiates the proxied connection

```
<LAYER = IPPP, DEVICEPIN = u29, DOMAINNAME = test.rim.net, CONNECTION_TYPE =
DEVICE_CONN, CONNECTIONID = 852164874, DURATION(ms) = 3500, MFH_KBytes = 0.908,
MTH_KBytes = 38.218, MFH_PACKET_COUNT = 1, MTH_PACKET_COUNT = 2>
```

Log file example: BlackBerry Enterprise Server initiates the proxied connection (push)

```
<LAYER = IPPP, DEVICEPIN = <devicepin>, DOMAINNAME = kmtestd, CONNECTION_TYPE =
PUSH_CONN, CONNECTIONID = -432667474, DURATION(ms) = 600090, MFH_KBytes = 0,
MTH_KBytes = 10.477, MFH_PACKET_COUNT = 0, MTH_PACKET_COUNT = 4>
```

Information in BlackBerry MDS Connection Service log files for proxied connections to BlackBerry devices

Attribute	Description
LAYER	protocol layer that the BlackBerry MDS Connection Service uses to proxy BlackBerry device connections
DEVICEPIN	PIN or BlackBerry Enterprise Server user ID of the BlackBerry device that connects using a proxy server
DOMAINNAME	domain that requests the BlackBerry device connection

Attribute	Description
CONNECTION_TYPE	initiator of the proxied connection, which can be either the BlackBerry device user (DEVICE_CONN) or BlackBerry Enterprise Server (PUSH_CONN)
CONNECTIONID	unique identifier for an IPPP connection, where - (minus sign) indicates a push connection
DURATION(ms)	duration of the proxied BlackBerry device connection, in milliseconds
MFH_KBytes	size of messages that the BlackBerry device sends, in KB
MTH_KBytes	size of messages that the BlackBerry device receives, in KB
MFH_PACKET_COUNT	number of packets that the BlackBerry device sends
MTH_PACKET_COUNT	number of packets that the BlackBerry device receives

BlackBerry Collaboration Service log files

Change which activities the BlackBerry Collaboration Service writes to a log file

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view** > **Collaboration**.
2. Expand a BlackBerry Collaboration Service, then click an instance.
3. On the **Instance information** tab, click **Edit instance**.
4. In the **Logging settings** section, perform any of the following tasks:

Task	Steps
Do not monitor activity at the BlackBerry instant messaging network layer.	In the **BBIM logging turned on** drop-down list, click **False**.
Do not trace how data packets travel inside the SRP network layer from the BlackBerry Collaboration Service to the BlackBerry Dispatcher.	In the **SRP logging turned on** drop-down list, click **False**.

Task	Steps
Trace how data packets travel inside the GME network layer from the BlackBerry Collaboration Service to the BlackBerry Dispatcher.	In the **GME logging turned on** drop-down list, click **True**.

5. Click **Save all**.

Related information

Restarting BlackBerry Enterprise Server components, 392

BlackBerry Enterprise Solution connection types and port numbers

35

The BlackBerry Enterprise Server components authenticate the port connections over a TCP/IP or UDP/IP connection that uses SSL or TLS.

BlackBerry Administration Service connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
for a Microsoft SQL Server, incoming data connections from, and outgoing data connections to, the BlackBerry Configuration Database	TCP	1433	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Database\Port • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node

Item	Connection type	Default port number	UI where you can configure the connection
			\Research In Motion \BlackBerry Enterprise Server \Database\Port
incoming data connections from, and outgoing data connections to, browsers	HTTPS	443	BlackBerry Configuration Panel
incoming data connections from, and outgoing data connections to, BlackBerry Enterprise Server components	HTTP	18180	BlackBerry Configuration Panel
incoming data connections from, and outgoing data connections to, BlackBerry Enterprise Server components for HA JNDI	TCP	11100	BlackBerry Configuration Panel
incoming data connections from, and outgoing data connections to, a BlackBerry Administration Service instance for local JNDI	TCP	11099	BlackBerry Configuration Panel
internal data connection	TCP	18083	BlackBerry Configuration Panel
incoming data connections from, and outgoing data connections to, BlackBerry Enterprise Server components for Java RMI	TCP	13873	BlackBerry Configuration Panel
incoming data connections from, and outgoing data connections to, BlackBerry Enterprise Server components for Java RMI over SSL	TLS	13843	BlackBerry Configuration Panel
internal data connection	TCP	14457	BlackBerry Configuration Panel
internal data connection	TCP	28083	BlackBerry Configuration Panel
internal data connection	TLS	23843	BlackBerry Configuration Panel
internal data connection	TCP	21099	BlackBerry Configuration Panel

Item	Connection type	Default port number	UI where you can configure the connection
data connections between BlackBerry Administration Service instances	UDP	multicast IP address/port 228.1.2.1/48858 228.1.2.1/48857 228.1.2.1/48855 228.1.2.5/45588	—
data connections between BlackBerry Administration Service instances using TCP ping	TCP	first unused port number from 17200 to 17209; 17400 to 17409; 17600 to 17609 and 17800 to 17809	BlackBerry Administration Service

BlackBerry Attachment Service connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
incoming document submissions from the BlackBerry Attachment Service	TCP	1900	BlackBerry Administration Service
outgoing conversion results to the BlackBerry Attachment Connector	TCP	1900	BlackBerry Administration Service
incoming connections and outgoing connections for BlackBerry Administration Service configuration	TCP	1999	BlackBerry Administration Service
incoming document queries from the BlackBerry Attachment Service	TCP	2000	BlackBerry Administration Service

Item	Connection type	Default port number	UI where you can configure the connection
outgoing conversion results of large attachments to the BlackBerry Attachment Connector for the BlackBerry Attachment Service	TCP	2000	BlackBerry Administration Service
incoming data connections from, and outgoing data connections to, the BlackBerry Configuration Database that a Microsoft SQL Server database hosts	TCP	1433 (static connections only)	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Database\Port • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Research In Motion\BlackBerry Enterprise Server\Database\Port

BlackBerry Collaboration Service connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
incoming data connections from, and outgoing data connections to, the Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007	HTTPS	443	BlackBerry Administration Service

Item	Connection type	Default port number	UI where you can configure the connection
incoming data connections from, and outgoing data connections to, the Microsoft Office Communications Server 2007 R2 or 2010	TLS or MTLS	5061	BlackBerry Administration Service
incoming data connections from, and outgoing data connections to, IBM Lotus Sametime	TCP/IP	1516	BlackBerry Administration Service
incoming data connections from, and outgoing data connections to, the Novell GroupWise Messenger	SSL	8300	BlackBerry Administration Service
incoming data connections from, and outgoing data connections to, the BlackBerry Dispatcher	TCP	3200	—
incoming data connections from, and outgoing data connections to, the BlackBerry Configuration Database that a Microsoft SQL Server hosts	TCP	1433 (for static port)	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Database\Port • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Research In Motion\BlackBerry Enterprise Server\Database\Port
outgoing syslog connections to the SNMP agent	UDP	4071	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerrySNMPAgent\Parameters\UDPPort

Item	Connection type	Default port number	UI where you can configure the connection
			• On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Research In Motion\BlackBerrySNMPAgent\Parameters\UDPPort

BlackBerry Configuration Database connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
for a Microsoft SQL Server, incoming data connections from, and outgoing data connections to, any of the following BlackBerry Enterprise Server components: • BlackBerry Administration Service • BlackBerry Attachment Service • BlackBerry Collaboration Service • BlackBerry Dispatcher • BlackBerry MDS Connection Service • BlackBerry Messaging Agent • BlackBerry Policy Service • BlackBerry Synchronization Service	TCP	1433 (for static port)	BlackBerry Configuration Panel Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Database\Port • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Research In Motion

Item	Connection type	Default port number	UI where you can configure the connection
			\BlackBerry Enterprise Server\Database\Port

Related information

Restarting BlackBerry Enterprise Server components, 392

BlackBerry Controller connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
incoming syslog connections from the BlackBerry Messaging Agent	UDP	4070	Microsoft Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Logging Info\Mailbox Agent\SysLogHost • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Research In Motion\BlackBerry Enterprise Server\Logging Info\Mailbox Agent\SysLogHost

Item	Connection type	Default port number	UI where you can configure the connection
outgoing syslog connections to the BlackBerry Messaging Agent	UDP	port number that the BlackBerry Messaging Agent provides	—

BlackBerry Dispatcher connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
incoming data connections from the BlackBerry Messaging Agent	TCP	5096	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Agents\TcpPortDispatcher • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Research In Motion\BlackBerry Enterprise Server\Agents\TcpPortDispatcher
incoming data connections from, and outgoing data connections to, one or more of the following BlackBerry Enterprise Server components:	TCP	3200	—

Item	Connection type	Default port number	UI where you can configure the connection
• BlackBerry Collaboration Service • BlackBerry MDS Connection Service • BlackBerry Policy Service • BlackBerry Synchronization Service			
outgoing data connection that uses SRP to the BlackBerry Router	TCP	3101	BlackBerry Administration Service
incoming data connections from, and outgoing data connections to, the BlackBerry Configuration Database that a Microsoft SQL Server hosts	TCP	1433	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Database\Port • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Research In Motion\BlackBerry Enterprise Server\Database\Port
incoming data connection from the BlackBerry database notification system	UDP	first unused port number from 4185 to 4499	—
outgoing syslog connection to the SNMP agent	UDP	4071	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion

Item	Connection type	Default port number	UI where you can configure the connection
			\BlackBerrySNMPAgent \Parameters\UDPPort • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE \WOW6432Node \Research In Motion \BlackBerrySNMPAgent \Parameters\UDPPort

BlackBerry Messaging Agent connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
outgoing data connections to the BlackBerry Dispatcher	TCP	5096	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Agents \TcpPortDispatcher • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE \WOW6432Node \Research In Motion \BlackBerry Enterprise

Item	Connection type	Default port number	UI where you can configure the connection
			Server\Agents \TcpPortDispatcher
incoming data connections from, and outgoing data connections to, the BlackBerry Configuration Database that a Microsoft SQL Server hosts	TCP	1433	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server \Database\Port • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE \WOW6432Node \Research In Motion \BlackBerry Enterprise Server\Database\Port
incoming syslog connections from the BlackBerry Controller and CalHelper	UDP	first unused port number from 4085 to 4499	—
outgoing syslog connections to the BlackBerry Controller	UDP	4070	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Agents \SysLogHost • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE

Item	Connection type	Default port number	UI where you can configure the connection
			\WOW6432Node \Research In Motion \BlackBerry Enterprise Server\Agents \SysLogHost
outgoing syslog connections to the SNMP agent	UDP	4071	Windows registry - On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Agents \UDPPort - On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE \WOW6432Node \Research In Motion \BlackBerry Enterprise Server\Agents\UDPPort
incoming data connections from the BlackBerry database notification system	UDP	first unused port number from 4185 to 4499	—

BlackBerry MDS Connection Service connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
if access control for push applications is turned on, incoming connections for the HTTP listener port	HTTP	8080	BlackBerry Administration Service
if access control for push applications is turned on, incoming connections for the HTTP listener port	HTTPS	8443	BlackBerry Administration Service
incoming data connections from, and outgoing data connections to, the BlackBerry Dispatcher	TCP	3200	—
incoming data connections from, and outgoing data connections to, the BlackBerry Configuration Database that a Microsoft SQL Server hosts	TCP	1433	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Database\Port • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Research In Motion\BlackBerry Enterprise Server\Database\Port
outgoing syslog connections to the SNMP agent	UDP	4071	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHIN

Item	Connection type	Default port number	UI where you can configure the connection
			E\SOFTWARE\Research In Motion \BlackBerrySNMPAgent \Parameters\UDPPort • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE \WOW6432Node \Research In Motion \BlackBerrySNMPAgent \Parameters\UDPPort
incoming data connections for reliable pushes	TCP	7874	BlackBerry Administration Service

BlackBerry Monitoring Service connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
for a Microsoft SQL Server, incoming data connections from, and outgoing data connections to, the BlackBerry Configuration Database and BlackBerry Monitoring Service database	TCP	1433	BlackBerry Configuration Panel
incoming data connections from, and outgoing data connections to, browsers	HTTP	58180	—
incoming data connections from, and outgoing data connections to, browsers	HTTPS	8443	—
incoming data connections from, and outgoing data connections to, the BlackBerry Enterprise Server and any	SNMP	161 and 162	BlackBerry Monitoring Service console

Item	Connection type	Default port number	UI where you can configure the connection
other applications that you configured the BlackBerry Monitoring Service to send SNMP traps to			
internal data connection to the BlackBerry Monitoring Service Application Core	TCP	55500	BlackBerry Configuration Panel
internal data connection to the BlackBerry Monitoring Service Polling Engine	TCP	55501	BlackBerry Configuration Panel
internal data connection to the BlackBerry Monitoring Service Data Collection Subsystem	TCP	55502	BlackBerry Configuration Panel
internal data connection to the BlackBerry Monitoring Service console	TCP	55503	BlackBerry Configuration Panel

BlackBerry Policy Service connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
incoming data connections from, and outgoing data connections to, the BlackBerry Dispatcher	TCP	3200	—
incoming data connections from, and outgoing data connections to, the BlackBerry Configuration Database that a Microsoft SQL Server hosts	TCP	1433 (for the static port)	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Database\Port • On a 64-bit version of Windows: HKEY_LOCAL_MACHIN

Item	Connection type	Default port number	UI where you can configure the connection
			E\SOFTWARE \WOW6432Node \Research In Motion \BlackBerry Enterprise Server\Database\Port
incoming data connections from the BlackBerry database notification system	UDP	first unused port number from 4185 to 4499	—

BlackBerry Router connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
incoming data connections from the BlackBerry Dispatcher that use SRP	TCP	3101	BlackBerry Configuration Panel Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion \BlackBerryRouter \ServicePort • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE \WOW6432Node

Item	Connection type	Default port number	UI where you can configure the connection
			\Research In Motion \BlackBerryRouter \ServicePort
outgoing data connections to the BlackBerry Infrastructure that use SRP	TCP	3101	BlackBerry Configuration Panel Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion \BlackBerryRouter \TcpPort • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE \WOW6432Node \Research In Motion \BlackBerryRouter \TcpPort
incoming data connections from, and outgoing data connections to, BlackBerry devices that use the BlackBerry Device Manager to bypass the wireless network and devices that connect using Wi-Fi	TCP	4101	BlackBerry Device Manager Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion \BlackBerryRouter \DevicePort • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE

Item	Connection type	Default port number	UI where you can configure the connection
			\WOW6432Node \Research In Motion \BlackBerryRouter \DevicePort
outgoing syslog connections to the SNMP agent	UDP	4071	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion \BlackBerrySNMPAgent \Parameters\UDPPort • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE \WOW6432Node \Research In Motion \BlackBerrySNMPAgent \Parameters\UDPPort

BlackBerry Synchronization Service connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
incoming data connections from, and outgoing data connections to, the BlackBerry Dispatcher	TCP	3200	—

Item	Connection type	Default port number	UI where you can configure the connection
incoming data connections from, and outgoing data connections to, the BlackBerry Configuration Database that a Microsoft SQL Server hosts	TCP	1433	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server \Database\Port • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE \WOW6432Node \Research In Motion \BlackBerry Enterprise Server\Database\Port
incoming data connections from the BlackBerry database notification system	UDP	first unused port number from 4185 to 4499	—

CalHelper connection type and port number

Item	Connection type	Default port number	UI where you can configure the connection
outgoing logger connections to the BlackBerry Messaging Agent	UDP	port number that the BlackBerry Messaging Agent provides	—

IBM Lotus Sametime connection type and port number

Item	Connection type	Default port number	UI where you can configure the connection
incoming data connections from and outgoing data connections to the BlackBerry Collaboration Service	TCP/IP	1533	IBM Lotus Sametime Administration Tool

Microsoft Exchange connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
RPC endpoint mapper	TCP	135	For more information, visit support.microsoft.com to read article 270836.
Microsoft Exchange System Attendant service	TCP	—	For more information, visit support.microsoft.com to read article 270836.
NSPI service	TCP	—	For more information, visit support.microsoft.com to read article 270836.
Microsoft Exchange Information Store service	TCP	—	For more information, visit support.microsoft.com to read article 270836.

Microsoft Office Live Communications Server 2005 connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
incoming data connections from, and outgoing data connections to, the connector for the Microsoft Office Live Communications Server	TLS	5061	Microsoft Office Live Communications Server
incoming data connections from, and outgoing data connections to, the connector for the Microsoft Office Live Communications Server	TCP	5060	Microsoft Office Live Communications Server

BlackBerry Client for use with Microsoft Office Live Communications Server 2005 connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
incoming data connections from, and outgoing data connections to, the Microsoft Office Live Communications Server	TLS	5061	BlackBerry Configuration Panel
incoming data connections from, and outgoing data connections to, the Microsoft Office Live Communications Server	TCP	5060	BlackBerry Configuration Panel

Novell GroupWise Messenger connection type and port number

Item	Connection type	Default port number	UI where you can configure the connection
incoming data connections from, and outgoing data connections to, the BlackBerry Collaboration Service	SSL	8300	Novell GroupWise server that hosts the Novell GroupWise Messaging Agent

SNMP agent connection types and port numbers

Item	Connection type	Default port number	UI where you can configure the connection
incoming syslog connections from the following BlackBerry Enterprise Server components: • BlackBerry Messaging Agent • BlackBerry Dispatcher • BlackBerry Router	UDP	4071	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerrySNMPAgent\Parameters\UDPPort • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Research In Motion

Item	Connection type	Default port number	UI where you can configure the connection
			\BlackBerrySNMPAgent \Parameters\UDPPort
incoming syslog connections from SNMP queries and traps	UDP	161	Windows registry
outgoing syslog connections from SNMP queries and traps	TCP	162	Windows registry

Syslog connection type and port number

Item	Connection type	Default port number	UI where you can configure the connection
listener port for the BlackBerry Enterprise Server events	UDP	514	Windows registry • On a 32-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server \Logging Info \<*component*>\(Default) • On a 64-bit version of Windows: HKEY_LOCAL_MACHINE\SOFTWARE \WOW6432Node \Research In Motion \BlackBerry Enterprise Server\Logging Info \<*component*>\(Default)

Troubleshooting

36

Troubleshooting: Connecting to the BlackBerry Administration Service

The web browser displays an HTTP 404 or HTTP 504 error message when it tries to connect to a BlackBerry Administration Service instance

Possible cause	Possible solution
You created a BlackBerry Administration Service pool using DNS round robin and you stopped the BlackBerry Administration Service services for the BlackBerry Administration Service instance that you currently use. Although you stopped the BlackBerry Administration Service services, it might take some time before the BlackBerry Administration Service instance completes the shutdown process. During this time, if the web browser sends an HTTP request to the BlackBerry Administration Service instance, the BlackBerry Administration Service instance accepts the request because the connection is still available. However, while the BlackBerry Administration Service instance processes the request, it completes its shutdown process and the connection becomes unavailable. The web browser displays an error message.	Wait a few seconds and then try to click a link in the BlackBerry Administration Service console again. The web browser redirects you to an instance in the BlackBerry Administration Service pool that is running and the web browser displays the login page for the instance.
The BlackBerry Administration Service cannot connect to the BlackBerry Configuration Database.	Verify the BlackBerry Administration Service can access the BlackBerry Configuration Database. If necessary, restart the BlackBerry Configuration Database.

Troubleshooting: BlackBerry Enterprise Server Performance

A BlackBerry Enterprise Server that you installed remotely from the BlackBerry Configuration Database uses an unexpected amount of system resources and increases wireless network traffic

Possible cause

Once daily, the BlackBerry Enterprise Server uses the BlackBerry Mailstore Service to refresh the user information from your organization's address book in the BlackBerry Configuration Database. If multiple BlackBerry Enterprise Server instances are associated with a BlackBerry Configuration Database, each BlackBerry Enterprise Server instance tries to use a BlackBerry Mailstore Service to refresh the address book information in the BlackBerry Configuration Database. The first BlackBerry Mailstore Service that starts the refresh process is responsible for completing it.

If the BlackBerry Mailstore Service that is responsible for completing the refresh process is associated with a BlackBerry Enterprise Server that is geographically remote from the BlackBerry Configuration Database, the BlackBerry Mailstore Service can take an unexpected amount of time to complete the refresh process. The refresh process can use an unexpected amount of system resources and increase wireless network traffic.

Possible solution

You can use TraitTool.exe to turn off the address book refresh feature for BlackBerry Enterprise Server instances that are geographically remote from the BlackBerry Configuration Database. As a result, BlackBerry Enterprise Server instances that are located geographically close to the BlackBerry Configuration Database can use the BlackBerry Mailstore Service to refresh the user information from your organization's address book in the BlackBerry Configuration Database.

TraitTool.exe is located in the Tools directory on the BlackBerry Enterprise Server installation media.

1. At the command prompt, navigate to the folder that **TraitTool.exe** is located in.
2. Type: **TraitTool -host** ***<name>*** **-trait MailstoreAddressRefreshEnabled -set False**, where <*name*> is the name of the BlackBerry Enterprise Server instance.
3. Press ENTER.

To turn on the address book refresh feature for a BlackBerry Enterprise Server again, use the same command with a value of True.

Microsoft SQL Server uses a considerable amount of disk space

Possible cause

Reorganizing or rebuilding an index in Microsoft SQL Server can cause the size of the transaction log file in the BlackBerry Configuration Database to grow larger than expected.

Possible solution

Add the following tasks to the end of your organization's regular maintenance plan:

1. Perform a complete backup of the transaction log file.
2. Perform a shrink log file task on the transaction log file.

Troubleshooting: Setting up user accounts

You cannot create a user account in the BlackBerry Administration Service

Possible cause	Possible solution
The BlackBerry Administration Service is configured to use static ports when it connects to the BlackBerry Configuration Database server, but the BlackBerry Configuration Database server uses a dynamic port.	Configure the BlackBerry Administration Service to use a dynamic port for the BlackBerry Configuration Database. 1. On the computer that hosts the BlackBerry Enterprise Server or BlackBerry Enterprise Server components, on the taskbar, click **Start** > **Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**. 2. On the **Database Connectivity** tab, select the **Use dynamic ports or specify SQL port** check box. 3. Click **OK**.

Possible cause	Possible solution
	4. In the Windows Services, restart the services for the BlackBerry Administration Service.

You cannot find a new user account in the directory using the BlackBerry Administration Service

Possible solution

Refresh the list of available user accounts that the BlackBerry Administration Service can access from the directory. By default, the BlackBerry Administration Service refreshes the list of available user accounts at 12:30 AM daily.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Component view**.
2. Click **Email**.
3. Click **Refresh available user list from company directory**.

The background process to refresh the user list starts. The amount of time that the BlackBerry Administration Service requires to refresh the user list depends on the size of the directory.

Troubleshooting: Messaging

Messages are not delivered to BlackBerry devices

Possible cause

A third-party application used the BlackBerry Enterprise Server extension API to filter messages that the BlackBerry Enterprise Server sends to BlackBerry devices.

Possible solution

1. On the computer that stores the BlackBerry Enterprise Server event logs, navigate to <*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\Logs .
2. Search for an event that indicates a third-party application filtered a message (for example, [30425] (07/25 00:11:10.274):{0x1700} {megan.ball@blackberry.com} Message is requested to be blocked. EntryId=123786).

3. Perform one of the following actions:
    - Remove the third-party application that uses the BlackBerry Enterprise Server extension API.
    - Change the third-party application so that it does not filter messages.

Text does not appear correctly in Unicode email messages

Possible cause

By default, when the BlackBerry Enterprise Server receives Unicode messages from BlackBerry devices, it uses UTF-8 character encoding to process the Unicode messages. If email applications cannot correctly display Unicode messages, you can configure the BlackBerry Enterprise Server to use a different character encoding format when it processes Unicode messages.

Possible solution

Change the character encoding that the BlackBerry Enterprise Server uses to process Unicode messages.

Related information

Change the character encoding that the BlackBerry Enterprise Server uses to send Unicode messages, 81

Troubleshooting: Instant messaging

Users cannot view phone numbers for contacts in the BlackBerry Client for IBM Lotus Sametime

Applies to: BlackBerry Enterprise Server version 4.1 SP5 or later with the BlackBerry Client for IBM Lotus Sametime version 2.0.25 or later

Possible cause

The IBM Lotus Sametime API cannot retrieve phone numbers for instant messaging contacts from the IBM Lotus Sametime server. If the BlackBerry Enterprise Server is located in a network that does not permit direct HTTP connections to the IBM Lotus Sametime server, the BlackBerry Collaboration Service cannot retrieve the phone numbers from the IBM Lotus Sametime server instead of the IBM Lotus Sametime API.

Possible solution

You must configure a proxy server that prevents your organization's BlackBerry Enterprise Server from receiving HTTP requests from external servers. If the BlackBerry Enterprise Server is located in an unrestricted network that permits direct HTTP connections to the IBM Lotus Sametime server, the BlackBerry Collaboration Service establishes an HTTP connection to the IBM Lotus Sametime server automatically to retrieve the phone numbers. If your organization's BlackBerry Enterprise Server is located in a restricted network that does not permit direct HTTP connections to the IBM Lotus Sametime server, you must specify an unauthenticated proxy server in the rimpublic.properties file that the BlackBerry Collaboration Service can use to establish an HTTP connection to the IBM Lotus Sametime server.

1. In the BlackBerry Administration Service, on the **Servers and components** menu, expand **BlackBerry Solution topology** > **BlackBerry Domain** > **Components** > **Collaboration**.
2. Click a BlackBerry Collaboration Service instance.
3. Click **Edit instance**.
4. On the **Proxy mappings** tab, configure the settings for an authenticated or unauthenticated proxy server. Use the default web address.
5. Click the **Add** icon.
6. Click **Save All**.
7. To verify that a new entry exists for the BlackBerry Collaboration Service, in the database management console, view the proxy configuration information for the BlackBerry Configuration Database.
8. If the BlackBerry Enterprise Server is located in a restricted network, perform steps 10 to 14.
9. On the computer that hosts the BlackBerry Collaboration Service, navigate to <*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\BBIM\Servers\Instance\Config .
10. In a text editor, open the **rimpublic.properties** file.
11. Copy the following text into the **rimpublic.properties** file. Replace <*host_name*> with the host name of an unauthenticated proxy server:

    [Java Security Property]

    networkaddress.cache.ttl=0

    improxy.proxy.type=http

    improxy.proxy.host=<*hostname*>

    improxy.proxy.port=8080

12. Save and close the **rimpublic.properties** file.
13. Restart the BlackBerry Collaboration Service.

Related information

Restarting BlackBerry Enterprise Server components, 392

A user did not accept a notification about an instant message on a computer and the notification disappeared

Applies to: BlackBerry Collaboration Service version 4.1 or later with the BlackBerry Client for use with Microsoft Office Live Communications Server 2005 or the BlackBerry Client for use with Microsoft Office Communications Server 2007.

Possible cause

A user logged in to Microsoft Office Communicator on a computer and on a BlackBerry device or on two computers.

If the user logged in to Microsoft Office Communicator on both a computer and a BlackBerry device or on two computers, the user received notifications about instant messages in both locations. The instant messaging conversation can occur only in the location where the user accepts the notification about an instant message.

If a user is logged in to Microsoft Office Communicator on both a computer and a BlackBerry device and the user does not accept a notification about an instant message on the computer before the notification disappears, the notification about the instant message disappears from the computer but remains on the BlackBerry device. If the user accepts the notification about the instant message on the computer, the notification about the instant message disappears from the BlackBerry device and the instant messaging conversation occurs on the computer. If the user accepts the notification about the instant message on the BlackBerry device, the notification about the instant message disappears from the computer and the instant messaging conversation occurs on the BlackBerry device.

During an instant messaging conversation, the user cannot switch between a computer and a BlackBerry device or between computers.

Possible solution

The user should look for notifications about instant messages on a BlackBerry device or on another computer where the user might also be logged in to Microsoft Office Communicator. If the user is logged in to Microsoft Office Communicator on a BlackBerry device or on a second computer, the user should only accept the notification about an instant message on the computer or BlackBerry device where the user wants to have the instant messaging conversation.

A user receives a 301 error when the user logs in to an instant messaging application on a BlackBerry device

Applies to: BlackBerry Collaboration Service version 4.1 or later with the BlackBerry Client for use with Microsoft Office Live Communications Server 2005 and the BlackBerry Client for use with Microsoft Office Communications Server 2007.

Possible cause	Possible solution
The BlackBerry Collaboration Service does not support the version of the instant messaging application that is installed on the BlackBerry device.	Remove the instant messaging application from the BlackBerry device. Install an earlier version of the instant messaging application on the BlackBerry device.
The Microsoft Office Communicator Web Access server is not configured correctly for AJAX service.	Verify that the port number for the AJAX service is configured correctly on the Microsoft Office Communicator Web Access server.
In the BlackBerry Client for use with Microsoft Office Live Communications Server 2005, the Microsoft Office Communicator Web Access server is not configured to use forms-based authentication and the BlackBerry Collaboration Service is configured to use HTTPS to connect to the Microsoft Office Communicator Web Access server.	Verify that forms-based authentication is configured on the Microsoft Office Communicator Web Access server.

Troubleshooting: BlackBerry Web Desktop Manager

Troubleshooting: Users cannot log in to the BlackBerry Web Desktop Manager

Possible cause	Possible solution
You might have specified an incorrect URL for the BlackBerry Configuration Database during the BlackBerry Administration Service installation process.	Change the BlackBerry Configuration Database URL.

Troubleshooting: Connections to the Wi-Fi network

A BlackBerry device cannot connect to a Wi-Fi network

Possible cause	Possible solution
On the BlackBerry device, Wi-Fi connections are not turned on.	1. On the BlackBerry device, on the Home screen, click **Manage Connections**. 2. Click **Wi-Fi Options**. 3. In the **Wi-Fi** field, verify that a checkmark appears.
A Wi-Fi profile is not configured on the BlackBerry device.	1. On the BlackBerry device, on the Home screen, click **Manage Connections**. 2. In the **Wi-Fi** field, verify that the name of the Wi-Fi network appears. If the name does not appear, resend the IT policy to the BlackBerry device, or instruct the user to configure a Wi-Fi profile on the BlackBerry device.
The BlackBerry device is not in the wireless coverage area of a wireless access point that has an SSID that is stored in one of the profiles on the BlackBerry device.	Move the BlackBerry device into a wireless coverage area.
The SSID of the access point is not configured on the BlackBerry device.	Check the SSID status indicator in the Wi-Fi status indicator group. The SSID is case-sensitive. If the SSID status indicator is not correct, run Set up Wi-Fi in the Setup Wizard on the BlackBerry device again.
The Wi-Fi settings on the BlackBerry device, IT policy, or Wi-Fi profile were not configured correctly.	Perform any of the following actions: • Using the BlackBerry Enterprise Server, resolve any issues with the IT policy and Wi-Fi profile. Resend the IT policy to the BlackBerry device. • On the BlackBerry device, run Set up Wi-Fi in the Setup Wizard again.
The user account is not configured correctly.	In the BlackBerry Administration Service, resolve any issues with the user account.

Possible cause	Possible solution
The BlackBerry device is not assigned to the correct user account.	In the BlackBerry Administration Service, assign the correct BlackBerry device to the user account.
The BlackBerry Enterprise Server cannot connect to the BlackBerry device.	Perform the following actions: • Ping the BlackBerry device from the BlackBerry Enterprise Server. • Resolve any connection issues in your organization’s network and with the BlackBerry Router.
The settings in the IT policy or Wi-Fi profile were not sent to the BlackBerry device.	Resend the IT policy to the BlackBerry device.
The BlackBerry device is not using the same channel as the access point.	Perform the following actions: • Use a wireless device, such as a laptop computer, to test the association with the access point. Use the settings that the BlackBerry uses to configure the wireless connection. • Use a wireless device, such as a computer, to ping the BlackBerry Router. The ping tests whether the BlackBerry Router is on the ACL of the access point. • If access point logs are available, view the logs to determine the error that occurred. For more information, see the documentation for your organization’s access points.
The authentication method is not configured correctly.	In the BlackBerry Administration Service, verify the configuration information for the authentication method. • If a WEP key or PSK is required, verify that the key is configured correctly. • For WEP authentication, verify that the access point is configured to not filter the MAC address of the BlackBerry device. • For LEAP authentication, verify that the user’s authentication credentials are correct. • For PEAP authentication, verify that the user’s authentication credentials are correct. • For EAP-TLS authentication, verify that the EAP-TLS certificate for the user account is correct.

Possible cause	Possible solution
	Verify that the correct authentication method is configured on the access point and BlackBerry device.
The static IP address and DHCP for the BlackBerry device are not configured correctly.	Perform any of the following actions: • If a static IP address is configured, verify that the parameters such as the subnet mask, default gateway IP address, and DNS IP address are configured correctly. • If the BlackBerry device uses DHCP, verify that the BlackBerry device can obtain a valid IP configuration (for example, an IP address, subnet mask, default gateway IP address, or DNS IP address). • Verify that a wireless device, such as a laptop computer, can connect to the network using DHCP and obtain an IP address. • Verify in the DHCP logs, if they are available, that a DHCP was granted to the BlackBerry device.
Low signal strength is causing intermittent drops in data connectivity.	Move the BlackBerry device into a wireless coverage area.
	1. On the BlackBerry device, in the device options, click **Wi-Fi Connections**. 2. Press the Menu key. 3. Click **Wi-Fi Tools** > **Wi-Fi Diagnostics**. 4. Verify the information in the status fields for the following connection groups: • Wi-Fi • VPN • UMA/GAN (if your organization's mobile network provider supports UMA or GAN and you subscribed for the service) • BlackBerry Infrastructure • Enterprise 5. To view more diagnostic information, press the Menu key and click **Options**. In the **Display Mode** drop-down list, click **Advanced**.

A user cannot see Wi-Fi connection settings on a Wi-Fi enabled BlackBerry device

Possible cause

The Wi-Fi enabled BlackBerry device is not configured to permit a user to make changes to the Wi-Fi configuration settings.

Possible solution

1. In the BlackBerry Administration Service, change the **WLAN Allowed Handheld Changes** configuration setting in the Wi-Fi profile to **Yes**.
2. Resend the IT policy to the BlackBerry device.

Status indicators

The status indicators for Wi-Fi diagnostic information on a BlackBerry device show the status of the BlackBerry device connection to a Wi-Fi network.

Indicator	Description
black	This indicator displays when you or a user did not configure a Wi-Fi network for a BlackBerry device.
yellow or white	This indicator displays when a BlackBerry device tries to connect to a Wi-Fi network but has not connected yet.
green	This indicator displays when a BlackBerry device is connected to a Wi-Fi network.
red	This indicator displays when a connection error exists between the BlackBerry device and a Wi-Fi network.

Status fields for Wi-Fi connections

Field	Description
Current Profile	This field specifies the name of the Wi-Fi profile that the user is currently using.
SSID	This field specifies the identifier for the Wi-Fi network. When the BlackBerry device displays an SSID value, the BlackBerry device is connected to a network, and the name of the network appears.
AP MAC Address	This field specifies the MAC address of the wireless access point that the BlackBerry device is associated with.

Field	Description
	When the BlackBerry device displays a value for the AP MAC Address, the BlackBerry device is associated with the access point.
Security Type	This field specifies the following link security methods: • No Security • WEP • PSK • PEAP • LEAP • EAP-TLS • EAP-FAST • EAP-TTLS When the BlackBerry device displays the link security method, the security on the Wi-Fi connection is turned on and active.
Association	This field shows the status of the BlackBerry device connection to the access point. The status indicators are the following icons: • green check mark: The authentication key is applied, authentication is complete, and keys are used to decrypt packets. • black filled circle: No network connection exists, or no profile exists for an association to a specific access point.
Authentication	This field shows the status of the authentication process on the BlackBerry device.
Local IP Address	This field specifies the IP address of the BlackBerry device. When a BlackBerry device displays a value, it displays the network that the BlackBerry device is associated with.
Signal Level	The field specifies the current signal strength of the BlackBerry device. The value is based on the signal percentage level, from none to excellent.
Connection Data Rate	This field specifies the data rate in Mbps. IEEE 802.11b has a data rate of 11 Mbps, and IEEE 802.11a and IEEE 802.11g have a data rate of 54 Mbps.
Status	This field provides a descriptive status message, such as `"Status acquired"` . It also specifies warnings and errors that a user encountered when the user tried to open a connection to an access point.
Network Type	This field specifies whether the wireless connection type is IEEE 802.11a, IEEE 802.11b, or IEEE 802.11g.

Field	Description
Network Channel	This field specifies the IEEE 802.11 channel that the access point uses.
Pairwise Cipher	This field specifies information about how the access point manages encryption keys for a user account on the network. You can configure an access point to support multiple pairwise ciphers. You can use a pairwise cipher with a group cipher.
Group Cipher	This field specifies information about how the access point manages encryption keys for all user accounts on the network or locally. You can use a pairwise cipher with a group cipher. The group ciphers have one of the following values: • None • WEP 40 • WEP 104 • TKIP • AES-CCMP An access point that you configure to support multiple pairwise ciphers is only as strong as the weakest pairwise cipher.
Gateway Address	This field specifies the IP address of the gateway that routes any packets that the gateway sends outside the local network. In an enterprise Wi-Fi network, this field specifies the IP address of the organization’s LAN gateway. In a personal Wi-Fi network, this field specifies the internal IP address of the router for the home network.
DHCP	This field specifies the status of the DHCP connection to the BlackBerry device. When a check mark displays, DHCP is complete.
Primary DNS	This field specifies the address of an optional computer that translates host names into IP addresses.
Secondary DNS	This field specifies the address of an optional computer that translates host names into IP addresses. The BlackBerry device can use the secondary DNS server if the primary DNS is not available.
DNS Suffix	This field specifies the domain name suffix, such as .com or .org.
Subnet Mask	This field specifies information about the subnet base for the IP address tha the access point assigned to the BlackBerry device.
Server Domain Suffix	This field specifies the domain name suffix for the network that the BlackBerry device is associated with.

Field	Description
Certificate	This field specifies the certificate that the BlackBerry device can use for Wi-Fi authentication, if applicable.
Software Token	If you configured a software token for the BlackBerry device, this field specifies the serial number of the software token.

Status fields for VPN connections

Field	Description
Current Profile	This field specifies the name of the VPN profile that the user is using.
Concentrator Address	This field specifies the IP address of the VPN concentrator.
Contact	This field displays the status of the BlackBerry device connection with the VPN concentrator. A green check mark appears when the BlackBerry device connects with the VPN concentrator.
Authentication	This field displays the status of the VPN authentication on the BlackBerry device. If the last authentication attempt was not successful, the field specifies an error state.
Secure Device IP	This field specifies the IP address of the BlackBerry device on the private network that the VPN protects.
Status	This field specifies a current status message, such as `"Error: Link down"` .
Resolving Concentrator	This field specifies that the IP address of the VPN concentrator was verified.
Concentrator IP	This field specifies the IP address of the VPN concentrator.
Primary DNS	When a VPN session is open, this field specifies the DNS address that corresponds to the primary DNS of the VPN concentrator. If a VPN session is not open, this field specifies the Wi-Fi address.
Secondary DNS	This field specifies the address of an optional computer that translates host names into IP addresses. The BlackBerry device uses the secondary DNS server if the primary DNS is not available.
DNS Suffix	This field specifies the domain that the BlackBerry device uses to resolve addresses on the enterprise Wi-Fi network.

Field	Description
Secure Subnet Mask	This field specifies the subnet mask of the BlackBerry device on the private network that the VPN protects. The subnet mask and IP address provide information about the subnet that the BlackBerry device has connected to.
Retry at	If a BlackBerry cannot log in, this field specifies the next date and time that the BlackBerry device can try to log in.
Session Lifetime	This field specifies the length of time, in seconds, that the BlackBerry device maintains the VPN session before the BlackBerry device renegotiates the session.
Re-login at	This field specifies the length of the periodic rollover or new login period. The BlackBerry device obtains this information from the VPN concentrator.
Failed Login Attempts	This field specifies the number of login attempts that are not successful. If a user logs in, the field is cleared and reverts to 0 automatically.
Certificate	This field specifies the certificate that the BlackBerry device uses for VPN authentication, if applicable.
Software Token	If you configured a software token for the BlackBerry device, this field specifies the serial number of the software token.

Status fields for UMA or GAN connections

If your organization's mobile network provider supports UMA or GAN and your organization subscribes to this service, a UMA/GAN connection group is present on the BlackBerry device.

Field	Description
Connection Preference	This field specifies how the BlackBerry device tries to connect to the mobile network provider’s voice and data services. Using the following settings, you or the user can configure how the BlackBerry device accesses the mobile network provider’s voice and data services: • Wi-Fi Preferred: If possible, the BlackBerry device uses a Wi-Fi connection. When the user is not in a wireless coverage area, the BlackBerry device uses a mobile network connection. • Wi-Fi Only: The BlackBerry device uses a Wi-Fi connection only. • Mobile Network Only: The BlackBerry device uses a mobile network connection to the mobile network provider only.

Field	Description
	- Mobile Network Preferred: If possible, the BlackBerry device uses a mobile network connection but the BlackBerry device can also use a Wi-Fi connection.
UMA Wi-Fi Available	This field specifies whether the user has a UMA profile. You can safely ignore this status field.
Connection	This field specifies whether the BlackBerry device is connected over UMA.
Status	This field specifies the status of the UMA connection.
Registered UNC Address	This field specifies the IP address or FQDN of the UNC.
Registration	This field specifies whether the BlackBerry device is registered with the UNC.
Authentication	This field specifies whether the BlackBerry device is authenticated with the UNC.
Serving UNC Address	This field specifies the UNC that the BlackBerry device is connected to.
Security Gateway IP	This field specifies the IP address of the mobile network provider's security gateway.
Cellular information	This field specifies the cellular information as received from or sent to the UNC, MNC, MCC, mobile network ID (also known as Cell ID) of the BlackBerry device, and ARFCN.
Cellular handover to UMA failures	This field specifies errors that the BlackBerry device received during the transition from one network type to the other when the user is on a call.
Cellular rove-in failures	This field specifies errors that the BlackBerry device received during the transition from one network type to the other when the BlackBerry device is idle.

Status fields for BlackBerry Infrastructure connections

The connection status indicators for the BlackBerry Infrastructure appear on a BlackBerry device when a user makes a Wi-Fi connection or tries to make a Wi-Fi connection.

Field	Description
Address Used	This field specifies the host name or IP address and port number that the BlackBerry device uses to connect to the BlackBerry Infrastructure.
IP Used	This field specifies the host name or IP address and port number that the BlackBerry device uses to connect to the BlackBerry Infrastructure.

Field	Description
Connecting	This field specifies the IP address and port number that the BlackBerry device uses to connect to the BlackBerry Infrastructure.
Authenticating router	This field specifies the IP address of the server that performs authentication, if applicable.
Authenticating server	This field specifies the IP address of the server that performs authentication.
Last Contact At	This field specifies the last time that the BlackBerry device had contact with the BlackBerry Enterprise Server through the BlackBerry Infrastructure.

Status fields for Enterprise connections

Field	Description
UIDs	This field specifies the SRP UID of the BlackBerry Enterprise Server that hosts the user account for the BlackBerry device.
Address Used	This field specifies the host name or IP address and port number that the BlackBerry device uses to connect to the BlackBerry Infrastructure.
IP Used	This field specifies the host name or IP address and port number that the BlackBerry device uses to connect to the BlackBerry Infrastructure.
Connecting	This field specifies the IP address and port number that the BlackBerry device uses to connect to the BlackBerry Infrastructure.
Authenticating router	This field specifies the IP address of the server that performs authentication, if applicable.
Authenticating server	This field specifies the IP address of the server that performs authentication.
Last Contact At	This field specifies the last time that the BlackBerry device had contact with the BlackBerry Enterprise Server through the BlackBerry Infrastructure.

A BlackBerry device cannot open a VPN connection

Possible cause	Possible solution
The connection to the VPN concentrator is not configured correctly.	• Verify that the VPN is turned on. • Ping the IP address of the VPN concentrator.

Possible cause	Possible solution
	- Verify that the VPN concentrator host name resolves to an IP address. If it does not, configure the VPN IP address.
The VPN authentication method is not configured correctly.	- Verify that the VPN server supports the security parameters. - Verify that the VPN login information for the user account are correct.

A BlackBerry device cannot connect to the mobile network using UMA or GAN

Possible cause	Possible solution
The UMA connection is not configured correctly.	1. On the BlackBerry device, in the device options, click **Mobile Network**. 2. Verify that **Wi-Fi Preferred** is selected. 3. On the **Mobile Network** screen, verify that the **Connection Preference** icon is displayed. 4. If the **Connection Preference** icon does not display, at the **Network** icon, type **ALT-GANN** to turn on UMA connectivity.
The UMA profile is not configured correctly.	1. On the BlackBerry device, in the device options, click **UMA**. 2. Verify whether a UMA profile exists. 3. If a UMA profile does not exist, create one using the credentials of the mobile network provider. 4. Verify that for the currently selected UMA profile, the mobile network provider’s security gateway certificate field is not empty and is associated with a certificate for the corresponding mobile network provider.
The BlackBerry device is not connected to the Wi-Fi network or has not registered on a UNC.	1. On the BlackBerry device, on the **Wi-Fi Diagnostics** screen, verify that the BlackBerry device is connected to a Wi-Fi network. 2. Connect a computer to the wireless access point. 3. To verify the IP address of the BlackBerry device, on the **Wi-Fi Diagnostics** screen, ping the computer. 4. If you do not receive a response to the ping, the reason for this error is an issue on the Wi-Fi network.

Possible cause	Possible solution
	5. If you receive a response to the the ping but the BlackBerry device does not display a success message, check the **Status** field for a reason for this error.

Verify whether a BlackBerry device can resolve an IP address

If a BlackBerry device cannot connect to a Wi-Fi network, you can determine which connections the BlackBerry device cannot make to it. You can ping the IP address of another wireless device, the Wi-Fi gateway, a VPN concentrator, the UNC of the mobile network provider, or the BlackBerry Router.

A user can ping network servers from a BlackBerry device to check the availability and responsiveness of network servers.

1. On the BlackBerry device, on the Home screen, click **Manage connections**.
2. Click **Wi-Fi Options**.
3. Press the **Menu** key, and click **Wi-Fi Tools** > **Ping**.
4. In the **Ping Type** field, perform one of the following actions:
   - To ping another wireless device, click **IP or Name**.
   - To ping the BlackBerry device, click **Self**.
   - To ping the security gateway, click **WLAN Gateway**.
   - To ping the VPN concentrator, click **VPN Concentrator**.
   - To ping the UNC of the mobile network provider, click **UNC**.
   - To ping the BlackBerry Router, click **BBR**.
5. In the **Ping to** field, type the IP address that you want to ping.
6. In the **Number of Pings** field, type the number of times that you want to ping the IP address.
7. On the menu, click **Send ping**.

Look up a computer name to resolve an IP address

Using a BlackBerry device, a user can look up a computer name in the DNS server to resolve network or domain names and IP addresses.

1. On the BlackBerry device, on the Home screen, click **Manage connections**.

2. Click **Wi-Fi Options**.
3. Press the **Menu** key and click **Wi-Fi Tools** > **DNS Lookup**.
4. In the **Host** field, type a name or an IP address that you want to look up.
5. Press the **Menu** key and click **DNS Lookup**.
6. Press the **Menu** key and click **Send ping**.

Troubleshooting: BlackBerry Administration Service pools

BlackBerry Administration Service instances located in different network segments are not connecting to each other

Possible cause

If BlackBerry Administration Service instances are located in different network segments that are separated by a firewall, the firewall can block the dynamic ports on the BlackBerry Administration Service.

Possible solution

Perform the following actions:

1. Make sure that you configured the BlackBerry Administration Service instances to communicate across network subnets using TCP with TCP ping, instead of multicast UDP.
2. On each computer that hosts a BlackBerry Administration Service instance, navigate to <*drive*>:\Program Files\Research in Motion\BlackBerry Enterprise Server\BAS\server\default\conf.
3. In a text editor, open **service-port-bindings.xml**.
4. Move the line <**attribute name** =**"secondaryBindPort'"**>**xyz**</**attribute**> that is located inside the comment tags outside of the comment tags.
5. Change **xyz** to an available port, for example port 14458.
6. Add the port that you configured in step 5 to the firewall.

Troubleshooting: BlackBerry Monitoring Service connections

A user cannot log in to the BlackBerry Monitoring Service

Possible cause

If your organization's environment includes a firewall located between the BlackBerry Administration Service and BlackBerry Monitoring Service, the firewall can block the JNDI delegate port on the BlackBerry Administration Service. By default, the JNDI delegate port is configured to 0 (any port).

Possible solution

Configure the JNDI delegate port to use a specific port number and open the port on the firewall by performing the following actions:

1. On the computer that hosts a BlackBerry Administration Service instance, navigate to <*drive*>:\Program Files\Research In Motion\BlackBerry Enterprise Server\BAS\server\default\conf.
2. In a text editor, open **service-port-bindings.xml**.
3. In the paragraph **cluster-service.xml**, uncomment the line <**attribute name="RmiPort"**>**11101**</**attribute**>. The port number can be port 11101 or any port from port 1000 to port 5000.
4. Comment out the line <**attribute name="RmiPort"**>**0**</**attribute**>.
5. Add the JNDI delegate port that you configured in step 3 to the firewall.

Troubleshooting: IT policies

I cannot find an IT policy rule in the BlackBerry Administration Service

Possible cause

The version of the BlackBerry Enterprise Server that you are using does not include the IT policy rule.

Possible solution

Import the IT policy rule from an IT policy pack that is available from www.blackberry.com/support. For more information about IT policy packs, search the BlackBerry Technical Solution Center at www.blackberry.com/support. For example, to find the IT policy pack that includes the IT policy rules for BlackBerry Device Software 5.0, search for "IT policy rules for BlackBerry Device Software 5.0".

Glossary

37

AAA	Authentication, Authorization, Accounting
AES	Advanced Encryption Standard
ACL	An access control list (ACL) is a list of permissions that are associated with an object, such as a file, directory, or other network resource. It specifies which users or components have permission to perform specific operations on an object.
ACP	ANSI code page
AES	Advanced Encryption Standard
AES-CCMP	Advanced Encryption Standard Counter Mode CBCMAC Protocol
AJAX	Asynchronous JavaScript and XML
ANSI	American National Standards Institute
API	application programming interface
ARFCN	absolute radio frequency channel
ASCII	American Standard Code for Information Interchange
BCC	blind carbon copy
BlackBerry CAL	A BlackBerry Client Access License (BlackBerry CAL) limits how many users you can add to a BlackBerry Enterprise Server.
BlackBerry Domain	A BlackBerry Domain consists of the BlackBerry Configuration Database with its users and any BlackBerry Enterprise Server instances that connect to it.
BlackBerry MDS	BlackBerry Mobile Data System
BlackBerry MVS	BlackBerry Mobile Voice System
BlackBerry transport layer encryption	BlackBerry transport layer encryption (formerly known as standard BlackBerry encryption) uses a symmetric key encryption algorithm to help protect data that is in transit between a BlackBerry device and the BlackBerry® Enterprise Server when the data is outside an organization's firewall.
CDMA	Code Division Multiple Access
CDO	Collaboration Data Object
CLDC	Connected Limited Device Configuration

CMIME	Compressed Multipurpose Internet Mail Extension
content protection	Content protection helps protect user data on a locked BlackBerry device by encrypting the user data using the content protection key and ECC private key.
CRL	certificate revocation list
CSR	certificate signing request
DES	Data Encryption Standard
device transport key	The device transport key (formerly known as the master encryption key) is unique to a BlackBerry device. The BlackBerry device and BlackBerry Enterprise Server use the device transport key to encrypt the message keys.
DFS	distributed file system
DHCP	Dynamic Host Configuration Protocol
DNS	A Domain Name System (DNS) is an Internet database that translates domain names that are meaningful and recognizable by people into the numeric IP addresses that the Internet uses.
DOM	Document Object Model
DSML	Directory Service Markup Language
DSML-enabled server	A BlackBerry device uses a DSML-enabled server to search for and download certificates.
EAP-FAST	Extensible Authentication Protocol Flexible Authentication via Secure Tunneling
EAP-GTC	Extensible Authentication Protocol Generic Token Card
EAP-TLS	Extensible Authentication Protocol Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol Tunneled Transport Layer Security
EAP	Extensible Authentication Protocol
Enterprise Service Policy	The Enterprise Service Policy controls which BlackBerry devices can connect to a BlackBerry Enterprise Server.
ETP	Email Transfer Protocol
FQDN	fully qualified domain name
GAN	generic access network
gateway message envelope	The gateway message envelope protocol is a Research In Motion proprietary protocol that allows the transfer of compressed and encrypted data between the wireless network and BlackBerry devices. The protocol defines a routing layer that specifies the types of message contents allowed and the addressing information for the data. Gateways and routing components use this information to identify the type and source of the BlackBerry device data, and the appropriate destination service to route the data to.

GPO	Group Policy Object
GPS	Global Positioning System
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IIS	Internet Information Services
IP address	An Internet Protocol (IP) address is an identification number that each computer or mobile device uses when it sends or receives information over a network, such as the Internet. This identification number identifies the specific computer or mobile device on the network.
IPPP	Internet Protocol Proxy Protocol
IPsec	Internet Protocol Security
IT administration command	An IT administration command is a command that you can send over the wireless network to protect sensitive information on a BlackBerry device or delete all BlackBerry device data.
IT policy	An IT policy consists of various IT policy rules that control the security features and behavior of BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager.
IT policy rule	An IT policy rule permits you to customize and control the actions that BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager can perform.
Java ME	Java Platform, Micro Edition
JDE	Java Development Environment
JNDI	Java Naming and Directory Interface
JRE	Java Runtime Environment
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over SSL
LEAP	Lightweight Extensible Authentication Protocol
LED	light-emitting diode
LTPA	Lightweight Third-Party Authentication
MAC	message authentication code
MAPI	Messaging Application Programming Interface
MCC	mobile country code

messaging server	A messaging server sends and processes messages and provides collaboration services, such as updating and communicating calendar and address book information.
MIDP	Mobile Information Device Profile
MIME	Multipurpose Internet Mail Extensions
mirror database	In database mirroring, a mirror database is a standby copy of a principal database.
MNC	mobile network code
MTLS	Mutual Transport Layer Security
NAT	network address translation
NSPI	Name Service Provider Interface
NTLM	NT LAN Manager
OCSP	Online Certificate Status Protocol
OEM	original equipment manufacturer
PAC	proxy auto-configuration
PAP	Push Access Protocol
PEAP	Protected Extensible Authentication Protocol
PIM	personal information management
PIN	personal identification number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
principal database	In database mirroring, a principal database is the database that starts the mirroring session.
PSK	pre-shared key
RMI	Record Management System
RPC	remote procedure call
RTF	Rich Text Format
SAN	subject alternative name
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPN	service principal name

SQL	Structured Query Language
SRP	Server Routing Protocol
SRP ID	The SRP ID is a unique identifier for the BlackBerry Enterprise Server that the BlackBerry Enterprise Server uses to identify itself to the BlackBerry Infrastructure during SRP authentication.
SSID	service set identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of communication protocols that is used to transmit data over networks, such as the Internet.
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
Triple DES	Triple Data Encryption Standard
UCS	Universal Content Stream
UDP/IP	User Datagram Protocol/Internet Protocol
UDP	User Datagram Protocol
UID	unique identifier
UMA	Unlicensed Mobile Access
UNC	Universal Naming Convention
USB	Universal Serial Bus
UTF	UCS Transformation Format
UTF-8	8-bit UCS/Unicode Transformation Format
UTF-16LE	UCS Transformation Format 16 Little Endian
VPN	virtual private network
VoIP	Voice over Internet Protocol
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
witness	In database mirroring, a witness is a Microsoft SQL Server instance that permits the mirror database to know when to promote itself.
WLAN	wireless local area network
XML	Extensible Markup Language

Legal notice

38

Adobe and Acrobat are trademarks of Adobe Systems Incorporated. ANSI is a trademark of the American National Standards Institute. Apache Tomcat is a trademark of The Apache Software Foundation. Bluetooth is a trademark of Bluetooth SIG. Cisco is a trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Corel and WordPerfect are trademarks of Corel Corporation. Eclipse is a trademark of Eclipse Foundation, Inc. Entrust Authority is a trademark of Entrust, Inc. Firefox is a trademark of Mozilla Foundation. GSM is a trademark of the GSM MOU Association. IBM, Domino, Lotus, Lotus Notes, Lotus Symphony, and Sametime are trademarks of International Business Machines Corporation. IEEE, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, and 802.1X are trademarks of the Institute of Electrical and Electronics Engineers, Inc. Linux is a trademark of Linus Torvalds. Java, JavaScript, and JRE are trademarks of Oracle and/or its affiliates. Kerberos is a trademark of the Massachusetts Institute of Technology. Microsoft, Active Directory, ActiveX, Excel, Internet Explorer, Outlook, Lync, PowerPoint, SQL Server, Visual Studio, Windows, Windows Event Log, Windows Server, Windows Vista, and Windows XP are trademarks of Microsoft Corporation. Netscape is a trademark of Netscape Communication Corporation. Novell and GroupWise are trademarks of Novell, Inc. PGP is a trademark of PGP Corporation. RSA and RSA SecurID are trademarks of RSA Security. Wi-Fi is a trademark of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at www.blackberry.com/go/docs is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). RIM does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by RIM of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A

COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-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.

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