BlackBerry Enterprise Server for Microsoft Exchange

Version: 4.1 | Service Pack: 7

Administration Guide

BlackBerry

Published: 2009-11-9
SWD-907816-1109013225-001

Contents

Creating administrator accounts

1

Administrative roles

You can use the predefined roles in the BlackBerry® Enterprise Server, that mirror typical administrative roles that exist in organizations, to control which administrators can perform specific tasks and what information the administrators can view.

You assign each BlackBerry Enterprise Server administrator to an administrative role. If you manage your organization's BlackBerry Enterprise Server using Windows® groups, you can assign the groups to the administrative roles so that you can manage role membership within the group.

If an administrator starts the BlackBerry Manager, the BlackBerry Manager checks the administrator's authentication credentials, determines which administrative role the administrator is assigned to, and displays a list of the tasks that the administrator can perform.

Role	Description
security administrator (rim_db_admin_security)	These administrators can perform all tasks and can view all information. They are the only administrators who can manage role membership. The administrator account that you created during the installation process is assigned the security administrator role automatically.
enterprise administrator (rim_db_admin_enterprise)	These administrators can perform all tasks for user accounts, BlackBerry Enterprise Server instances, and global application data. These administrators can perform some security tasks. These administrators cannot view role membership.
device administrator (rim_db_admin_handheld)	These administrators can perform tasks for managing BlackBerry devices and user accounts.
senior help desk administrator (rim_db_admin_sr_helpdesk)	These administrators can perform all device management tasks that relate to user account management.
junior help desk administrator (rim_db_admin_jr_helpdesk)	These administrators can perform specific tasks to manage user accounts. However, these administrators cannot add, move, or delete user accounts or send specific IT administration commands.

Creating a BlackBerry Enterprise Server administrator in a Microsoft SQL Server environment

BlackBerry® Enterprise Server administrators are database users who can access the BlackBerry Configuration Database using the BlackBerry Manager. This access is restricted to the administrative roles that the BlackBerry Enterprise Server administrators are assigned to.

Only administrators who are assigned to the security administrator role can create other BlackBerry Enterprise Server administrators accounts. When creating administrator accounts, perform one of the following tasks:

- assign an administrative role to an existing database account
- create a new database account and assign it an administrative role

Assign an administrative role to a new or existing Microsoft SQL Server database account

Note: Do not assign an administrative role using the Microsoft® SQL Server® consoles or assign more than one administrative role to an administrator. The BlackBerry® Configuration Database uses the most restrictive settings to determine which tasks the BlackBerry Manager displays, so an administrator who is assigned both enterprise and junior help desk roles sees only the tasks for the junior help desk role.

Before you begin:

- Verify that you have the system administrator role on the database server.
- If you are assigning an administrator to the security or enterprise administrative role, verify that the administrator has administrative permission on the Microsoft® Exchange messaging server.
- If you are creating a new database account and want to use Windows® authentication, verify that the Windows user account or group already exists.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Role Administration** tab, click a role.
3. Complete one of the following actions:
   - To add an administrative role to an existing Microsoft SQL Server database account, click **List Administrators**.
   - To create a new Microsoft SQL Server database account and assign it to an administrative role, click **Add Administrators**.
4. Complete one of the following actions:
   - To add an administrative role to an existing administrator account, click the administrator account that you want to add the role to.
   - To create a database account only and add an administrative role to the account, type a user name.
   - To create a database account for an existing Windows user account or group and add an administrative role to the account, type a user name preceded by a domain name (for example, DOMAIN\username).
5. If prompted, type and confirm a password.

6. Click **OK**.

Configure the BlackBerry Manager to use database authentication in a Microsoft SQL Server environment

During the installation process, if you choose to connect to the BlackBerry® Configuration Database using Windows® authentication, the BlackBerry Manager uses Windows authentication automatically. If you create database accounts for your administrators, you must change the type of authentication that the BlackBerry Manager uses.

1. In the BlackBerry Manager, on the **Tools** menu, click **Options**.
2. Click **Database**.
3. In the **Authentication** drop-down list, click **Database Authentication**.
4. Click **OK**.
5. Restart the BlackBerry Manager.

Configuring security options

2

How the BlackBerry Enterprise Solution encrypts data on the transport layer

The BlackBerry® Enterprise Solution uses a symmetric key encryption algorithm (Triple DES or AES) to protect all data that the BlackBerry® Enterprise Server and a BlackBerry device send between them.

The BlackBerry Enterprise Solution uses the symmetric key encryption algorithm to create message keys and master encryption keys, and uses those encryption keys to encrypt all data that the BlackBerry device sends or receives, while the data travels between the BlackBerry device and the BlackBerry Enterprise Server.

This data encryption process occurs automatically and is designed to verify that a message that a user sends from a BlackBerry device, which is outside the organization's firewall, remains protected on the transport layer until the BlackBerry Enterprise Server receives the message.

Symmetric key encryption algorithms that the BlackBerry Enterprise Solution uses

Encryption type	Description
Triple DES (default encryption method)	• uses the Triple DES algorithm to encrypt and decrypt all of the data that the BlackBerry® Enterprise Server and BlackBerry devices that are associated with the BlackBerry Enterprise Server send between each other
AES	• uses the AES algorithm to encrypt and decrypt all of the data that the BlackBerry Enterprise Server and BlackBerry devices that are associated with the BlackBerry Enterprise Server send between each other • designed to use a longer encryption key to provide a better combination of security and performance than Triple DES • designed to protect user data and encryption keys from traditional attacks and side-channel attacks • requires BlackBerry® Desktop Software version 4.0 or later and BlackBerry® Device Software version 4.0 or later
Triple DES and AES	• by default, uses AES encryption on BlackBerry devices that support AES

Encryption type	Description
	• permits use of the Triple DES algorithm or AES algorithm to encrypt and decrypt all data that the BlackBerry Enterprise Server and BlackBerry devices that are associated with the BlackBerry Enterprise Server send between each other • uses Triple DES encryption for BlackBerry devices that do not support AES (BlackBerry devices that are running BlackBerry Device Software versions earlier than version 4.0)

Change the encryption type

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. Click **General**.
4. In the **Security** section, click **Encryption Algorithm**.
5. In the drop-down list, select an encryption type.
6. Click **OK**.

After you finish: If you changed the encryption type, you must reactivate all of the BlackBerry devices in the BlackBerry Domain so that users can send and receive messages on their BlackBerry devices.

Related topics
Assigning BlackBerry devices to user accounts, 71

Options for extending messaging security

When a user sends a message from the BlackBerry® device, by default, the BlackBerry® Enterprise Server does not encrypt the message when it forwards the message to the message recipient. To extend the messaging security that standard BlackBerry encryption provides, the user must install additional secure messaging technology on the BlackBerry device, and you must set the BlackBerry device to use that secure messaging technology.

To offer an additional layer of messaging security between the sender and recipient of an email message or PIN message, you can turn on S/MIME technology or PGP® technology for BlackBerry devices. When you use either one of these technologies, you allow sender-to-recipient authentication and confidentiality. These technologies also help to maintain the integrity and privacy of the data from the time that a BlackBerry device user sends a message from the BlackBerry device to when the message recipient decrypts and opens the message.

Protection of data using the PGP Support Package for BlackBerry devices

BlackBerry® devices that are running the PGP® Support Package for BlackBerry® devices can digitally sign, encrypt, or sign and encrypt data that they send to the BlackBerry® Enterprise Server.

With supported versions of the PGP Support Package for BlackBerry devices installed, BlackBerry devices can receive PGP/MIME format messages. With both the PGP Support Package for BlackBerry devices and the S/MIME Support Package for BlackBerry® devices installed and turned on, BlackBerry devices can download PGP® keys with attached S/MIME X.509 certificates from the PGP® Universal Server and use them in compliance with the PGP Universal Server secure email policy. The PGP Support Package for BlackBerry devices continues to support OpenPGP format messages.

For more information, see the *PGP Support Package for BlackBerry Devices Security Technical Overview*.

Prerequisites: Protecting data using the PGP Support Package for BlackBerry devices

- Set the PGP® Universal Server Address IT policy rule in the IT policy that you assign to BlackBerry® device users.
- Instruct the BlackBerry device users to install the PGP® Support Package for BlackBerry® devices on their BlackBerry devices and enroll with the PGP Universal Server so that the BlackBerry devices can process PGP messages.
- Instruct the BlackBerry device users to enroll with PGP when the BlackBerry devices prompt them to.

Prerequisites: Protecting data using the S/MIME Support Package for BlackBerry smartphones

- Turn on S/MIME message processing on the BlackBerry® Enterprise Server so that the BlackBerry Enterprise Server can process S/MIME messages.
- Instruct users to install the S/MIME Support Package for BlackBerry® smartphones on the BlackBerry devices so that the BlackBerry devices can process S/MIME messages.
- 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 or configure the BlackBerry Enterprise Server to permit users to enroll certificates over the wireless network.

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

1. In the BlackBerry® Manager, in the left pane, click **Servers**.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Messaging**.
4. In the **Secure Messages** section, click **Enable S/MIME Message Processing**.
5. In the drop-down list, click **True**.
6. Click **OK**.

How S/MIME-protected messages on BlackBerry devices discard appended disclaimers

If a user installs and configures the S/MIME Support Package for BlackBerry® smartphones on a BlackBerry device, the BlackBerry® Enterprise Server does not apply an appended disclaimer to S/MIME-protected messages that the 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.

Define encryption options for S/MIME-protected messages

1. In the BlackBerry® Manager, in the left pane, click **Servers**.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Messaging**.
4. In the **Secure Messages** section, select the encryption options to include when processing S/MIME-protected messages.
5. Click **OK**.

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 BlackBerry devices that can decrypt PIN messages that users in your organization send from their BlackBerry devices, you can generate a new PIN encryption key that is stored on and known only to BlackBerry devices in your organization. BlackBerry devices with a PIN encryption key that is specific to your organization can send and receive PIN messages only with other BlackBerry devices that store the same PIN encryption key.

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

Generate a new peer-to-peer encryption key

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, expand **Service Control & Customization**.
3. Click **Update Peer-to-Peer Encryption Key**.
4. Click **Set or update the Peer-to-Peer encryption key for all devices within this organization**.
5. Click **Yes**.

Authenticating the BlackBerry MDS Integration Service to the BlackBerry Manager and web services

After you install the BlackBerry® MDS Integration Service, you must install a digital certificate for the BlackBerry MDS Integration Service in the key store on the same computer. This certificate allows server-authenticated communication between the BlackBerry MDS Integration Service and the BlackBerry Manager.

You can install a self-signed certificate for the BlackBerry MDS Integration Service, or you can get a signed root certificate from a certificate authority and install it in the key store using the Java® keytool. You can replace the self-signed certificate with a signed root certificate at any time, but you should install the certificate that you want to use immediately after you install the BlackBerry MDS Integration Service and before you allow authentication with the BlackBerry Manager or web services using that certificate.

You can also export the certificate for the BlackBerry MDS Integration Service to allow client authentication with external web services.

For more information about using the Java keytool, visit java.sun.com/javase/6/docs/technotes/tools/windows/keytool.html.

Allow the BlackBerry MDS Integration Service to communicate with the BlackBerry Manager

When the BlackBerry® Manager connects to the BlackBerry MDS Integration Service for the first time after installation, the BlackBerry Manager prompts you to view and install the BlackBerry MDS Integration Service self-signed certificate. This certificate allows server-authenticated communication between the BlackBerry MDS Integration Service and the BlackBerry Manager.

Before you begin: Perform this task immediately after you install the BlackBerry MDS Integration Service.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Integration Service.
2. In the certificate installation dialog box, click **View Certificate**.
3. Review the certificate information.
4. Click **Install Certificate**.
5. Complete the instructions on the screen. Accept the default settings.
6. When prompted, click **Cancel**.

Allow client authentication between the BlackBerry MDS Integration Service and web services

The self-signed certificate for the BlackBerry® MDS Integration Service allows client authentication between the BlackBerry MDS Integration Service and web services hosts. If the BlackBerry® MDS Runtime Applications in your organization's environment use HTTPS to communicate with web servers to receive application data and application updates, you must export the certificate for the BlackBerry MDS Integration Service to the web services hosts. This allows BlackBerry MDS Runtime Applications that use web services to authenticate to the web services and access them.

Before you begin:

- Contact your organization's application developers for information about the web services that the BlackBerry MDS Runtime Applications in your environment use.
- If you replaced the self-signed certificate for the BlackBerry MDS Integration Service with a signed root certificate from a certificate authority, the web services must trust the root certificate authority to authenticate to the BlackBerry MDS Integration Service.

1. Using Microsoft® Internet Explorer®, export the self-signed certificate for the BlackBerry MDS Integration Service from the trusted root certificate authorities area of the computer's key store.
2. Send the self-signed certificate to the web services servers that the BlackBerry MDS Runtime Applications use.
3. Verify that the certificate is installed in the trusted key store of the web services servers.

After you finish:

- If multiple BlackBerry MDS Integration Service servers are installed, export the certificate for each BlackBerry MDS Integration Service.
- Allow BlackBerry MDS Runtime Applications to access web services using HTTPS.

Setting up proxy servers for BlackBerry Enterprise Server components 3

Configuring certain BlackBerry Enterprise Server components to use proxy servers

You can configure the BlackBerry® MDS Connection Service, BlackBerry MDS Integration Service, and 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.

The BlackBerry MDS Integration Service sends application updates and data to BlackBerry devices through the BlackBerry MDS Connection Service. The BlackBerry MDS Integration Service can only accept and respond to messages that it receives from a direct connection with the BlackBerry MDS Connection Service. If you configured the BlackBerry MDS Connection Service to use a proxy server, you must configure proxy rules to permit a direct connection between the BlackBerry MDS Connection Service and the BlackBerry MDS Integration Service. You cannot use a proxy server to exchange data between these components. If you use a .pac file configuration, you can change the .pac file to permit a direct connection between the BlackBerry MDS Connection Service and BlackBerry MDS Integration Service.

Related topics

Configuring multiple BlackBerry Enterprise Server instances to use the same BlackBerry Enterprise Server component, 25

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

You can configure the BlackBerry® MDS Connection Service, BlackBerry MDS Integration Service, or BlackBerry Collaboration Service to use a .pac file.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry® Enterprise Server component.
2. On the appropriate tab for a BlackBerry Enterprise Server component, click **Edit Properties**.
3. In the left pane, click **Proxy**.
4. Double-click **Proxy Mappings**.
5. Click **New**.
6. Double-click **Universal Resource Locator**.
7. Type the URL regular expression that you want the proxy mapping rule to control.

8. Double-click **Proxy String**.
9. Click **New**.
10. In the **Proxy Type** drop-down list, perform one of the following actions:
    - To detect a .pac file automatically, click **AUTO**. Double-click the **Proxy String** field and delete the default values.
    - To specify the location of the .pac file, click **PAC**. Double-click the **Proxy String** field and type the proxy server name, port number, and location of the .pac file (for example, http://*<ProxyServer>*:*<Port>*/*<PACFilePath>*/*<PACFileName>*).
11. Click **OK**.

Configure a BlackBerry Enterprise Server component to use a proxy server

You can configure the BlackBerry® MDS Connection Service, BlackBerry MDS Integration Service, or 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 typed, until it accesses the web server successfully.

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 Manager, in the left pane, click a BlackBerry Enterprise Server component.
2. On the appropriate tab for a BlackBerry Enterprise Server component, click **Edit Properties**.
3. In the left pane, click **Proxy**.
4. Click **New**.
5. In the **Universal Resource Locator** field, type the regular expression for the web address that you want the proxy mapping rule to control.
6. Double-click **Proxy String**.
7. Click **New**.
8. In the **Proxy Type** drop-down list, perform any of the following actions:
    - To configure a proxy server, click **PROXY**. Double-click the **Proxy String** field and type the proxy server name and port number.
    - To exclude the web address from routing through the proxy server, click **DIRECT**. Double-click the **Proxy String** field and delete the default value.
9. Click **OK**.

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, BlackBerry MDS Integration Service, or BlackBerry Collaboration Service to authenticate to a proxy server on behalf of BlackBerry devices.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry® Enterprise Server component.
2. On the appropriate tab, click **Edit Properties**.
3. In the left pane, click **Proxy**.
4. Double-click **Proxy Mappings**.
5. Click a URL.
6. Click **Properties**.
7. 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.
8. In the **Password** field, type the password for the user name.
9. In the **Password (Confirmation)** field, retype the password.
10. Click **OK**.

Sharing BlackBerry Enterprise Server components 4

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, BlackBerry MDS Integration 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 from BlackBerry devices, and to manage HTTP requests from the BlackBerry® Browser.

Before you begin: You must set a BlackBerry MDS Connection Service in your BlackBerry Domain as the central push server.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Service Control & Customization**.
3. Click **MDS CS to BES Mapping**.
4. In the **MDS CS to BES Mappings** dialog box, in the left pane, click the BlackBerry MDS Connection Service that you have set as the central push server.
5. In the right pane, click the BlackBerry Enterprise Server instances that you want to use the central push server.
6. Click **OK**.

Related topics

Specifying a BlackBerry MDS Connection Service as the central push server, 58

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

You can configure multiple instances of the BlackBerry® Enterprise Server to use the same BlackBerry MDS Integration Service to send BlackBerry MDS Runtime Applications and updates to BlackBerry devices. By associating multiple instances of the BlackBerry Enterprise Server with a single BlackBerry MDS Integration Service, you can make the BlackBerry MDS Runtime Applications that are stored in a single BlackBerry MDS Application Repository available to users on multiple BlackBerry Enterprise Server instances.

Before you begin: You must configure server authentication between the BlackBerry MDS Integration Service and the BlackBerry Manager. Complete the instructions on the screen the first time that you click the BlackBerry MDS Integration Service.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **MDS Integration Service**.
4. Click **BlackBerry MDS Integration Service Server URL**.
5. In the drop-down list, click the BlackBerry MDS Integration Service that you want to assign to the BlackBerry Enterprise Server.
6. Click **OK**.

After you finish: Repeat this task for each BlackBerry Enterprise Server that you want to associate with the same BlackBerry MDS Integration Service.

Related topics

Allow the BlackBerry MDS Integration Service to communicate with the BlackBerry Manager, 20

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 that you use in your organization's BlackBerry Domain.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Service Control & Customization**.
3. Click **IM to BES Mapping**.
4. In the **IM to BES Mappings** dialog box, in the left pane, click the BlackBerry Collaboration Service that you want multiple BlackBerry Enterprise Server instances to use.
5. In the right pane, select the BlackBerry Enterprise Server instances that you want to have use the BlackBerry Collaboration Service.
6. Click **OK**.

Configuring user accounts

5

Adding user accounts to the BlackBerry Enterprise Server

When you add a user account to the BlackBerry® Enterprise Server, the BlackBerry device user's Microsoft® Exchange mailbox does not have to be located in the same Microsoft Exchange site or routing group as the BlackBerry Enterprise Server.

Add a user account to one BlackBerry Enterprise Server at a time.

Related topics
Assigning BlackBerry devices to users, 70

Add user accounts to the BlackBerry Enterprise Server

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Common**.
3. Click **Add Users**.
4. In the **Show Names from the** drop-down list, click an address group.
5. In the user list, click one or more users.
6. Click **Select**.
7. Click **OK**.

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 user group

Create groups of user accounts in the BlackBerry® Domain to apply common configuration properties for the user group or to perform administrative tasks on all user accounts in the user group. User accounts in a user group can be located on different BlackBerry® Enterprise Server instances in the BlackBerry Domain.

1. In the BlackBerry Manager, in the left pane, click **User Groups**.
2. Click **Create Group**.
3. Type a name and description for the user group.
4. Click **OK**.

Add a user account to a user group

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click one or more user accounts.
3. Click **Assign User to Group**.
4. Click a group name.
5. Click **OK**.

When you add user accounts to a group, the BlackBerry Manager assigns the group properties to the user accounts automatically.

Sending software and BlackBerry Java Applications to BlackBerry devices

6

Making BlackBerry Device Software and Java applications available to users

You can make BlackBerry® Device Software or applications available on a network drive, and make the software available to a user account or user group using one of the following methods:

- send BlackBerry Java® Applications, the collaboration client, or the BlackBerry® MDS Runtime to BlackBerry devices over the wireless network
- install BlackBerry Device Software on or add applications to a BlackBerry device that is connected to the computer that hosts the BlackBerry Manager
- make the BlackBerry Device Software and applications available so that a user can install the software and add applications using the application loader tool

You can also create a software configuration to define how the BlackBerry® Enterprise Server delivers the applications to BlackBerry devices, and which applications users can add to BlackBerry devices.

Making software and applications available on a network drive

To make the BlackBerry® Device Software or applications available for users to install on or add to their BlackBerry devices, you must save the BlackBerry Device Software and applications to a network drive and create a software index. You can maintain only one version of software or an application on the network drive at a time.

Install the BlackBerry Device Software on a network drive

You install the BlackBerry® Device Software on a network drive to make the BlackBerry Device Software available to users to install on their BlackBerry devices.

Before you begin: Your organization's wireless service provider must provide you with the BlackBerry Device Software installation media.

1. Copy the BlackBerry Device Software installation media to a network drive in your organization's environment.
2. On the network drive, double-click the .exe file.
3. Complete the installation process.

After you finish: Verify that the files are located at *<drive>*:\Program Files\Common Files\Research In Motion\Shared\Loader Files.

Add a Java application to a network drive

You add a Java® application to a network drive so that the application can be made available to users' BlackBerry® devices.

Before you begin: If a third-party developer requires you to add an application to copy the application files, you must complete the instructions that the vendor provides. You can then copy the required application files and module files to a network drive in your organization's environment.

1. If necessary, on the network drive, create the path *<drive>*:\Program Files\Common Files\Research In Motion\Shared \Applications.
2. In the **Applications** folder, create a subfolder for the application that you want to add.
3. Copy the .alx, .cod, and .dll files to the subfolder.

Add a collaboration client to a network drive

You add a collaboration client to a network drive to make the application avaliable for users to install on their BlackBerry® devices. 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.

1. If necessary, on the network drive, create the path *<drive>*:\Program Files\Common Files\Research In Motion\Shared \Applications.
2. Visit www.na.blackberry.com/eng/support/downloads to download the collaboration client for your organization's environment.
3. Double-click the .zip file that you downloaded.
4. Extract the .alx and .cod files to the path that you created in step 1.

Add the BlackBerry MDS Runtime to a network drive

You add the BlackBerry® MDS Runtime to a network drive for users to install on their BlackBerry devices so that they can use BlackBerry MDS Runtime Applications.

1. Visit www.na.blackberry.com/eng/support/downloads to download the most recent version of the BlackBerry MDS Runtime.
2. If necessary, on the network drive, create the path *<drive>*:\Program Files\Common Files\Research In Motion\Shared \Applications.
3. Create a folder for the BlackBerry MDS Runtime.
4. From the .zip file that you downloaded, extract the **MdsRuntime.alx** file and the .cod files for the applicable BlackBerry® Device Software version to the BlackBerry MDS Runtime folder that you created in step 3.

Indexing applications on a network drive

To inform the application loader tool and software configurations of the applications that are available to add to BlackBerry® devices, you create a software index for the applications that you add to your organization's network drive. When you create a software index, the BlackBerry® Enterprise Server creates a specification.pkg file and a PkgDBCache.xml index file for each application.

Create or update a software index for applications on a network drive

Not all software or applications require indexing. If you add BlackBerry® Device Software version 4.0 or later for Java® based BlackBerry devices, it creates the index files automatically. If you change an .alx file for an application that already appears in a software index on your organization's network drive, you must update the software index.

1. At the command prompt, navigate to *<drive>*:\Program Files\Common Files\Research In Motion\Apploader.
2. Perform one of the following actions:
   - To create a software index, type **loader.exe /index**.
   - To update a software index, type **loader.exe /reindex**.

The application loader tool creates or updates the software index structure on the network drive, and it adds any missing index files.

Share a network drive for applications

You share a network drive for applications to make the applications available for users to install on their BlackBerry® devices.

1. Share *<drive>*:\Program Files\Common Files\Research In Motion\Shared\Applications.
2. Set the permission attributes to **Read-only**.

Defining software configurations

Software configurations permit you to perform the following actions to manage applications on BlackBerry® devices for specific user accounts or groups:

- remotely add and remove third-party Java® applications, the collaboration client, and the BlackBerry® MDS Runtime using the application loader tool on BlackBerry devices that are connected to computers that run the BlackBerry® Device Manager
- define application control policies and add them to software configurations to specify the resources that third-party Java applications, the collaboration client, and the BlackBerry MDS Runtime can access on BlackBerry devices from behind the organization's firewall

You must create a separate software configuration for each BlackBerry device series in your organization.

You must either install all of the application files that you want to install on a specific BlackBerry device model on the BlackBerry® Enterprise Server or on a computer with a shared network drive before you can set an application control policy on a BlackBerry device. You set up a software configuration to point to the location of the application files.

Create a software configuration

If you have more than one BlackBerry® device series in your organization, you must create a different software configuration for each series.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Software Configurations** tab, click **Add New Configuration**.
3. Type a configuration name and description in the appropriate fields.
4. Click **Change**.
5. Type the location of the BlackBerry® Device Software or applications.
6. Click **OK**.
7. In the **Application Name** list, select the check box beside the BlackBerry device series that you want to configure the BlackBerry Device Software or applications for.
8. Perform one of the following actions:
   - To permit users to add applications to BlackBerry devices, select the check box beside the application name.
   - To prevent users from adding the application to BlackBerry devices, clear the check box beside the application name.
9. Click **OK**.

After you finish: Define an application control policy.

Define an application control policy

For more information about defining application control policy rules, see the *Policy Reference Guide*.

Before you begin: Create a software configuration.

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Software Configurations** tab, click **Manage Application Policies**.
3. Click **New**.
4. Type a new policy name.
5. Customize the application control policy rules.
6. Click **OK**.

After you finish: Assign an application control policy to an application in a software configuration.

Assign an application control policy to an application

Before you begin: To assign an application control policy other than the default application control policy settings, you must first define an application control policy.

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Software Configurations** tab, in the **Configuration Name** list, click a software configuration.
3. Click **Edit Configuration**.
4. Expand the **Application Software** application tree.
5. In the **Policy** drop-down list, click an option to assign an application control policy to the application:

Option	Description
Assign the default application control policy.	To assign the application control policy that is assigned at the application software level, click **<default>**.
Assign an application control policy that you have defined.	To assign an application control policy that you have defined to all applications that are not currently assigned to an application control policy, click that application control policy.
Allow the user to set application controls on the BlackBerry device.	To allow the application control settings that are configured on the BlackBerry device, click **<none>**.

6. Click **OK**.

After you finish: Assign the software configuration to a user group or user account.

Assign a software configuration to a user group

1. In the BlackBerry® Manager, in the left pane, click a user group.
2. On the **Group Configuration** tab, click **Device Management**.
3. Click **Assign Software Configuration**.
4. Click the software configuration that you want to assign.
5. Click **OK**.

Assign a software configuration to a user account

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click the user account that you want to assign the software configuration to.
3. Click **Device Management**.
4. Click **Assign Software Configuration**.
5. Click the software configuration that you want to assign.
6. Click **OK**.

Send an application to a BlackBerry device over the wireless network

You can send a BlackBerry® Java Application, the collaboration client, and the BlackBerry® MDS Runtime over the wireless network to supported BlackBerry devices that have 16 MB or more of flash memory. In the next configured application polling interval, the BlackBerry® Enterprise Server searches for BlackBerry devices that do not have all required applications installed, and sends the applications. The default polling interval is 4 hours.

Before you begin: To send an application over the wireless network, your organization's IT policy must permit third-party applications on BlackBerry devices.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Software Configurations** tab, click a software configuration.
3. Click **Edit Configuration**.
4. Click the application that you want to send over the wireless network.
5. In the **Delivery** drop-down list, click **Wireless**.
6. To make sure that the application remains installed on a BlackBerry device, change the **Disposition** application control policy to **Required**.
7. Click **OK**.

Monitor wireless application push failures

You can retrieve information from the BlackBerry® Configuration Database to identify any issues with the wireless delivery of applications to BlackBerry devices.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. Click the **Software Config Status** tab.
3. In the **Name** field, type the name of the user whose BlackBerry device you want to monitor. If you leave the **Name** field empty, the search applies to all users in the BlackBerry Domain.
4. In the **Status** field, click the status that you want to monitor.
5. To change the information that displays for each database entry, right-click a column heading. Select the columns that you want to display.
6. In the **Entries per page** field, type the maximum number of database entries to display.
7. Click **Search**.

Error messages: Wireless application push

To troubleshoot push failures for wireless applications, collect 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 device information

If the preceding information does not address the issue, you might also require the following information:
- BlackBerry Policy Service log files from the day the issue was reported (log level 6 recommended)
- event log of the BlackBerry device from the day the issue was reported
- system event logs and application event logs
- software configuration files created on the network drive that the BlackBerry device is associated with
- copy of the BlackBerry Configuration Database
- SQL trace of the BlackBerry Policy Service communicating with the BlackBerry Configuration Database

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

Device timed out waiting for module

This message appears when a BlackBerry device reports a timeout failure while waiting for the application modules.

Resend the application to the BlackBerry device. If the second wireless application push is not successful, in the log files that you collected, locate the user account that is experiencing the issue. Trace the installation activity.

Device reported insufficient memory to install module

This message appears when a BlackBerry device does not have enough flash memory available to install the application modules.

Instruct the user to make more flash memory available on the BlackBerry device. Resend the application.

Device reported that there was an Incomplete Module

This message appears when an application module is not installed successfully on a BlackBerry device.

Resend the application. If the second wireless application push is not successful, in the log files that you collected, locate the user account that is experiencing the issue. Trace the installation activity.

Device reported that the Module Save Failed

This message appears when a BlackBerry device cannot save an application module.

Resend the application. If the second wireless application push is not successful, in the log files that you collected, locate the user account that is experiencing the issue. Trace the installation activity.

Device reported a general failure installing the module

This message appears when an application does not install successfully on a BlackBerry device.

Verify that the BlackBerry device has enough memory available to install the application. Resend the application.

Incomplete ACK data for APPD request

This message appears when the BlackBerry Policy Service does not receive an acknowledgment message that a BlackBerry device has received application data.

Verify that the BlackBerry device is turned on and is located in a wireless coverage area. Resend the application.

Device reported a %s error while installing module

This message appears when an error occurs in the BlackBerry Policy Service that prevents the application from installing successfully on a BlackBerry device.

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

Device reported Data Format Error in packet while installing module

This message appears when an error occurs in the BlackBerry Policy Service that prevents the application from installing successfully on a BlackBerry device.

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

Device reported Invalid Command while installing module

This message appears when an error occurs in the BlackBerry Policy Service that prevents the application from installing successfully on a BlackBerry device.

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

Device Reported Insufficient Body Data while installing module

This message appears when an error occurs in the BlackBerry Policy Service that prevents the application from installing successfully on a BlackBerry device.

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

Device reported Invalid Module Hash while installing module

This message appears when an error occurs in the BlackBerry Policy Service that prevents the application from installing successfully on a BlackBerry device.

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

Device reported Invalid App Data Length while installing module

This message appears when an error occurs in the BlackBerry Policy Service that prevents the application from installing successfully on a BlackBerry device.

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

Device reported Insufficient App Data while installing module

This message appears when an error occurs in the BlackBerry Policy Service that prevents the application from installing successfully on a BlackBerry device.

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

Related topics

Log files for the BlackBerry Enterprise Server components, 154
Change the logging level for a BlackBerry Enterprise Server component, 156

Install the BlackBerry Device Software or BlackBerry Applications on a BlackBerry device using the BlackBerry Manager

If you want to save network bandwidth, or if you want to install the BlackBerry® Device Software or add applications to BlackBerry devices before you distribute the BlackBerry devices to users, you can use the BlackBerry Manager to complete the installation process.

1. Connect the BlackBerry device to the computer that hosts the BlackBerry Manager.
2. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
3. On the **Software Configurations** tab, click a software configuration.
4. Click **Edit Configuration**.
5. Click the software or application that you want to install on the BlackBerry device.
6. In the **Delivery** drop-down list, click **Wireline only**.
7. To make sure that the application remains installed on a BlackBerry device, change the **Disposition** application control policy to **Required**.
8. Click **OK**.

Installing the collaboration client on BlackBerry devices

You can use one of the following methods to install the collaboration client on users' BlackBerry® devices.

Method	Resource
over the wireless network using the BlackBerry® Enterprise Server	See the "Making BlackBerry Device Software and Java applications available to users" section of the *BlackBerry Enterprise Server Administration Guide*. You must verify that your organization's IT policy permits third-party applications on BlackBerry devices. For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.
using the BlackBerry® Desktop Software or the BlackBerry® Web Desktop Manager	To read the *Deploying Java Applications* document, visit www.blackberry.com/developers and click the White Papers link.
using the BlackBerry Application Web Loader	To read the *Deploying Java Applications* document, visit www.blackberry.com/developers and click the White Papers link.
using the standalone application loader tool	To read the *Deploying Java Applications* document, visit www.blackberry.com/developers and click the White Papers link.

Method	Resource
using the BlackBerry® Browser	To read the *Deploying Java Applications* document, visit www.blackberry.com/developers and click the White Papers link.

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.

Setting up the messaging environment 7

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 users

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Global Filters**.
4. Double-click **Global Filter Definition**.
5. Click **New**.
6. In the **New Message Conditions** section, double-click **Filter Name**.
7. Type a name for the email message filter.
8. Configure the options for the email message filter.
9. Click **Action**.
10. Perform one of the following tasks:

Task	Steps
Create an email message filter that does not deliver messages that match the filter criteria.	In the drop-down list, click **Hold**.
Create an email message filter that forwards messages that match the filter criteria.	a. In the drop-down list, click **Forward**. b. Double-click **Forwarding Options**. c. Select the appropriate message forwarding options.

11. Click **OK**.
12. In the **Filter Name** list, click the email message filter that you created.
13. To move the email message filter higher or lower in the list, click **Move Up** or **Move Down**.
    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.
14. Click **OK**.

Turn on an email message filter that applies to all user accounts

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Global Filters**.
4. Double-click **Global Filter Definition**.
5. In the **Filter Name** list, click an email message filter.
6. Click **Properties**.
7. In the **New Message Conditions** section, in the **Enabled** drop-down list, click **True**.
8. Click **OK**.

The BlackBerry Enterprise Server applies email message filters in the order that they are listed in.

Create an email message filter that applies to a user group

1. In the BlackBerry® Manager, in the left pane, click a user group.
2. On the **Group Configuration** tab, click **Edit Group Template**.
3. In the left pane, click **Filters**.
4. Double-click **Filter Rules**.
5. Click **New**.
6. In the **New Message Conditions** section, double-click **Filter Name**.
7. Type a name for the email message filter.

8. Configure the options for the email message filter.
9. Click **Action**.
10. Perform one of the following tasks:

Task	Steps
Create an email message filter that does not deliver messages that match the filter criteria.	In the drop-down list, click **Hold**.
Create an email message filter that forwards messages that match the filter criteria.	a. In the drop-down list, click **Forward**. b. Double-click **Forwarding Options**. c. Select the appropriate message forwarding options.

11. Click **OK**.
12. In the **Filter Name** list, click the email message filter that you created.
13. To move the email message filter higher or lower in the list, click **Move Up** or **Move Down**.
    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.
14. Click **OK**.
15. Select the **Filter Rules** check box.
16. Click **Reapply Template**.

Turn on an email message filter that applies to a user group

1. In the BlackBerry® Manager, in the left pane, click a user group.
2. On the **Group Configuration** tab, click **Edit Group Template**.
3. In the left pane, click **Filters**.
4. Double-click **Filter Rules**.
5. In the **Filter Name** list, click an email message filter.
6. Click **Properties**.
7. In the **New Message Conditions** section, in the **Enabled** drop-down list, click **True**.
8. Click **OK**.
9. Select the **Filter Rules** check box.
10. Click **Reapply Template**.

The BlackBerry® Enterprise Server 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® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, double-click a user account.
3. In the left pane, click **Filters**.
4. Double-click **Filter Rules**.
5. Click **New**.
6. In the **New Message Conditions** section, double-click **Filter Name**.
7. Type a name for the new email message filter.
8. Configure the options for the email message filter.
9. Click **Action**.
10. Perform one of the following tasks:

Task	Steps
Create an email message filter that does not deliver messages that match the filter criteria.	In the drop-down list, click **Hold**.
Create an email message filter that forwards messages that match the filter criteria.	a. In the drop-down list, click **Forward**. b. Double-click **Forwarding Options**. c. Select the appropriate message forwarding options.

11. Click **OK**.
12. In the **Filter Name** list, click the email message filter that you created.
13. Click **Move Up** or **Move Down** to move the filter higher or lower in the list.

    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.
14. Click **OK**.

Turn on an email message filter that applies to a specific user account

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, double-click a user account.
3. In the left pane, click **Filters**.
4. Double-click **Filter Rules**.
5. In the **Filter Name** list, click an email message filter.
6. Click **Properties**.

7. In the **New Message Conditions** section, in the **Enabled** drop-down list, click **True**.
8. Click **OK**.

The BlackBerry Enterprise Server applies email message filters in the order that they are listed in.

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 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 secure messaging package on the BlackBerry device, the user cannot send the email message.

Configure message classifications

Create a message classification

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. In the list of IT policies, select an IT policy.
6. Click **Properties**.
7. Click **OK**.
8. Click **Security Policy Group**.
9. Double-click the **Message Classification** IT policy rule.
10. Click **New**.

11. Type a display name to appear in the Classifications list on the BlackBerry device.
12. Type a subject suffix to append, in parentheses, to the message subject. For example, type the subject suffix (U) for a classification that is named Unclassified.
13. In the drop-down list, click a minimum action for encoding the message. For example, click **Signed** to permit the user to select all encoding types for the secure messaging packages that are installed on the BlackBerry device.
14. Click **Apply**.
15. Click **OK**.

After you finish: If you create more than one message classification, order the 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.

Create a message classification based on an existing classification

Before you begin: Create a message classification.

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. In the list of IT policies, select an IT policy.
6. Click **Properties**.
7. Click **Security Policy Group**.
8. Double-click the Message Classification IT policy rule.
9. Click a display name.
10. Click **New Copy**.
11. Type a new display name.
12. Type a new subject suffix.
13. In the drop-down list, click a minimum action for encoding the message.
14. Click **Apply**.
15. Click **OK**.

Order message classifications

Before you begin: Create message classifications.

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.

2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. In the list of IT policies, select an IT policy.
6. Click **Properties**.
7. Click **Security Policy Group**.
8. Double-click the Message Classification IT policy rule.
9. Click a display name.
10. Perform any of the following actions:
    - To move the selected classification to the top of the list, click **Make First**.
    - To move the selected classification one position higher in the list, click **Move Up**.
    - To move the selected classification one position lower in the list, click **Move Down**.
    - To move the selected classification to the bottom of the list, click **Make Last**.
11. Click **Apply**.

Delete message classifications

Before you begin: Create a message classification.

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. In the list of IT policies, select an IT policy.
6. Click **Properties**.
7. Click **Security Policy Group**.
8. Double-click the Message Classification IT policy rule.
9. Click a display name.
10. Click **Remove**.
11. Click **Apply**.

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 lists on the BlackBerry® devices. The information in the fields synchronize to BlackBerry devices and you can display them in contact lookups. 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 custom 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 an address book field in the email application to an address book field on all BlackBerry devices

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Service Control & Customization**.
3. Click **Edit PIM Sync Global Field Mapping**.
4. In the **Desktop Field** column, click a field.
5. In the **Device Field** column, in the drop-down list, click the address book field for the BlackBerry device that you want to map to the field in the email application.
6. Click **OK**.

Map an address book field in the email application to an address book field on a specific BlackBerry device

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. In the lower pane, click **Service Control & Customization**.
4. Click **Edit PIM Sync Field Mapping**.
5. In the **Desktop Field** column, click a field.
6. In the **Device Field** column, in the drop-down list, click the address book field for the BlackBerry device that you want to map to the field in the email application.
7. Click **OK**.

Map address book fields that users defined to address book fields on all BlackBerry devices

You can map up to four address book fields that users define in the email application to BlackBerry® devices.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Service Control & Customization**.
3. Click **Edit PIM Sync Global Field Mapping**.
4. In the **Desktop Field** column, click **User Defined String 1**.
5. In the **Device Field** column, in the drop-down list, click the address book field for the BlackBerry device that you want to map to the address book field in the email application.
6. Click **OK**.

Map address book fields that users defined to address book fields on a specific BlackBerry device

You can map up to four address book fields that users define in the email application to a specific BlackBerry® device.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. In the lower pane, click **Service Control & Customization**.
4. Click **Edit PIM Sync Field Mapping**.
5. In the **Desktop Field** column, click **User Defined String 1**.
6. In the **Device Field** column, in the drop-down list, click the address book field for the BlackBerry device that you want to map to the address book field in the email application.
7. Click **OK**.

Making BlackBerry MDS Runtime Applications available to users 8

Creating BlackBerry MDS Runtime Applications and sending them to BlackBerry devices

To see the documentation for administrators of the BlackBerry® Enterprise Server, visit www.blackberry.com/go/serverdocs. To see the *BlackBerry Mobile Data System Technical Overview* and documentation for BlackBerry developer tools, visit www.blackberry.com/developers.

Task	Actor	Resource
Install the BlackBerry Enterprise Server with the BlackBerry MDS Integration Service.	Administrator	*BlackBerry Enterprise Server Installation Guide*
Authenticate the BlackBerry MDS Integration Service to the BlackBerry Manager.	Administrator	*BlackBerry Enterprise Server Administration Guide* • Section: Setting up security options
Download the BlackBerry® MDS Runtime.	Administrator	na.blackberry.com/eng/services/mobile_upgrade.jsp
Install the BlackBerry MDS Runtime on a network drive.	Administrator	*BlackBerry Enterprise Server Administration Guide* • Section: Sending software and Java applications to BlackBerry devices
Send the BlackBerry MDS Runtime to BlackBerry devices.	Administrator	*BlackBerry Enterprise Server Administration Guide* • Section: Sending software and Java applications to BlackBerry devices *BlackBerry MDS Runtime Deployment Guide*

Task	Actor	Resource
Install the BlackBerry® MDS Studio or the BlackBerry® Plug-in for Microsoft® Visual Studio®.	Developer	*BlackBerry MDS Studio Developer Guide* • Section: Installing, configuring, and removing the BlackBerry MDS Studio *BlackBerry Plug-in for Microsoft Visual Studio Release Notes and Known Issues List*
Create a BlackBerry MDS Runtime Application.	Developer	*BlackBerry MDS Studio Getting Started Guide* *BlackBerry MDS Studio Developer Guide* *BlackBerry MDS Studio Fundamentals Guide* *BlackBerry Plug-in for Microsoft Visual Studio Developer Guide* BlackBerry Plug-in for Microsoft Visual Studio online help
Publish a BlackBerry MDS Runtime Application to the BlackBerry MDS Application Repository.	Developer	*BlackBerry MDS Studio Developer Guide* • Section: Publishing BlackBerry MDS Studio applications on BlackBerry devices *BlackBerry MDS Studio Fundamentals Guide* • Section: Deployment cycle for BlackBerry Applications *BlackBerry Plug-in for Microsoft Visual Studio Developer Guide* • Section: Publish the BlackBerry application

Task	Actor	Resource
Establish client authentication between the BlackBerry MDS Integration Service and web services.	Administrator	*BlackBerry Enterprise Server Administration Guide* • Section: Setting up security options
Configure authentication for BlackBerry MDS Runtime Applications.	Administrator	*BlackBerry Enterprise Server Administration Guide* • Section: Making BlackBerry MDS Runtime Applications available to users • Topic: Configuring access to web services and managing signed and unsigned applications
Assign a BlackBerry MDS Integration Service device policy to BlackBerry devices.	Administrator	*BlackBerry Enterprise Server Administration Guide* • Section: Making BlackBerry MDS Runtime Applications available to users • Topic: Configuring how users access and use BlackBerry MDS Runtime Applications
Install BlackBerry MDS Runtime Applications on BlackBerry devices.	Administrator	*BlackBerry Enterprise Server Administration Guide* • Section: Making BlackBerry MDS Runtime Applications available to users

Preparing BlackBerry devices to install BlackBerry MDS Runtime Applications

BlackBerry® MDS Runtime Applications can only be installed and used on BlackBerry devices that have the BlackBerry® MDS Runtime installed and activated. You can install the BlackBerry MDS Runtime on BlackBerry devices over the wireless network, or you can add it to a network drive and instruct users to install it on their BlackBerry devices using the application loader tool in the BlackBerry® Desktop Manager.

To download the latest version of the BlackBerry MDS Runtime, visit na.blackberry.com/eng/services/mobile_upgrade.jsp. For more information about installing and activating the BlackBerry MDS Runtime on BlackBerry devices, visit www.blackberry.com/developers.

Related topics
Sending software and BlackBerry Java Applications to BlackBerry devices, 29

Configuring access to web services and managing signed and unsigned applications

Allow BlackBerry MDS Runtime Applications to access web services using HTTPS

If you configured authentication between the BlackBerry® MDS Integration Service and web services, you must configure the BlackBerry MDS Integration Service to allow BlackBerry MDS Runtime Applications to establish HTTPS connections to external web services.

Before you begin: Configure the BlackBerry MDS Integration Service to authenticate to web services.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Integration Service.
2. On the **MDS Integration Services** tab, click **Edit Properties**.
3. In the left pane, click **General**.
4. Click **Allow Web Services Access over SSL**.
5. In the drop-down list, click **True**.
6. Click **OK**.
7. On the **MDS Integration Services** tab, click **Common**.
8. Click **Stop Service**.
9. When the status displays "Stopped," click **Start Service**.

Related topics
Authenticating the BlackBerry MDS Integration Service to the BlackBerry Manager and web services, 20

Define a BlackBerry MDS Runtime Application as a trusted application

A developer in your organization can sign a BlackBerry® MDS Runtime Application with a digital certificate. Add this digital certificate to the BlackBerry MDS Integration Service to define the BlackBerry MDS Runtime Application as a trusted application that can send data to and receive data from application servers or web servers.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Integration Service.
2. On the **MDS Integration Services** tab, click **Common**.
3. Click **Add Certificate**.
4. In the **Alias** field, type a name for the certificate.

5. In the **Certificate file** field, click **Browse**. Click the certificate that you want to add.
6. Click **OK**.

Configure whether users can install unsigned BlackBerry MDS Runtime Applications on BlackBerry devices

You can configure whether users are allowed to install BlackBerry® MDS Runtime Applications that are not signed with a digital certificate. By default, users are allowed to install unsigned BlackBerry MDS Runtime Applications on their BlackBerry devices.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Integration Service.
2. On the **MDS Integration Services** tab, click **Edit Properties**.
3. In the left pane, click **General**.
4. Click **Allow Unsigned Applications**.
5. In the drop-down list, perform one of the following actions:
   - To allow users to install unsigned BlackBerry MDS Runtime Applications, click **True**.
   - To prevent users from installing unsigned BlackBerry MDS Runtime Applications, click **False**.
6. Click **OK**.
7. On the **MDS Integration Services** tab, expand **Common**.
8. Click **Stop Service**.
9. When the status displays "Stopped," click **Start Service**.

Configuring how users access and use BlackBerry MDS Runtime Applications

You can create BlackBerry® MDS Integration Service device policies and assign them to users and user groups to control how users access and use BlackBerry® MDS Runtime Applications on their BlackBerry devices. Device policies define whether users can upgrade the BlackBerry MDS Runtime, and whether users can discover, install, and remove BlackBerry MDS Runtime Applications from their BlackBerry devices. You can also use device policies to define whether BlackBerry MDS Runtime Applications can access data and other applications on the BlackBerry devices, and to specify message queue limits for data that BlackBerry MDS Runtime Applications send and receive.

Create a BlackBerry MDS Integration Service device policy

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Integration Service.
2. On the **MDS Integration Services** tab, click **Edit Properties**.
3. Click **Device Policies**.
4. Double-click **BlackBerry MDS Integration Service Device Policy Definition**.
5. Click **New**.

6. Click **Device Policy**.
7. Double-click **Policy Name**.
8. Type a name for the device policy.
9. Specify the device policy rule settings.
   For more information about the device policy settings, see the *Policy Reference Guide*.
10. Click **OK**.

After you finish: Assign the device policy that you created to a user or user group.

Assign a BlackBerry MDS Integration Service device policy to a user group

Before you begin: Make sure that all of the users in the group are connected to the same BlackBerry® MDS Integration Service. The group must contain at least one user.

1. In the BlackBerry Manager, in the left pane, click a user group.
2. On the **Group Configuration** tab, click **MDS Integration Service**.
3. Click **Assign Device Policy**.
4. In the **Device Policy** drop-down list, click the device policy that you want to assign to the user group.
5. Click **OK**.

Assign a BlackBerry MDS Integration Service device policy to a specific user

1. In the BlackBerry® Manager, in the left pane, expand a BlackBerry MDS Integration Service.
2. Click **Devices Registered**.
3. On the **Devices Registered** tab, click a user account.
4. In the lower pane, click **Common**.
5. Click **Assign Device Policy**.
6. In the **Device Policy** drop-down list, click the device policy that you want to assign to the user.
7. Click **OK**.

Sending BlackBerry MDS Runtime Applications and BlackBerry Browser Applications to BlackBerry devices

You can send BlackBerry® MDS Runtime Applications and BlackBerry® Browser Applications to BlackBerry devices over the wireless network. Users can use the BlackBerry MDS Control Center on their BlackBerry devices to search the BlackBerry MDS Application Repository for available BlackBerry MDS Runtime Applications, and install the applications on their BlackBerry devices. Users cannot search for or install BlackBerry Browser Applications using the BlackBerry MDS Control Center.

Users can use the BlackBerry MDS Control Center after the BlackBerry® MDS Runtime is installed and activated on their BlackBerry devices.

Install a BlackBerry MDS Runtime Application on BlackBerry devices

1. In the BlackBerry® Manager, in the left pane, click a user group.
2. On the **View** menu, click **Choose Columns**. Add the **MDS Integration Service Server URL** column.
3. Click the **MDS Integration Service Server URL** column heading.
4. Click the user accounts that are connected to the same BlackBerry MDS Integration Service server.
5. On the **Group Configuration** tab, click **MDS Services**.
6. Click **Install on Device**.
7. Click the BlackBerry MDS Runtime Application that you want to install.
8. Click **Next**.
9. In the **Group size for pushing** field, type the number of BlackBerry devices to send the installation request to at the same time.
10. In the **Push interval** field, type an interval for the BlackBerry MDS Integration Service to send the installation request to BlackBerry devices.
11. To set a specific time to send the installation request at, click the **Schedule** check box. Specify the start date and time.
12. To display a prompt on BlackBerry devices that allows users to cancel the installation, clear the **Required** check box.
13. Click **Next**.
14. Click **Finish**.

Install a BlackBerry MDS Runtime Application on a specific BlackBerry device

Before you begin: Obtain the PIN of the BlackBerry® device.

1. In the BlackBerry Manager, in the left pane, expand a BlackBerry MDS Integration Service.
2. Click **Application Registry**.

3. Click the BlackBerry MDS Runtime Application that you want to install.
4. In the lower pane, click **Device Management**.
5. Click **Install on Device**.
6. In the **Install application on devices** drop-down list, click **without application installed**.
7. Clear the **Select all** check box.
8. Click the PIN of the BlackBerry device that you want to install the application on.
9. Click **Next**.
10. To set a specific time at which to send the installation request, click the **Schedule** check box. Specify the start date and time.
11. To display a prompt on the BlackBerry device that allows the user to cancel the installation, clear the **Required** check box.
12. Click **Next**.
13. Click **Finish**.

Applying an application control policy to a BlackBerry MDS Runtime Application

In BlackBerry® Enterprise Server version 4.1 SP5 and later, you can apply an application control policy to a BlackBerry® MDS Runtime Application that was created using BlackBerry® MDS Studio version 2.0 or later or the BlackBerry® Plug-in for Microsoft® Visual Studio® version 1.1 or later. You can use an application control policy to specify the types of data on BlackBerry devices that the BlackBerry MDS Runtime Application can and cannot access. For example, you can apply an application control policy that restricts a BlackBerry MDS Runtime Application from accessing the organizer data on BlackBerry devices.

To apply an application control policy to a BlackBerry MDS Runtime Application, you must add an application launcher file (.cod) for the BlackBerry MDS Runtime Application to a software configuration. You must then apply an application control policy to the application launcher file. When you assign the software configuration to users, the application launcher file installs on BlackBerry devices and enforces the application control policy for the BlackBerry MDS Runtime Application. Only BlackBerry devices that are running BlackBerry® MDS Runtime version 4.5 or later can use the application launcher file.

Add the application launcher file for a BlackBerry MDS Runtime Application to the network drive

Before you begin: Get the application launcher (.cod) file for the BlackBerry® MDS Runtime Application from the application developer.

1. If necessary, on the network drive, create the path *<drive>*:\Program Files\Common Files\Research In Motion\Shared \Applications.
2. In the **Applications** folder, create a folder for the BlackBerry MDS Runtime Application.
3. Copy the application launcher file to the folder that you created.

4. In the folder, create a .txt file.
5. Rename the .txt file to <*application_name*>.alx.
6. In a text editor, open the .alx file.
7. Copy the following text into the .alx file. For the variables, use information that the application developer provides.

```
<loader version="1.0">
<application id="application_launcher_id">
<name>application_launcher_name</name>
<description>application_launcher_description</description>
<version>application_launcher_version</version>
<vendor>vendor</vendor>
<copyright>copyright_information</copyright>
<directory SystemSize="normal"></directory>
<fileset Java="1.0" Color="true">
<files>name_of_.cod_application_launcher</files>
</fileset>
</application>
</loader>
```

8. Save and close the .alx file.

After you finish: Re-index the applications that are located at <*drive*>:\Program Files\Common Files\Research In Motion \Shared\Applications. Share the network drive.

Related topics
Indexing applications on a network drive, 31

Assign an application control policy to a BlackBerry MDS Runtime Application

Before you begin: Add the application launcher (.cod) file for the BlackBerry® MDS Runtime Application to the network drive.

1. In the BlackBerry Manager, create a software configuration that includes the application launcher file for the BlackBerry MDS Runtime Application.
2. Apply an application control policy to the application launcher file.
3. Assign the software configuration to a user account or user group that has the BlackBerry MDS Runtime Application installed on the users' BlackBerry devices.

Related topics
Defining software configurations, 31

Configuring how users access enterprise applications and web content 9

Specifying a BlackBerry MDS Connection Service as the central push server

You can specify one BlackBerry® MDS Connection Service in a BlackBerry Domain as the central push server. The central push server receives content push requests from server-side applications that are located on an application server, on a web server, or in a database. It also manages push requests and sends application data and application updates to BlackBerry Applications on BlackBerry devices.

Specify the central push server

Only one BlackBerry® MDS Connection Service in your organization's BlackBerry Domain can be specified as the central push server. When you specify a BlackBerry MDS Connection Service as the central push server, any other BlackBerry MDS Connection Service specified as the central push server in your organization's BlackBerry Domain has the designation removed.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Common**.
3. Click **Set as Push Server**.

After you finish:

- If you have the BlackBerry MDS Integration Service installed, verify that the central push server appears in the list of BlackBerry MDS Connection Service instances that are available to the BlackBerry MDS Integration Service. You can configure multiple instances of the BlackBerry® Enterprise Server in your organization's BlackBerry Domain to use the BlackBerry MDS Connection Service that you defined as the central push server.
- Notify the push application developers in your organization's environment that you have designated a new central push server.

Related topics

Make a BlackBerry MDS Connection Service available to a BlackBerry MDS Integration Service, 133
Configure multiple BlackBerry Enterprise Server instances to use the same BlackBerry MDS Connection Service, 25

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

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 do not configure an authentication method for BlackBerry MDS Connection Service connections, users are prompted to provide login information on their authenticated BlackBerry devices every 30 minutes. The BlackBerry device prompts users only if the connection to the content server persists for more than 30 minutes.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. In the left pane, click **HTTP**.
4. Click **Support HTTP Authentication**.
5. In the drop-down list, perform one of the following actions:
   - If you want BlackBerry devices to authenticate to content servers directly, click **False**.
   - If you want the BlackBerry MDS Connection Service to store authentication information and perform HTTP authentication on behalf of BlackBerry devices, click **True**.
6. Double-click **Authentication Timeout**.
7. 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.
8. Click **OK**.

After you finish: If you set **Support HTTP Authentication** to **True**, 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.

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 they store the HTTP cookies that they use to authenticate to content servers that use LTPA authentication technology. For BlackBerry devices that use previous versions of the BlackBerry Device Software, you must allow the BlackBerry MDS Connection Service to manage HTTP cookie storage on the BlackBerry devices.

Before you begin: Configure the BlackBerry MDS Connection Service to authenticate to the content servers in your environment on behalf of BlackBerry devices.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. In the left pane, click **HTTP**.
4. Click **Support HTTP Cookie Storage**.
5. In the drop-down list, click **True**.
6. Click **OK**.

Configure the BlackBerry MDS Connection Service to authenticate BlackBerry devices to the RSA Authentication Manager

When you turn on RSA® authentication, users must type their login information on their BlackBerry® devices before they can access intranet or Internet content. After a user is authenticated, if proxy authentication is configured, the BlackBerry device prompts the user to authenticate to the proxy server.

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 Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. In the left pane, click **RSA Authentication**.
4. Click **Enable RSA Authorization Support**.
5. In the drop-down list, click **True**.
6. To specify how long an authenticated BlackBerry device can remain connected to your organization's network while the user is active, double-click **RSA Authentication Timeout**. Type a number, in minutes.

   By default, the authenticated connection persists for 24 hours.
7. To specify how long a BlackBerry device can remain connected to your organization's network while the user is inactive, double-click **RSA Inactivity Timeout**. Type a number, in minutes.

   By default, an authenticated connection persists for 60 minutes of user inactivity on the BlackBerry device.
8. Click **OK**.

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. If the BlackBerry device requires JavaScript® support in its HTTP requests, the BlackBerry device processes cookies.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. In the left pane, click **HTTP**.
4. Click **Support HTTP Cookie Storage**.
5. In the drop-down list, click **True**.
6. Click **OK**.

After you finish: To prevent the BlackBerry MDS Connection Service from managing HTTP cookie storage, set the **Support HTTP Cookie Storage** drop-down list to **False**.

Configure the timeout limit for HTTP connections with BlackBerry devices

You can specify how long the BlackBerry® MDS Connection Service waits for a BlackBerry device to send data before it closes the HTTP connection to the BlackBerry device. The default timeout limit is 120,000 milliseconds (2 minutes).

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. In the left pane, click **HTTP**.
4. Double-click **HTTP Device Connection Timeout**.
5. Type a number, in milliseconds.
6. Click **OK**.

Configure the timeout limit for HTTP connections to web servers

You can specify how long the BlackBerry® MDS Connection Service waits for a web server to send data before it closes the HTTP connection to the web server. The default timeout limit is 120,000 milliseconds (2 minutes).

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. In the left pane, click **HTTP**.
4. Double-click **HTTP Server Connection Timeout**.
5. Type a number, in milliseconds.
6. Click **OK**.

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 five redirections.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. In the left pane, click **HTTP**.
4. Double-click **Maximum Number of Redirects**.
5. Type a number.
6. Click **OK**.

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.	a. Type **keytool -genkey -alias tomcat -keyalg RSA -keystore webserver.keystore**. b. Type the required information. c. To confirm the information that you typed, type **Yes**.
Add a publicly signed certificate to the key store.	a. Type **keytool -import -trustcacerts -alias tomcat -file *<trustedserver.cer>* -keystore webserver.keystore**. b. Type the key store password. c. 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.

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.

Related topics

Create a key store to store certificates for use with HTTPS connections, 63

Allow BlackBerry devices to connect to untrusted web servers

You can allow BlackBerry® devices to connect to untrusted web servers so that applications on those servers can push content to BlackBerry devices.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Click **TLS/HTTPS**.
4. Perform one of the following tasks:

Task	Steps
Allow outgoing requests from the BlackBerry device that the BlackBerry MDS Connection Service encrypts with HTTPS.	a. Click **Allow Untrusted HTTPS Connections**. b. In the drop-down list, click **True**.
Allow outgoing requests from the BlackBerry device that the BlackBerry MDS Connection Service encrypts with TLS.	a. Click **Allow Untrusted TLS Connections**. b. In the drop-down list, click **True**.

Configure the BlackBerry MDS Connection Service to retrieve certificates for web servers

You must define a user name and password for the BlackBerry® MDS Connection Service to authenticate with LDAP servers on behalf of BlackBerry devices.

Do not change the default LDAP port parameters unless there is a port conflict with another service on the same computer. If you change the port number or host server information, you must stop and restart the BlackBerry MDS Connection Service to reload this information.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Click **LDAP**.
4. Configure the LDAP server settings.
5. Click **OK**.

After you finish: Configure the BlackBerry MDS Connection Service to retrieve the status of certificates for web servers.

Configure the BlackBerry MDS Connection Service to retrieve the status of certificates for web servers

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Click **OCSP**.
4. Perform any of the following tasks:

Task	Steps
Configure the BlackBerry MDS Connection Service to accept OCSP servers (responders) that the BlackBerry device specifies.	a. Click **Use Device Responders**. b. In the drop-down list, click **True**.
Configure the OCSP handler to use the OCSP responder extension in a certificate.	a. If a certificate is present, click **Use Certificate Extension Responders**. b. In the drop-down list, click **True**.
Configure the default web address of the OCSP responder.	a. Double-click **Default Responder URL**. b. Type the web address of the OCSP responder.
Configure the web address of the server that the CRL is located on.	a. Double-click **Default CRL Server URL**. b. Type the web address of the CRL server.

5. Click **OK**.

After you finish: Install retrieved certificates for web servers.

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 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.

Configuring how the BlackBerry MDS Connection Service connects to BlackBerry devices

Specify the maximum amount of data that the BlackBerry MDS Connection Service can send to BlackBerry devices

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. In the left pane, click **General**.
4. Double-click **Maximum KB/Connection**.
5. Type a number, in KB.
6. Click **OK**.

Specify the pending content timeout limit for the BlackBerry MDS Connection Service

You can specify how long the BlackBerry® MDS Connection Service waits for acknowledgement from a BlackBerry device before it deletes pending content for that BlackBerry device.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. In the left pane, click **General**.

4. Double-click **Flow Control Timeout**.
5. Type a number, in milliseconds.
6. Click **OK**.

Allow Java applications to use persistent socket connections with the BlackBerry MDS Connection Service

Before you begin: Verify that your system memory supports persistent socket connections.

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. In the left pane, click **General**.
4. Click **Use Persistent Socket**.
5. In the drop-down list, click **True**.
6. Click **OK**.

Specify the thread pool size of the BlackBerry MDS Connection Service

You can specify the maximum number of threads that the BlackBerry® MDS Connection Service can process simultaneously.

Before you begin: Verify that your system memory can support the thread pool size that you want to specify.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Click **General**.
4. Double-click **Thread Pool Size**.
5. Type a number between 100 and 1000.
6. Click **OK**.

Specify the maximum number of persistent socket connections

You can specify the maximum number of persistent socket connections that can be open simultaneously between BlackBerry® devices and the BlackBerry MDS Connection Service.

Before you begin: Verify that your system memory can support the number of persistent socket connections that you want to specify.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.

3. Click **General**.
4. Double-click **Maximum Simultaneous Persistent Sockets**.
5. Type a number between 100 and 3500.
6. Click **OK**.

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. Change the default port parameters only if a port conflict exists with another service on the same computer.

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Click **General**.
4. Perform one of the following actions:
   - To specify the port for HTTP requests, double-click **Web Server Listen Port**. Type the port number.
   - To specify the port for HTTPS requests, double-click **Web Server SSL Listen Port**. Type the port number.
5. Click **OK**.

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.

Specify how often the BlackBerry MDS Connection Service polls for configuration information

You can specify how often the BlackBerry® MDS Connection Service polls the BlackBerry Configuration Database for changes to the BlackBerry MDS Connection Service and BlackBerry Collaboration Service administrative settings. The default interval is 5 minutes.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Click **General**.
4. Double-click **Admin Configuration Cycle Timer**.
5. Type a number, in minutes.
6. Click **OK**.

Assigning BlackBerry devices to users

10

Preparing to distribute BlackBerry devices

Before you assign BlackBerry® devices to users, you can configure the BlackBerry® Enterprise Server to add messages that users previously sent and received on supported BlackBerry devices. You can add messages for new users and for users whose PINs change when they receive replacement BlackBerry devices.

When the BlackBerry Enterprise Server adds messages to a BlackBerry device, the BlackBerry Enterprise Server applies the message filter rules and redirection settings for the user account.

Change how the BlackBerry Enterprise Server loads users' existing messages onto BlackBerry devices

By default, the BlackBerry® Enterprise Server loads the headers of 200 messages from the previous 5 days onto a user's BlackBerry device when it is activated. If you change the BlackBerry Enterprise Server settings to load the headers and body of messages onto a user's BlackBerry device when it is activated, the BlackBerry Enterprise Server can load up to 750 messages from the last 14 days for each user.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. Click **Messaging**.
4. To load the body and headers of messages onto BlackBerry devices, in the **Send Headers Only** drop-down list, click **False**.
5. To specify the number of previous days that you want to load messages for, in the **Prepopulation By Message Age** field, type a number.
6. To specify the maximum number of messages to load, in the **Prepopulation By Message Count** field, type a number.
7. Click **OK**.

Prevent the BlackBerry Enterprise Server from loading legacy messages onto new BlackBerry devices

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Messaging**.
4. In the **Message Prepopulation** section, perform the following actions:
   - In the **Prepopulation By Message Age** field, type **0**.

- In the **Prepopulation By Message Count** field, type **0**.

Assigning BlackBerry devices to user accounts

When you assign a BlackBerry® device to a user account, you associate the BlackBerry device with that user's email account. To assign BlackBerry devices to user accounts and activate the BlackBerry devices, you can use any of the following methods:

Method	Description
using the BlackBerry Manager	You can activate BlackBerry devices before distributing them to users by connecting the BlackBerry devices to the computer that hosts the BlackBerry Manager.
over the wireless network	New BlackBerry device users and users receiving replacement BlackBerry devices can activate their BlackBerry devices without requiring a physical connection to your organization's network.
over the LAN	New BlackBerry device users and users receiving replacement BlackBerry devices can activate their BlackBerry devices by connecting the BlackBerry devices to a computer that has the BlackBerry® Desktop Manager installed.

If you added a user account that was 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 that user account using the BlackBerry Manager.

Option 1: Activate a BlackBerry device using the BlackBerry Manager

1. Connect the BlackBerry® device to the computer that hosts the BlackBerry Manager.
2. In the BlackBerry Manager, in the left pane, click a BlackBerry® Enterprise Server.
3. On the **Users** tab, click the user account that you want to assign to the BlackBerry device.
4. Click **Device Management**.
5. Click **Assign Handheld**.
6. Click the BlackBerry device that you want to assign to the user account.
7. Click **OK**.

Option 2: Activating BlackBerry devices over the wireless network

To activate BlackBerry® devices over the wireless network, you assign activation passwords to user accounts. Users receive their activation passwords in email messages and associate their BlackBerry devices with their email accounts by typing the passwords on their BlackBerry devices.

Save bandwidth by synchronizing organizer data over the LAN

When BlackBerry® devices are activated over the wireless network, by default, the BlackBerry® Enterprise Server synchronizes the initial load of organizer data over the wireless network. To save bandwidth, you can set an IT policy to synchronize the initial load of organizer data through the BlackBerry Router and over your organization's LAN when users connect their BlackBerry devices to a computer that the BlackBerry® Device Manager is installed on.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. In the list of policies, click **Default**.
6. Click **Properties**.
7. Click **PIM Sync Policy Group**.
8. Click the Disable Wireless Bulk Loads IT policy rule.
9. In the drop-down list, click **True**.
10. Click **OK**.
11. Instruct users to connect their BlackBerry devices to their computers and start the BlackBerry Device Manager.

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 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 console to configure the 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.

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 BlackBerry device user account.

Item	Description
length of 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 console: 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 except accented characters.
security	The wireless activation authentication protocol is designed so that short activation passwords do not compromise the security of the protocol. You must distribute the activation password securely to the authenticated user. If the user received the activation password, but does not activate the BlackBerry device on the BlackBerry Enterprise Server, a user with malicious intent 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 user with malicious intent 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 by default after 48 hours. You can set an activation 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 a 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 character length of the activation password and the type of activation password that you send to users in a BlackBerry® Domain. For example, for the BlackBerry® 7100 Series, you can assign the 7100 Friendly password type to require users to press only one key at a time.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **General**.
4. To change the activation password length, double-click **Auto-generated password length**. Type a character length.
5. To change the activation password type, in the **Auto-generated password type** drop-down list, click a password type.
6. Click **OK**.

Customize the activation message

To provide troubleshooting information or to make sure that the activation message conforms to your organization's messaging policies, you can customize the default activation message that users receive in the email applications on their computers.

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **General**.
4. In the **Administration** section, double-click **Custom Activation Email Message**.
5. Type the parameters, subject, and message.
6. Click **OK**.

Send an activation password to a user

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. Click **Service Access**.
4. Click **Set Activation Password**.
5. Type an activation password.
6. Retype the password to confirm it.
7. Type the PIN of the BlackBerry device for the user.
8. In the **Password Expires in** drop-down list, click an expiration time.
9. Notify the user of the new password manually, or click **Generate and Email Activation Password** to send the password to the user automatically.
10. Click **OK**.

Send an activation password to a group of users

1. In the BlackBerry® Manager, in the left pane, click **User Groups**.
2. On the **User Groups List** tab, click a group.
3. Click **Service Access**.
4. Click **Generate and Email Activation Password**.
5. Click **OK**.

Option 3: Activating BlackBerry devices over the LAN

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

When users complete the activation process, the BlackBerry® Enterprise Server adds 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.

Managing administrator accounts

11

Assign a BlackBerry Enterprise Server administrator to a different administrative role

As organizational changes occur, you might need to move an administrator to a different administrative role.

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Role Administration** tab, click the role that the administrator is assigned to.
3. Click **List Administrators**.
4. Remove the administrator from the list.
5. Click the role that you want to assign the administrator to.
6. Click the administrator.
7. Click **OK**.

   The database permissions change immediately.

After you finish: Instruct the administrator to restart the BlackBerry Manager.

Delete an administrator account from a BlackBerry Enterprise Server

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Role Administration** tab, click the role that the administrator is assigned to.
3. Click **Remove Administrators**.
4. In the drop-down list, click the administrator.
5. Click **OK**.

After you finish: Optionally, you can delete the database account associated with that administrator from the database.

Controlling the BlackBerry Enterprise Solution 12

Controlling BlackBerry device access to the BlackBerry Enterprise Server

You can turn on the Enterprise Service Policy to control which BlackBerry® devices can connect to the BlackBerry® Enterprise Server. After you turn on the Enterprise Service Policy, by default, the BlackBerry Enterprise Server prevents connections from new BlackBerry devices that you associate with it; however, it allows connections from BlackBerry devices that are already activated on the BlackBerry Enterprise Server. The Enterprise Service Policy also applies to devices with BlackBerry® Connect™ software, devices with BlackBerry® Built-In™ software, and devices that are running the BlackBerry® Application Suite.

You can use the Enterprise Service Policy to create allowed lists that control which BlackBerry devices users can activate on a BlackBerry Enterprise Server, over the wireless network, or over a serial connection. BlackBerry devices that meet the allowed list criteria can complete the activation process on that BlackBerry Enterprise Server.

You can define the following types of criteria:

- specific, allowed BlackBerry device PINs as a string
- allowed range of BlackBerry device PINs

You can also control access to the BlackBerry Enterprise Server based on specific manufacturers and models of BlackBerry devices. The BlackBerry Manager includes lists of allowed manufacturers and models based on the properties of the BlackBerry devices that are associated with the BlackBerry Enterprise Server. You can clear items in these lists to prevent further connections by BlackBerry devices of a specific manufacturer or model.

You can allow a specific user to override the Enterprise Service Policy so that the user can still connect to the BlackBerry Enterprise Server even if that user's BlackBerry device or BlackBerry enabled device meets criteria that you exclude from the allowed list.

Turn on the Enterprise Service Policy

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. In the right pane, click **Service Control & Customization**.
3. Click **Enable Enterprise Service Policy**.
4. Click **OK**.
5. On the **Global** tab, click **Edit Properties**.
6. Click **Enterprise Service Policy**.
7. Configure the necessary properties.
8. Click **OK**.

Permit a user to override the Enterprise Service Policy

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. Click **Edit Properties**.
4. Click **ES Policy Override**.
5. In the drop-down list, click **True**.
6. Click **OK**.

Controlling BlackBerry device behavior using IT policies

You can use one or more IT policies to control the behavior of BlackBerry® devices and the BlackBerry® Desktop Software in your organization. The Default IT policy includes all standard IT policy rules on the BlackBerry® Enterprise Server. After new users in a BlackBerry Domain activate their BlackBerry devices on the BlackBerry Enterprise Server, the BlackBerry Enterprise Server automatically pushes the Default IT policy to their BlackBerry devices.

The default settings for IT policy rules reflect the default behavior of BlackBerry devices or the BlackBerry Desktop Software. You can use IT policy rules to change the behavior of supported BlackBerry device types. For more information, see the *Policy Reference Guide*.

You can customize and control the behavior of BlackBerry devices and the BlackBerry Desktop Software by performing the following actions:

- changing an IT policy rule to a True or False value
- typing a string, which simultaneously turns on an IT policy rule and provides the parameters for its use
- selecting a predefined, permitted value to assign to an IT policy rule

Create an IT policy

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click **New**.
6. Double-click **IT Policy Name**.
7. Type a name for the new IT policy.
8. Configure the IT policy rules by performing the following actions:
   - In the left pane, click a policy group.

- In the right pane, double-click the IT policy rule.
- Specify a value for the IT policy rule.

9. Click **OK**.

Create an IT policy based on an existing IT policy

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click an IT policy.
6. Click **New Copy**.
7. Type a name for the new IT policy.
8. Configure the IT policy rules by performing the following actions:
   - In the left pane, click a policy group.
   - In the right pane, double-click the IT policy rule.
   - Specify a value for the IT policy rule.
9. Click **OK**.

Import an IT policy

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, expand **Service Control & Customization**.
3. Click **Import IT Policy Definitions**.
4. Click an .xml file that contains IT policy rule definitions.
5. Click **Open**.
6. Click **OK**.

Assign an IT policy to a group of users

1. In the BlackBerry® Manager, in the left pane, click **User Groups**.
2. On the **User Groups List** tab, in the **Group Name** list, click a group.
3. Click **Edit Group Template**.
4. Click **IT Policy**.
5. To override any user exceptions to the IT policy rules, in the right pane, select the **IT Policy Name** option.
6. In the drop-down list, click an IT policy.

7. Click **Reapply Template**.
8. Click **Yes**.
9. Click **OK**.

Assign an IT policy to a user account

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policy to User Mapping**.
5. In the left pane, click a user account.
6. In the right pane, click the IT policy that you want to assign.
7. Click **OK**.

Enforcing IT policy changes over the wireless network

You can send an IT policy over the wireless network to enforce IT policy rule additions, deletions, or changes immediately on C++ based BlackBerry® devices that are running BlackBerry® Device Software version 2.5 or later and on Java® based BlackBerry devices that are running BlackBerry Device Software version 3.6 or later. When a BlackBerry device receives an IT policy update or a new IT policy, the BlackBerry device and BlackBerry® Desktop Software apply the configuration changes.

The BlackBerry® Enterprise Server must resend the IT policy update over the wireless network to the BlackBerry device to update the BlackBerry device behavior and the BlackBerry Desktop Software. By default, the BlackBerry Enterprise Server is designed to resend the IT policy to the BlackBerry devices that you assigned to that IT policy within a short period of time after you update the IT policy.

You can also resend an IT policy to a specific BlackBerry device manually. You can configure the BlackBerry Enterprise Server to resend IT policies to BlackBerry devices at an interval that you schedule regardless of whether you have changed the IT policies. When the BlackBerry device receives an IT policy update or a new IT policy, the BlackBerry device and the BlackBerry Desktop Software apply the configuration changes.

Resend an IT policy to a BlackBerry device manually

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. Click **IT Admin**.
4. Click **Resend IT Policy**.

Resend an IT policy to a BlackBerry device automatically

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the **IT Admin** section, double-click **Policy Resend Interval**.
4. Type the interval, in hours, at which you want the BlackBerry Enterprise Server to resend the IT policy.
5. Click **OK**.

Deactivating BlackBerry devices without applied IT policies

To prevent BlackBerry® devices that do not have an IT policy applied successfully from remaining active on a BlackBerry® Enterprise Server, you can set the Disable Users With Unapplied IT Policy field to True. The Disable User Time Limit field specifies the amount of time (in hours) that a BlackBerry device can be active on a BlackBerry Enterprise Server without having an IT policy applied on that device.

If you set the Disable Users With Unapplied IT Policy field, by default, the BlackBerry Enterprise Server sends the IT policy to the BlackBerry device every 30 minutes until the device applies the IT policy successfully or the time limit expires. If the time limit expires, the BlackBerry Enterprise Server deactivates the PIN for the BlackBerry device user. The allowed range for this setting is 0 hours (to deactivate BlackBerry devices in a failed IT policy state automatically) through 8760 hours.

Deactivate BlackBerry devices without applied IT policies

Before you begin: Activate the BlackBerry® devices on the BlackBerry® Enterprise Server.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **IT Admin**.
4. Click **Disable Users With Unapplied IT Policy**.
5. In the drop-down list, click **True**.
6. In the **Disable User Time Limit** field, type the time limit (in hours) after which the PINs for BlackBerry devices that do not have an IT policy applied are deactivated on the BlackBerry Enterprise Server.
7. Click **Apply**.
8. Click **OK**.

After you finish: Before reactivating the BlackBerry devices on the BlackBerry Enterprise Server, instruct users to click Wipe Device in the Security Options on their BlackBerry devices to delete all data on their BlackBerry devices.

Changing the default behavior of BlackBerry devices and the BlackBerry Desktop Software

To change the default behavior of the BlackBerry® devices and BlackBerry® Desktop Software in your organization, you can change the values of IT policy rules in the Default IT policy, or you can create an IT policy, specify values for the IT policy rules, and assign the new IT policy to one or more user accounts or groups.

You cannot add, delete, or change the permitted values for an existing IT policy rule. You can add, delete or change custom IT policy rules that are specific to your organization's environment

Some IT policy rules have corresponding fields on BlackBerry devices. Users cannot change the value for the corresponding fields when you perform the following actions:

- you change an IT policy rule value to Yes or No
- you configure an IT policy rule value by typing a string that turns on the IT policy rule and provides the parameters for its use at the same time
- you select a predefined, permitted value for the IT policy rule

When you configure a numeric range to assign to an IT policy rule, users can select any numerical value within the permitted range to change the behavior of the BlackBerry device. Users can select the maximum value that you specify for the IT policy rule, regardless of whether it appears in the numeric range.

If a lock icon is located beside a field on a BlackBerry device, this indicates that an IT policy controls the setting and a user cannot change it.

Change the setting for an IT policy rule

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. In the list of policies, click an IT policy.
6. Click **Properties**.
7. Configure the IT policy rules by performing the following actions:
   - In the left pane, click a policy group.
   - In the right pane, click an IT policy rule.
   - Specify a value for the IT policy rule.
8. Click **OK**.

Returning to the default behavior of BlackBerry devices and the BlackBerry Desktop Software

To restore the default behavior of a feature on BlackBerry® devices or in the BlackBerry® Desktop Software, you can change the IT policy rule value to Default, if that option is available, or delete the value that you previously specified.

If you assign users to a new IT policy, you can delete the IT policy to return those users to the Default IT policy. The Default IT policy provides the default behavior for all of the features on the BlackBerry devices and in the BlackBerry Desktop Software. The BlackBerry® Enterprise Server reassigns the users to the Default IT policy automatically and resends the Default IT policy to the BlackBerry devices.

Delete an IT policy

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click the IT policy that you want to delete.
6. Click **Remove**.
7. Click **OK**.

Creating new IT policy rules to control third-party applications

You can create new 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 BlackBerry device applications and features.

Create an IT policy rule for a third-party application

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click the IT policy.
6. Click **Properties**.
7. In the **Properties** list, click **User Defined Items**.
8. Double-click **IT Policy Template**.

9. Click **New**.
10. Type a name and description for the IT policy rule.
11. In the drop-down list, click the type of values that the IT policy rule uses.
12. In the drop-down list, click the location where the IT policy rule is enforced.
13. Type the minimum and maximum values that an integer IT policy rule can accept.
14. Type the data that a bitmask IT policy rule can accept. Include up to eight related Boolean values. You can assign a bit option name for one, some, or all of the 8-bit values. For example, you might create a bitmask IT policy rule called Allowed Features with three Boolean bit values, where bit 0 is named Phone, bit 1 is named Browser, and bit 2 is named Third-Party Apps.
15. Click **OK**.
16. In the **Policy Item Settings** section, provide a value for the IT policy rule in this IT policy.
17. Click **OK**.

Change or delete IT policy rules for third-party applications

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click **Default**.
6. Click **Properties**.
7. In the **Properties** list, click **User Defined Items**.
8. Double-click **IT Policy Template**.
9. Click an IT policy rule.
10. Perform one of the following actions:
    - To change an IT policy rule, click **Properties**. Change the necessary values.
    - To delete an IT policy rule, click **Remove**.

Managing user accounts

13

Managing user groups

You can specify exceptions to user group properties by changing the properties for a single user account after you add that user account to the user group. If you change and reapply the user group properties, the updated group properties override any previous exceptions in the properties of user accounts.

If you move a user account out of a user group, the user account remains in the global users list, but it does not appear in the user group lists.

Change the properties of a user group

After you create a user group, specify the properties that you want to apply to all user accounts in the group. When you add user accounts to a group, you assign the group properties to the user accounts automatically. You can copy properties from one group to another. When you apply configuration properties to a group, or perform administrative tasks on a group, these settings apply to all user accounts in the group.

1. In the BlackBerry® Manager, in the left pane, click **User Groups**.
2. On the **User Groups List** tab, click a group.
3. Click **Edit Group Template**.
4. Change settings for the properties.
5. Click **Apply**.
6. Select the check boxes beside the properties that you want to update for all users in the group.
7. Click **Reapply Template**.
8. Click **Yes**.
9. Click **OK**.

Rename a user group

1. In the BlackBerry® Manager, in the left pane, click **User Groups**.
2. On the **User Groups List** tab, click a group.
3. In the lower pane, click **Group Admin**.
4. Click **Modify Group Definition**.
5. In the **Group Name** field, type a new name.
6. Click **OK**.

Delete a user group

1. In the BlackBerry® Manager, in the left pane, click **User Groups**.
2. On the **User Groups List** tab, click a group.
3. In the lower pane, click **Group Admin**.
4. Click **Delete Group**.
5. Click **Yes**.

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 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 user group

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. In the lower pane, click **Account**.
4. Click **Assign To Group**.
5. Click the group that you want to move the user account to.
6. Click **OK**.

Move a user account out of a user group

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. In the lower pane, click **Account**.
4. Click **Remove From Group**.

5. Click **Yes**.

Move a user account from one BlackBerry Enterprise Server to another

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. In the lower pane, click **Account**.
4. Click **Move User**.
5. Click the destination BlackBerry Enterprise Server.
6. Click **OK**.

Delete a user account from the BlackBerry Enterprise Server

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. In the lower pane, click **Account**.
4. Click **Delete User**.
5. Click **Yes**.
6. Perform one of the following actions:
   - To retain the BlackBerry Enterprise Server information in the user's mailbox, click **No**.
   - To delete the BlackBerry Enterprise Server information from the user's mailbox, click **Yes**.

Update a user account manually

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. In the lower pane, click **Account**.
4. Click **Reload User**.
5. Click **OK**.

Protecting and reassigning BlackBerry devices

14

Protecting lost, stolen, or replaced BlackBerry devices

You can send IT administration commands over the wireless network immediately to protect your organization's confidential data that is stored on BlackBerry® devices.

IT administration command	Description
Set a Password and Lock Handheld	This command creates a new password and locks a lost BlackBerry device remotely. You can communicate the new password to the user when the user locates the BlackBerry device. When the user unlocks the BlackBerry device, the BlackBerry device prompts the user to accept or reject the password change.
Erase Data and Disable Handheld	This command deletes all user information and application data remotely that a BlackBerry device stores. You can use this command to prepare a BlackBerry device to assign it to another user in your organization or to protect a stolen BlackBerry device.

Protect a lost BlackBerry device

If a user misplaces a BlackBerry® device or a BlackBerry device is stolen, you can protect the data on the BlackBerry device by locking the BlackBerry device or making it unavailable.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. Click **IT Admin**.
4. Click **Set Password and Lock Handheld**.
5. In the **New Password** field and the **New Password Again** field, type a password that is between 4 and 14 characters long.
   CAUTION: Do not use special characters. Some BlackBerry devices do not support special characters in passwords. Those BlackBerry devices do not unlock when the user types a password that uses special characters.
6. Click **OK**.

Protect a lost BlackBerry device that a user might recover

If a BlackBerry® device is lost but the user might recover it, you can protect the BlackBerry device by scheduling it to start deleting all user information and application data and 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 BlackBerry device.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. Click **IT Admin**.
4. Click **Erase Data and Disable Handheld**.
5. Click **Yes**.
6. Type the number of hours that you want to pass before the BlackBerry device starts deleting user information and application data.
7. To allow the user to cancel the scheduled command on the BlackBerry device if the user recovers it, select the check box.
8. Click **OK**.

Protect a stolen BlackBerry device

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. Click **IT Admin**.
4. Click **Erase Data and Disable Handheld**.
5. Click **Yes**.

After you finish: You must contact your service provider to turn off service for a BlackBerry device after you send the **Erase Data and Disable Handheld** command to the BlackBerry device and verify that the BlackBerry device received the command.

Reissuing BlackBerry devices to new users

When you reissue a BlackBerry® device to a new user, you have the following options:

- prepare the BlackBerry device for redistribution by deleting the previous user's application data from the BlackBerry device and installing applications on or removing applications from the BlackBerry device
- prepare the BlackBerry device for redistribution by deleting all applications and data from the BlackBerry device to return the BlackBerry device to its default application configuration
- turn off message prepopulation for the new user before redistributing the BlackBerry device if the new user used the BlackBerry® Desktop Manager to back up messages that the previous BlackBerry device received
- register the new PIN for message forwarding by activating the new BlackBerry device after the user receives it

Preparing a BlackBerry device for redistribution

Before you reissue a BlackBerry® device to a new user, delete application data from the BlackBerry device, and then replace the applications on the BlackBerry device.

1. Choose a method to delete the previous user's application data from the BlackBerry device and make the BlackBerry device unavailable to that user before assigning the BlackBerry device to a new user.

Task	Steps
Delete the previous user's application data.	a. Connect the BlackBerry device to the computer on which the BlackBerry Manager is installed. b. In the BlackBerry Manager, in the left pane, click **Local Ports (Device Management)**. c. In the **Connection** list, click a connection. d. Click **Wipe Handheld File System**. e. Click **Yes**. f. If prompted, type the BlackBerry device password to complete the task.
Delete all applications and data from the BlackBerry device.	a. Connect the BlackBerry device to the computer on which the BlackBerry Manager is installed. b. In the BlackBerry Manager, in the left pane, click **Local Ports (Device Management)**. c. In the **Connection** list, click a connection. d. Click **Nuke Handheld**. e. Click **Yes**.

2. Replace the applications on the BlackBerry device.
   a. Connect the BlackBerry device to the computer on which the BlackBerry Manager is installed.
   b. In the BlackBerry Manager, in the left pane, click **Local Ports (Device Management)**.
   c. In the **Connection** list, click a connection.
   d. Click **Load Device (Interactive)**.
   e. Click a software configuration.
   f. Click **OK**.
   g. In the **Device Software Configuration Screen**, clear the check boxes beside the applications to remove, and select the check boxes beside the applications to install.
   h. Complete the application loader wizard.

Managing the delivery of BlackBerry Java Applications, BlackBerry Device Software, and device settings to BlackBerry devices

15

Managing BlackBerry Java Applications on BlackBerry devices

Upgrade an application on a BlackBerry device over the wireless network

You can upgrade a BlackBerry® Java Application, the collaboration client, and the BlackBerry® MDS Runtime on BlackBerry devices over the wireless network. The BlackBerry® Enterprise Server might take up to 4 hours to upgrade an application on a BlackBerry device.

1. In the network drive, add or upgrade the application.
2. Re-index the application.

If the application control policy for an application has a Disposition set to Required, the application upgrade is automatically sent over the wireless network.

Related topics

Making BlackBerry Device Software and Java applications available to users, 29
Create or update a software index for applications on a network drive, 31

Remove applications from BlackBerry devices over the wireless network

You can remove a BlackBerry® Java Application, the collaboration client, and the BlackBerry® MDS Runtime from BlackBerry devices over the wireless network. The BlackBerry® Enterprise Server might take up to 4 hours to remove an application from a BlackBerry device.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Software Configurations** tab, click **Manage Application Policies**.
3. Double-click an application control policy.
4. In the **Disposition** drop-down list, click **Disallowed**.
5. Click **OK**.

Change an application control policy

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Software Configurations** tab, click **Manage Application Policies**.

3. Click the application control policy that you want to change.
4. Click **Properties**.
5. Change the properties of the application control policy.
6. Click **OK**.

Managing software configurations

Delete a software configuration from a user account

1. In the BlackBerry® Manager, click a BlackBerry® Enterprise Server.
2. In the **Users** list, click the user account that you want to delete the software configuration from.
3. Click **Device Management**.
4. Click **Assign Software Configuration**.
5. Click **<none>**.
6. Click **OK**.

Create a software configuration based on an existing software configuration

1. In the BlackBerry® Manager, click **BlackBerry Domain**.
2. On the **Software Configurations** tab, click a software configuration.
3. Click **Copy Configuration**.
4. Double-click the copied software configuration.
5. In the **Configuration Name** field, rename the software configuration.
6. Specify the software configuration properties you want.
7. Click **OK**.

Managing organizer data synchronization 16

Turning off organizer data synchronization

Turn off synchronization of organizer data for all user accounts

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. In the left pane, click **Global PIM Sync**.
4. For each type of organizer data that you do not want to synchronize, in the **Synchronization enabled** drop-down list, click **False**.
5. Click **OK**.

Turn off synchronization of organizer data for a user group

1. In the BlackBerry® Manager, in the left pane, click **User Groups**.
2. On the **User Groups List** tab, click a group.
3. In the lower pane, click **Edit Group Template**.
4. In the left pane, click **PIM Sync**.
5. Perform one of the following actions:
   - If you do not want to synchronize organizer data, in the **Wireless Synchronization Enabled** drop-down list, click **False**.
   - If you want to prevent the synchronization of specific types of organizer data, in the **Wireless Synchronization Enabled** drop-down list, click **True**. For each type of organizer data that you do not want to synchronize, in the **Synchronization enabled** drop-down list, click **False**.
6. Select the check boxes beside the fields that you changed.
7. Click **Reapply Template**.
8. Click **OK**.

Turn off synchronization of organizer data for a specific user account

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, double-click a user account.
3. In the left pane, click **PIM Sync**.

4. Perform one of the following actions:
   - If you do not want to synchronize organizer data for the user, in the **Wireless Synchronization Enabled** drop-down list, click **False**.
   - If you want to prevent the synchronization of specific types of organizer data, in the **Wireless Synchronization Enabled** drop-down list, click **True**. For each type of organizer data that you do not want to synchronize, in the **Synchronization enabled** drop-down list, click **False**.
5. Click **OK**.

Changing how organizer data synchronizes

Change the direction of organizer data synchronization for all user accounts

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. In the left pane, click **Global PIM Sync**.
4. 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**.
5. Click **OK**.

Change the direction of organizer data synchronization for a user group

1. In the BlackBerry® Manager, in the left pane, click **User Groups**.
2. On the **User Groups List** tab, click a group.
3. In the lower pane, click **Edit Group Template**.
4. In the left pane, click **PIM Sync**.
5. For each type of organizer data that you want to specify the synchronization type for, in the **Synchronization enabled** drop-down list, click **True**.
6. 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**.

7. Select the check boxes beside the fields that you changed.
8. Click **Reapply Template**.
9. Click **OK**.

Change the direction of organizer data synchronization for a specific user account

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, double-click a user account.
3. In the left pane, click **PIM Sync**.
4. 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**.
5. Click **OK**.

Change how conflicts during organizer data synchronization are resolved for all user accounts

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. In the left pane, click **Global PIM Sync**.
4. 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**.
5. Click **OK**.

Change how conflicts during organizer data synchronization are resolved for a user group

1. In the BlackBerry® Manager, in the left pane, click **User Groups**.
2. On the **User Groups List** tab, click a group.
3. In the lower pane, click **Edit Group Template**.
4. In the left pane, click **PIM Sync**.
5. For each type of organizer data that you want to change the conflict resolution method for, in the **Synchronization enabled** drop-down list, click **True**.
6. 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 overrules the BlackBerry device data, click **Server Wins**.

- To specify that the BlackBerry device data overrules the BlackBerry Enterprise Server data, click **Device Wins**.

7. Select the check boxes beside the fields that you changed.
8. Click **Reapply Template**.
9. Click **OK**.

Change how conflicts during organizer data synchronization are resolved for a specific user account

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **User List** tab, double-click a user account.
3. In the left pane, click **PIM Sync**.
4. 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**.
5. Click **OK**.

Managing your organization's messaging environment and attachment support

17

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 messages to a BlackBerry device when no filter rules apply

You can configure the 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 Manager, in the left pane, click a BlackBerry Enterprise Server.
2. Click the **Users** tab.
3. Double-click a user account.
4. In the left pane, click **Filters**.
5. In the **Default Action** section, set **Forward messages to BlackBerry device** to **True**.
6. Click **OK**.

Do not deliver messages to a BlackBerry device when no filter rules apply

You can configure the BlackBerry® Enterprise Server to prevent the delivery of incoming messages to a user's BlackBerry device when no email message filters apply to those messages.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Enterprise Server.
2. Click the **Users** tab.
3. Double-click a user account.
4. In the left pane, click **Filters**.
5. In the **Default Action** section, set **Forward messages to BlackBerry device** to **False**.
6. Click **OK**.

Forward messages from inbox subfolders to a BlackBerry device

You can specify which subfolders in a user's email application the BlackBerry® Enterprise Server can forward messages from. By default, the BlackBerry Enterprise Server forwards messages from the inbox only.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Enterprise Server.
2. Click the **Users** tab.
3. Click a user account.
4. In the lower pane, click **Service Access**.
5. Click **Choose Folders for Redirection**.
6. Click **Redirect the following selected folders**.
7. Select the check boxes beside the folders that you want to forward messages from.
8. Click **OK**.

Turn off synchronization for messages sent from BlackBerry devices that belong to a user group

You can turn off synchronization for sent messages if you do not want the members of a user group to receive copies of messages sent from their BlackBerry® devices in the email applications on their computers.

1. In the BlackBerry Manager, in the left pane, click **User Groups**.
2. On the **User Groups List** tab, click a user group.
3. In the lower pane, click **Edit Group Template**.
4. In the left pane, click **Redirection**.
5. In the **Message Forwarding** section, in the **Do Not Save Sent Messages** drop-down list, click **True**.
6. Click **OK**.
7. Select the **Do Not Save Sent Messages** check box.
8. Click **Reapply Template**.

Turn off synchronization for messages sent from a BlackBerry device

You can turn off synchronization for sent messages if you do not want a user's email application to receive a copy of messages that the user sends from the BlackBerry® device.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. Click the **Users** tab.
3. Double-click a user account.
4. In the left pane, click **Redirection**.
5. In the **Message Forwarding** section, in the **Do Not Save Sent Messages** drop-down list, click **True**.

6. Click **OK**.

Turn off message forwarding to user accounts in a user group

You can temporarily stop the BlackBerry® Enterprise Server from forwarding messages to user accounts that are in 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 messages during that time). When you turn off message forwarding for user accounts, the users can send messages from their BlackBerry devices, but cannot receive messages.

1. In the BlackBerry Manager, in the left pane, click **User Groups**.
2. On the **Users Groups List** tab, click a user group.
3. In the lower pane, click **Service Access**.
4. Click **Disable Redirection**.

After you finish: Users can turn on message forwarding on the BlackBerry device manually.

Turn off message forwarding to a user account

You can temporarily stop the BlackBerry® Enterprise Server from forwarding messages to a BlackBerry device (for example, if a user is out of a wireless coverage area and does not want to receive messages during that time). When you turn off message forwarding for a user account, the user can send messages from the BlackBerry device, but cannot receive messages.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Enterprise Server.
2. Click the **Users** tab.
3. Click a user account.
4. In the lower pane, click **Service Access**.
5. Click **Disable Redirection**.

After you finish: The user can turn on message forwarding on the BlackBerry device manually.

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

You can turn off wireless message reconciliation to reduce wireless network traffic or to manage individual user accounts. If you turn off wireless message reconciliation, users can reconcile their messages only by connecting their BlackBerry® devices to the BlackBerry® Desktop Manager.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Messaging**.
4. In the **Messaging Options** section, in the **Wireless Message Reconciliation Enabled** drop-down list, click **False**.
5. Click **OK**.

Turn on reconciliation for permanently deleted messages

Users can delete messages permanently in Microsoft® Outlook® by pressing SHIFT+DELETE. You can turn on hard deletes reconciliation if you want to delete permanently deleted messages from users' BlackBerry® devices. This feature also deletes messages that users move to personal folders or archive in Microsoft Outlook. The BlackBerry Messaging Agent uses recurring message scans to detect permanently deleted messages on the messaging server and delete them from the users' BlackBerry devices. This feature requires BlackBerry® Device Software version 3.6 or later.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Messaging**.
4. In the **Messaging Options** section, in the **Hard Deletes Reconciliation** drop-down list, click **True**.
5. Click **OK**.

After you finish: On the computer that hosts the BlackBerry Dispatcher, in the Windows® Services, restart the BlackBerry Dispatcher.

Managing content in RTF and HTML-formatted messages

The BlackBerry® Enterprise Server supports RTF and HTML-formatted messages 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 messages. Users can configure the message settings on their BlackBerry devices. The settings that you define override the settings that users define.

View settings for HTML-formatted messages

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, double-click a user account.
3. In the left pane, click **Redirection**.

4. In the **Messaging Options** section, view the settings for **Rich Content Enabled** and **Download Images Automatically**.

Turn off rich content and inline images for groups of users

You can prevent the BlackBerry® Enterprise Server from sending email messages in RTF and HTML format to BlackBerry devices. When rich-text formatting is turned off, the BlackBerry Enterprise Server sends all email messages in plain-text format. You can also prevent the BlackBerry Enterprise Server from sending email messages with inline images to BlackBerry devices.

Turning off rich-content and inline images reduces resource consumption on the computers that are running the messaging server, the BlackBerry Attachment Service, and the BlackBerry MDS Services.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. Click **Messaging**.
4. In the **Messaging Options** section, perform one of the following actions:
   - To turn off rich-content formatting, click **Rich Content Enabled**. In the drop-down list, click **False**.
   - To turn off inline images, click **Inline Images Enabled**. In the drop-down list, click **False**.
5. Click **OK**.

Turn off rich content and inline images in messages for individual users

You can prevent the BlackBerry® Enterprise Server from sending email messages in RTF and HTML format to individual BlackBerry devices. When rich text formatting is turned off, the BlackBerry Enterprise Server sends all email messages in plain-text format. You can also prevent the BlackBerry Enterprise Server from sending email messages with inline images to specific BlackBerry devices, or allow specific device users to request inline images manually.

Turning off rich content formatting and inline images reduces resource consumption on the computers that are running the messaging server, the BlackBerry Attachment Service, and the BlackBerry MDS Services.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. In the list of IT policies, click an IT policy.
4. Click **Properties**.
5. In the **Email Messaging policy group** section, perform one of the following actions:
   - To turn off rich-content formatting, click **Disable Rich Content Email**. In the drop-down list, click **True**.
   - To turn off inline images, click **Inline Content Requests**. In the drop-down list, click **Disabled**.
6. Click **OK**.

Managing access to remote message data

Turn off the ability to check meeting invitee availability on the BlackBerry device

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. Click **Messaging**.
4. In the **Messaging Options** section, click **Free Busy Lookup Enabled**.
5. In the drop-down list, click **False**.
6. Click **OK**.

Turn off the ability to search for remote email messages from the BlackBerry device

You can prevent BlackBerry® device users from searching for email messages that are located on the messaging server from their BlackBerry devices.

Before you begin: Wireless email reconciliation must be turned on to use the feature.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Messaging**.
4. In the **Messaging Options** section, click **Remote Search Enabled**.
5. In the drop-down list, click **False**.
6. Click **OK**.

Managing signatures and disclaimers in email messages

Add a signature to all messages sent by members of a user group

Users can change their message signatures on their BlackBerry® devices or by using the BlackBerry® Desktop Manager. To enforce any signature format policies in your organization, you can add a standard signature to your organization's disclaimer.

1. In the BlackBerry Manager, in the left pane, click **User Groups**.
2. On the **User Groups List** tab, click a group.
3. In the lower pane, click **Edit Group Template**.
4. In the left pane, click **Redirection**.
5. In the **Auto Signature** section, double-click the **Signature** field.

6. Type the signature that you want to appear in the messages that the users send from their BlackBerry devices.
7. Click **OK**.
8. Select the **Signature** check box.
9. Click **Reapply Template**.

Add a signature to all messages sent from a user's BlackBerry device

Users can change their message signatures on their BlackBerry® devices or by using the BlackBerry® Desktop Manager. To enforce any signature format policies in your organization, you can add a standard signature to your organization's disclaimer.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, double-click a user account.
3. In the left pane, click **Redirection**.
4. In the **Auto Signature** section, double-click the **Signature** field.
5. Type the signature that you want to appear in the messages that the user sends from the BlackBerry device.
6. Click **OK**.

Add a disclaimer to all messages sent from BlackBerry devices

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Messaging**.
4. In the **Messaging Options** section, perform one of the following actions:
   - To add a disclaimer before the message body, double-click **Prepended Disclaimer Text**.
   - To add a disclaimer after the user signature, double-click **Appended Disclaimer Text**.
5. Type the disclaimer.
6. Click **OK**.

Users cannot change the disclaimers that you define.

Add a disclaimer to all messages sent by members of a user group

1. In the BlackBerry® Manager, in the left pane, click **User Groups**.
2. On the **User Groups List** tab, click a group.
3. Click **Edit Group Template**.
4. In the **Messaging Options** section, perform one of the following actions:
   - To add a disclaimer before the message body, double-click **Prepended Disclaimer Text**.
   - To add a disclaimer after the user signature, double-click **Appended Disclaimer Text**.

5. Type the disclaimer.
6. Click **OK**.
7. Select the check box to the left of the appropriate disclaimer field.
8. Click **Reapply Template**.
9. Click **Yes**.
10. Click **OK**.

Users cannot change the disclaimers that you define.

Add a disclaimer to all messages sent from a user's BlackBerry device

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, double-click a user account.
3. Perform one of the following actions:
   - To add a disclaimer before the message body, double-click **Prepended Disclaimer Text**.
   - To add a disclaimer after the user signature, double-click **Appended Disclaimer Text**.
4. Type the disclaimer.
5. Click **OK**.

Users cannot change the disclaimers that you define.

Specify conflict rules for disclaimers

You can add a disclaimer to all messages that are sent by an individual user that is different from the disclaimer that you added for all users on a BlackBerry® Enterprise Server. You can specify conflict rules for dislaimers 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, followed by the BlackBerry Enterprise Server disclaimer.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Messaging**.
4. In the **Messaging Options** section, perform one of the following actions:
   - To specify conflict rules for disclaimers that appear before the message body, click **Prepended Disclaimer Conflict Rule**.
   - To specify conflict rules for disclaimers that appear after the user signature, click **Appended Disclaimer Conflict Rule**.
5. In the drop-down list, click a rule.
6. Click **OK**.

Turn off disclaimers

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Messaging**.
4. In the **Messaging Options** section, perform any of the following actions:
   - To turn off disclaimers that appear before the message body, click **Prepended Disclaimer Conflict Rule**. In the drop-down list, click **Disable all disclaimer text**.
   - To turn off disclaimers that appear after the user signature, click **Appended Disclaimer Conflict Rule**. In the drop-down list, click **Disable all disclaimer text**.
5. Click **OK**.

Monitor messages that users send from their 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 Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. Click **Messaging**.
4. In the **Messaging Options** section, double-click **Auto BCC Addresses**.
5. Import a list of addresses or type the addresses, separated by a semicolon (;).
6. Click **OK**.

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 messages for a specific user from the incoming message queue

You can delete messages for a specific user from the incoming message queue to manage the size of the queue and to manage user accounts with high pending message counts.

When you delete pending messages from the incoming message queue, the BlackBerry® Enterprise Server does not send the messages to the user's BlackBerry device. The messages still appear in the email application on the user's computer.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Enterprise Server.
2. On the **Users** tab, click a user account.
3. In the lower pane, click **Service Control & Customization**.
4. Click **Purge Pending Messages**.

If the user account has wireless calendar synchronization turned on, the BlackBerry Enterprise Server deletes pending calendar messages from the incoming message queue and resends them later. The BlackBerry Enterprise Server does not delete IT policies and IT administration commands from the incoming message queue.

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 group

1. In the BlackBerry® Manager, in the left pane, click **User Groups**.
2. On the **User Groups List** tab, click a group.
3. In the lower pane, click **Edit Group Template**.
4. In the left pane, click **PIM Sync**.
5. Click **Automatic Wireless Backup Enabled**.
6. In the drop-down list, click **False**.
7. Select the **Automatic Wireless Backup Enabled** check box.
8. Click **Reapply Template**.
9. Click **OK**.

Turn off the wireless backup of organizer data for a user account

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, double-click a user account.
3. In the left pane, click **PIM Sync**.
4. Click **Automatic Wireless Backup Enabled**.

5. In the drop-down list, click **False**.
6. Click **OK**.

Delete a user's organizer data from the BlackBerry Enterprise Server

If the BlackBerry® Enterprise Server is not writing a user's organizer data from the BlackBerry device 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 user's BlackBerry device to synchronize the user's current organizer data with the BlackBerry Enterprise Server over the wireless network.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Enterprise Server.
2. On the **Users** tab, click a user account.
3. In the lower pane, click **Service Control & Customization**.
4. Click **Clear PIM Sync Backup Data**.
5. Click **OK**.

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 for contact pictures on a user account

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. In the lower pane, click **Service Control & Customization**.
4. Click **Edit PIM Sync Field Mapping**.
5. In the **Desktop Field** column, click **Picture**.
6. In the **Device Field** column, in the drop-down list, click **<Clear>**.
7. Click **OK**.

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 the BlackBerry Domain

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Account**.
3. Click **Send Message**.
4. Complete the instructions on the screen.

Send a notification message to all users on a BlackBerry Enterprise Server

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Account**.
3. Click **Send Message**.
4. Complete the instructions on the screen.

Send a notification message to the members of a user group

1. In the BlackBerry® Manager, in the left pane, click **User Groups**.
2. On the **User Groups List** tab, click a group.
3. In the lower pane, click **Account**.
4. Click **Send Message**.
5. Complete the instructions on the screen.

Send a notification message to a specific user

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Users** tab, click a user account.
3. In the lower pane, click **Account**.

4. Click **Send Message**.
5. Complete the instructions on the screen.

Managing instant messaging

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 Microsoft® Office Live Communications Server 2005, Microsoft® Office Communications Server 2007, and IBM® Lotus® Sametime® server. 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.

Change the instant messaging server that the BlackBerry Collaboration Service connects to

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry Collaboration Service.
2. On the **Collaboration Service** tab, click **Edit Properties**.
3. In the left pane, click **General**.
4. In the **Connection** section, double-click **Host**.
5. Type the host name of the instant messaging server.
6. In the **Connection** section, double-click **Port**.
7. Type the port number of the instant messaging server.
8. Click **OK**.

Changing the transport protocol that the BlackBerry Collaboration Service uses to connect to the instant messaging server

If users are using the BlackBerry® Client for use with Microsoft® Office Live Communications Server 2005 or the BlackBerry® Client for use with Microsoft® Office Communications Server 2007, you can change the transport protocol that the BlackBerry Collaboration Service uses to connect to the instant messaging server in your organization's environment.

Change the transport protocol for a Windows Messenger environment

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry Collaboration Service.
2. On the **Collaboration Service** tab, click **Edit Properties**.
3. In the left pane, click **General**.

4. In the **Connection** section, click **Transport Protocol**.
5. In the drop-down list, click one of the following protocol types:
   - **TLS**: Use TLS if you want the Microsoft® Office Live Communications Server connector to encrypt the data that it sends to the Microsoft Office Live Communications Server. The computer running the Microsoft Office Live Communications Server connector must trust the TLS certificate on the Microsoft Office Live Communications Server.
     If you use TLS, the Microsoft Office Live Communications Server uses one socket connection for each user login. This allows you to support up to 2000 instant messaging sessions at the same time.
   - **TCP**: Use standard TCP if you do not want the Microsoft Office Live Communications Server connector to encrypt the data that it sends to the Microsoft Office Live Communications Server.
     If you use TCP, the Microsoft Office Live Communications Server uses up to three socket connections for each user login; you cannot support up to 2000 instant messaging sessions at the same time.
6. Click **OK**.

Change the transport protocol for a Microsoft Office Communicator environment

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry Collaboration Service.
2. On the **Collaboration Service** tab, click **Edit Properties**.
3. In the left pane, click **General**.
4. In the **Connection** section, click **Transport Protocol**.
5. In the drop-down list, click one of the following protocol types:
   - **HTTPS**: Use 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.
   - **HTTP**: Use standard 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 **OK**.

Change the transport protocol for a mixed instant messaging environment

If your environment supports Microsoft® Office Communicator for use with Microsoft® Office Live Communications Server 2005 and Microsoft® Windows® Messenger, when you install or upgrade the BlackBerry® Enterprise Server, you can configure support for a mixed instant messaging environment.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Collaboration Service.
2. On the **Collaboration Service** tab, click **Edit Properties**.
3. In the left pane, click **General**.
4. Specify the transport protocol for the primary server for instant messaging.
5. To change the transport protocol for the related server for instant messaging, in the **Related Services** section, double-click **Related Services**.

6. Double-click the related server for instant messaging.
7. Change **Transport Protocol** to the transport protocol that you want to use for the appropriate environment for enterprise instant messenging.

Specify the Microsoft Windows domain name for users who log in to the collaboration client

You can specify your organization's Microsoft® Windows® domain name so that users do not have to type their user names when they log in to the collaboration client on their BlackBerry® devices.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Collaboration Service.
2. On the **Collaboration Service** tab, click **Edit Properties**.
3. In the left pane, click **General**.
4. In the **Service** section, double-click **Default Domain Name**.
5. Type the Microsoft Windows domain name.
6. Click **OK**.

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 environment, 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 Manager, in the left pane, click a BlackBerry Collaboration Service.
2. On the **Collaboration Service** tab, click **Edit Properties**.
3. In the left pane, click **General**.
4. In the **Service** section, double-click **Maximum Simultaneous Sessions**.
5. Type a number.
6. Click **OK**.

Specify the idle timeout limit for instant messaging sessions

If the maximum number of instant messaging sessions that can be open at the same time is reached, the BlackBerry® Collaboration Service closes idle sessions that have exceeded the idle timeout limit.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Collaboration Service.
2. On the **Collaboration Service** tab, click **Edit Properties**.
3. In the left pane, click **General**.

4. In the **Service** section, double-click **Idle Timeout**.
5. Type a value, in seconds.
6. Click **OK**.

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 Manager, in the left pane, click a BlackBerry Collaboration Service.
2. On the **Collaboration Service** tab, click **Edit Properties**.
3. In the left pane, click **General**.
4. In the **Service** section, double-click **Inactivity timeout**.
5. Type a value, in milliseconds.
6. Click **OK**.

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 topics

Change the setting for an IT policy rule, 82

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 topics
Configure a maximum file size for media types, 137

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 topics
Change the setting for an IT policy rule, 82

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 topics
Change the setting for an IT policy rule, 82

Manage the icon that appears on the BlackBerry device for mobile contacts

If users are using the BlackBerry® Client for IBM® Lotus® Sametime® or the BlackBerry® Client for Novell® GroupWise® Messenger, you can control whether an icon appears on the BlackBerry device beside the names of contacts who are using the same collaboration client. By default, the icon appears.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Collaboration Service.
2. On the **Collaboration Service** tab, click **Edit Properties**.
3. In the left pane, click **General**.

4. In the **Service** section, perform one of the following actions:
   - To display the icon, set **Show Mobile Icon** to **True**.
   - To hide the icon, set **Show Mobile Icon** to **False**.
5. Click **OK**.

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="OfficePhone" FieldName="OfficePhoneNumber" Type="text/plain"/>
<Detail Id="HomePhone" FieldName="PhoneNumber" Type="text/plain"/>
<Detail Id="CellPhone" FieldName="CellPhoneNumber" Type="text/plain"/>
<Detail Id="Manager" FieldName="Manager" Type="text/plain"/>
<Detail Id="Department" FieldName="Department" Type="text/plain"/>
<Detail Id="WorkAddress" FieldName="OfficeStreetAddress" Type="text/plain"/>
<Detail Id="WorkZip" FieldName="OfficeZip" Type="text/plain"/>
<Detail Id="WorkState" FieldName="OfficeState" Type="text/plain"/>
<Detail Id="WorkCity" FieldName="OfficeCity" Type="text/plain"/>
<Detail Id="HomeAddress" FieldName="StreetAddress" Type="text/plain"/>
<Detail Id="HomeZip" FieldName="Zip" Type="text/plain"/>
<Detail Id="HomeState" FieldName="State" Type="text/plain"/>
<Detail Id="HomeCity" FieldName="City" Type="text/plain"/>
<Detail Id="LoginId" FieldName="ShortName" Type="text/plain"/>
```

5. Copy the following text into the **ParamsSets** section of the **UserInfoConfig.xml** file:

<Set SetId="2"
params="MailAddress,Name,Title,Location,Telephone,Photo,Company,OfficePhone,HomePhone,CellPhone,Manager,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:
   a. Create a test user account in the IBM Lotus Domino Directory.
   b. Using the IBM Lotus Sametime administration web page, change the test user account by typing values for the contact information fields.
   c. In a browser, type **http://<*Sametime_Server_Name*>/servlet/UserInfoServlet?operation=3&setid=2&userid=<*Test_Account_Name*>**.
   d. 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.

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 BlackBerry 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 BlackBerry Enterprise Server from receiving HTTP requests from external servers. If your 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 Manager, in the left pane, click a BlackBerry Collaboration Service.
2. On the **Collaboration Service** tab, click **Edit Properties**.
3. In the left pane, click **Proxy**.
4. Double-click **Proxy Mappings**.
5. Click **New**.
6. Configure the settings for an authenticated or unauthenticated proxy server. Use the default URL.
7. Click **OK**.
8. 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.
9. If the BlackBerry Enterprise Server is located in a restricted network, complete steps 10 through 14.
10. On the computer that hosts the BlackBerry Collaboration Service, navigate to *<drive>*:\Program Files\Research In Motion \BlackBerry Enterprise Server\BBIM\Servers\Instance\Config.
11. In a text editor, open the **rimpublic.properties** file.
12. Copy the following text into the **rimpublic.properties** file, and replace *<hostname>* 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
13. Save and close the **rimpublic.properties** file.
14. In the BlackBerry Manager, restart the BlackBerry Collaboration Service.

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.

Optimize how the BlackBerry Attachment Service converts attachments

1. On the computer that hosts the BlackBerry® Attachment Service, on the taskbar, click **Start > Programs > BlackBerry Enterprise Server > BlackBerry Server Configuration**.
2. On the **Attachment Server** tab, in the **Configuration Option** drop-down list, click **Attachment Server**.
3. Configure the BlackBerry Attachment Service optimization settings.
4. Click **OK**.
5. In the Microsoft® Windows® Services, restart the BlackBerry Attachment Service.

BlackBerry Attachment Service optimization settings

Setting	Description	Range	Default
Concurrent Caching	The BlackBerry® Attachment Service maintains the cache for 25 minutes or until a new request exceeds the cache limit for that conversion process. If the cache limit is exceeded, the BlackBerry Attachment Service deletes the document with the oldest time stamp from the cache. To prevent multiple requests for the same attachment from using the first cached copy of the attachment DOM in a conversion process, you can set this drop-down list to Disabled.	—	Enabled
Document Cache Size (docs)	This field specifies the maximum number of converted documents that can be located in the document cache (as DOM) for an individual conversion process.	1 through 128	32
Conversion Processes	This field specifies the number of conversion requests that the BlackBerry Attachment Service can process simultaneously. When you specify this value, consider the amount of available memory and the competing services on the computer that hosts the BlackBerry Attachment Service.	1 through 64	4

Setting	Description	Range	Default
Recycle Time	This field specifies a time limit for an application conversion process to reuse system resources to reclaim space and prevent failed processes from occupying memory resources.	300 through 3600 seconds	1500
Max. Threads Per Process	This field specifies the number of documents that the BlackBerry Attachment Service can convert simultaneously in a single conversion process. You can use this setting with the Busy Threshold(s) setting to control thread saturation and to manage the BlackBerry Attachment Service workload.	2 through 32	4
Busy Threshold (s)	This field specifies the busy threshold at which the BlackBerry Attachment Service does not accept new conversion requests.	60 through 270 seconds	120

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 and 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. On the computer that hosts the BlackBerry Attachment Service, on the taskbar, click **Start > Programs > BlackBerry Enterprise Server > BlackBerry Server Configuration**.
2. On the **Attachment Server** tab, in the **Configuration Option** drop-down list, click **Attachment Server**.
3. In the **Distiller Settings** section, in the **Max. File Size (Kb)** column, click the value for the distiller that you want to change.
4. Type a value in KB.
5. Click **OK**.

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

File format	Suggested size
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
OpenDocument	less than 2000 KB
RTF	less than 2000 KB
ZIP archives	less than 2000 KB

Change the maximum dimensions for image attachments that users can view

You can control the dimensions of image attachments that users can view on their BlackBerry® devices. By default, the BlackBerry Attachment Service sets a maximum width of 5000 pixels and a maximum height of 4000 pixels.

1. On the computer that hosts the BlackBerry Attachment Service, on the **Start** menu, click **Run**.
2. Type **regedit**.
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\BBAttachEngine\Distillers\LoadImageDistiller.
   - If you are running a 64-bit version of Windows, navigate to HKEY_LOCAL_MACHINE\Software\WOW6432Node\Research In Motion\BBAttachEngine\Distillers\LoadImageDistiller.
4. Change the **MaxWidth** DWORD value to the maximum width, in pixels, that you want to permit.
5. Change the **MaxHeight** DWORD value to the maximum height, in pixels, that you want to permit.
6. In the Microsoft® Windows® Services, restart the BlackBerry Attachment Service.

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 attachments that users can send is 3072 KB, and the maximum total for multiple attachment uploads in a single message is 5120 KB.

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Messaging**.
4. Perform any of the following actions:
   - To change the maximum file size for a single attachment that BlackBerry devices can send, in the **Maximum Upload Attachment Size** field, type a number that is between 1 and 3072 KB.
   - To change the maximum file size for multiple attachments that BlackBerry devices can send at one time, in the **Maximum Upload Total Attachment Size** field, type a number that is between 1 and 5120 KB and that is greater than the value in the **Maximum Upload Attachment Size** field.
5. Click **OK**.

Prevent users from sending large attachments

If you prevent users from sending large attachments, they can only send specific attachments—certificates and address book entries—that are less than a single packet.

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Messaging**.
4. In the **Maximum Upload Attachment Size** field, type **0**.
5. Click **OK**.

Change the maximum file size of attachments that users can download

Certain versions of the BlackBerry® Device Software enable users to download attachments in their native formats (for example, .txt for a text file) to their BlackBerry devices. Users can open and make changes to the downloaded files using an appropriate third-party application on their BlackBerry devices. Depending on the file format, a user might be able to open the file 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 Manager, in the left pane, click a BlackBerry® Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. In the left pane, click **Messaging**.
4. Click **Maximum Download Attachment Size**.
5. Type a number, in KB, between 0 and 10240 (10 MB). If you type **0**, users cannot download attachments in a native format to their BlackBerry devices.
6. Click **OK**.

Turn off support for an attachment file format

The BlackBerry® Attachment Service uses distillers to convert attachments 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 in a specific file format. For example, if you turn off the .pdf distiller, users cannot view .pdf attachments on their BlackBerry devices.

1. On the computer that hosts the BlackBerry Attachment Service, on the taskbar, click **Start > Programs > BlackBerry Enterprise Server > BlackBerry Server Configuration**.
2. On the **Attachment Server** tab, in the **Configuration Option** drop-down list, click **Connector Configuration**.
3. In the **Format Extension** field, delete one or more file format extensions that you want to turn off support for.
4. On the **Attachment Server** tab, in the **Configuration Option** drop-down list, click **Attachment Server**.
5. In the **Distiller Settings** section, clear the check box beside each file format that you want to turn off support for.
6. Click **OK**.
7. On the computer that hosts the BlackBerry® Enterprise Server, in the Windows® Services, restart the BlackBerry Dispatcher.
8. On the computer that hosts the BlackBerry Attachment Service, in the Windows Services, restart the BlackBerry Attachment Service.

Add support for additional attachment file formats

If your organization's messaging server connects to a document management system that renames file format extensions, you must add the extensions to the list of supported file formats.

1. On the computer that hosts the BlackBerry® Attachment Service, on the taskbar, click **Start > Programs > BlackBerry Enterprise Server > BlackBerry Server Configuration**.
2. On the **Attachment Server** tab, in the **Configuration Option** drop-down list, click **Connector Configuration**.
3. In the **Format Extension** field, type the file format extensions that you want to add support for.
4. Click **OK**.
5. On the computer that hosts the BlackBerry® Enterprise Server, in the Microsoft® Windows® Services, restart the BlackBerry Dispatcher.

Managing calendars

18

Correcting calendar synchronization errors on BlackBerry devices

You can run the calendar synchronization process on a BlackBerry® Enterprise Server instance to find and correct differences between the calendar entries on BlackBerry devices and the calendar entries on a computer.

You can specify the recurring day and time when the process runs and how many days before a specific date occurs that the process checks the calendars for synchronization errors. You can also specify whether the process checks calendar entries for a specific user, users on a specific BlackBerry Enterprise Server, or all users. The process follows a hierarchy to determine what calendar entries to check. The hierarchy determines that 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.

You can configure the calendar synchronization process using the BlackBerry® Enterprise Trait Tool. The BlackBerry Enterprise Trait Tool is located in the Tools directory of the BlackBerry Enterprise Server installation files.

By default, when the calendar synchronization process finds differences between the calendar entries on a BlackBerry device and the calendar entries on a computer, the process writes information about the differences to the BlackBerry Messaging Agent log file. You can use this information to troubleshoot calendar synchronization issues. You can configure the process to automatically correct the calendar synchronization errors that it finds.

Configuration levels using the BlackBerry Enterprise Trait Tool

You can specify whether the calendar synchronization process checks calendar entries for a specific user, users on a specific BlackBerry® Enterprise Server, or all users by setting the configuration level using the BlackBerry® Enterprise Trait Tool. The tool uses a hierarchy to determine what calendar entries the calendar synchronization process should check. The hierarchy determines that settings at the user level override settings at the server levels settings at the server level override settings at the global levels 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 on the calendar synchronization process

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 on calendar synchronization for a specific user account, type **TraitTool -user <*smtp_address*> -trait ExchangeSmartSyncEnable -set true**.
   - To turn on calendar synchronization for all user accounts that are associated with a BlackBerry Enterprise Server, type **TraitTool -server <*server_name*> -trait ExchangeSmartSyncEnable -set true**.
   - To turn on calendar synchronization for all user accounts, type **TraitTool -global -trait ExchangeSmartSyncEnable -set true**.
5. Press ENTER.

Example: Turning on the process for all users

```
TraitTool -global -trait ExchangeSmartSyncEnable -set true
```

Example: Turning off the process for a specific user

```
TraitTool -user greg.stark@blackberry.com -trait ExchangeSmartSyncEnable -set false
```

After you finish: To turn off the calendar synchronization process, type **TraitTool -<*level*> -trait ExchangeSmartSyncEnable -set false**, 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 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
```

Permit the calendar synchronization process to correct errors automatically

You can specify whether the calendar synchronization process adds calendar synchronization errors to the BlackBerry® Messaging Agent log file or adds and corrects calendar synchronization errors. By default, the process adds calendar synchronization errors to the BlackBerry Messaging Agent log file without correcting the errors.

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 turn on automatic correction of calendar synchronization errors for a specific user account, type **TraitTool -user *<smtp_address>* -trait ExchangeSmartSyncSendUpdate -set True**.
   - To turn on 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 true**.
   - To turn on automatic correction of calendar synchronization errors for all user accounts, type **TraitTool -global -trait ExchangeSmartSyncSendUpdate -set true**.
5. Press ENTER.

Example: Configuring the process to correct calendar synchronization errors for a specific user

```
 TraitTool -user greg.stark@blackberry.com -trait ExchangeSmartSyncSendUpdate -set
true
```

After you finish: To turn off calendar synchronization error correction, type **TraitTool -*<level>* -trait ExchangeSmartSyncSendUpdate -set false**, 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 days that the calendar synchronization process verifies

You can configure the calendar synchronization process to check for calendar synchronization errors a specific number of days before a specific date occurs.

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 turn on the calendar synchronization process so that it checks for errors for a specific user account a specific number of days before a specific date occurs, type **TraitTool -user *<smtp_address>* -trait ExchangeSmartSyncDays -set *<value>***, where *<value>* is a number from 1 to 365.

- To turn on the calendar synchronization process so that it checks for errors a specific number of days before a specific date occurs 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 turn on the calendar synchronization process so that it checks for errors a specific number of days before a specific date occurs for all user accounts, type **TraitTool -global -trait ExchangeSmartSyncDays -set <*value*>**, where *<value>* is a number from 1 to 365.

5. Press ENTER.

Example: Configuring the calendar synchronization process to check calendar entries 3 days in advance for all users

```
TraitTool -global -trait ExchangeSmartSyncDays -set 3
```

Configure when the calendar synchronization process runs

You can configure the calendar synchronization process to start running at a specific hour or to run on recurring days or on only one recurring day. To specify more than one value for when the calendar synchronization process 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 (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 (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 (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 the calendar synchronization process 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: Configuring the calendar synchronization process to run at 11:00 PM for all users on the BlackBerry Enterprise Server that is named SERVER02

```
TraitTool -server SERVER02 -trait ExchangeSmartSyncTriggerHour -set 23
```

Example: Configuring the calendar synchronization process to run on weekdays for all users

```
TraitTool -global -trait ExchangeSmartSyncSchedule -set Weekdays
```

Example: Configuring the calendar synchronization process to run on Monday, Wednesday, and Friday for a specific user

```
TraitTool -user greg.stark@blackberry.com -trait ExchangeSmartSyncSchedule -set
Monday,Wednesday,Friday
```

Delete a calendar synchronization setting

If you delete a calendar synchronization setting, the calendar synchronization process uses the setting that you defined 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 defined at the server level because the server level is the next highest level. If you do not define 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: Deleting the setting for the hour that the process runs on the BlackBerry Enterprise Server that is named SERVER01

```
TraitTool -server SERVER01 -trait ExchangeSmartSyncTriggerHour -erase
```

Managing BlackBerry MDS Runtime Applications and BlackBerry Browser Applications

19

Upgrade a BlackBerry MDS Runtime Application on BlackBerry devices

1. In the BlackBerry® Manager, in the left pane, expand a BlackBerry MDS Integration Service.
2. Click **Application Registry**.
3. On the **Application Registry** tab, click the BlackBerry MDS Runtime Application that you want to upgrade.
4. In the lower pane, click **Device Management**.
5. Perform one of the following tasks:

Task	Steps
Upgrade a BlackBerry MDS Runtime Application on specific BlackBerry devices.	a. Click **Upgrade on Device**. b. In the **Upgrade application on devices** drop-down list, click **with old version of application**. c. Clear the **Select all** check box. d. Click the PINs of the BlackBerry devices that you want to upgrade the BlackBerry MDS Runtime Application on.
Upgrade a BlackBerry MDS Runtime Application on BlackBerry devices, and install the application on BlackBerry devices that do not have the application.	a. Click **Install on Device**. b. In the **Install application on devices** drop-down list, click **with or without application installed**.

6. Click **Next**.
7. In the **Group size for pushing** field, type the number of BlackBerry devices that you want to send the upgrade request to simultaneously.
8. In the **Push interval (minute)** field, type an interval after which the BlackBerry MDS Integration Service sends the upgrade request to BlackBerry devices.
9. To set a specific date to send the upgrade request on, click the **Schedule** check box. Specify the start date and end date.
10. To display a prompt on BlackBerry devices that allows users to cancel the upgrade or installation, clear the **Required** check box.
11. Click **Next**.
12. Click **Finish**.

Users receive a prompt to start the upgrade the next time that they open the BlackBerry MDS Runtime Application on their BlackBerry devices.

Remove a trusted certificate from the BlackBerry MDS Integration Service

If you do not want the BlackBerry® MDS Integration Service to authenticate BlackBerry MDS Runtime Applications that use a specific digital certificate, remove the digital certificate from the BlackBerry MDS Integration Service.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Integration Service.
2. On the **MDS Integration Services** tab, click **Edit Properties**.
3. In the left pane, click **Certificate**.
4. Double-click **BlackBerry MDS Integration Service Certificate Definition**.
5. Click a certificate.
6. Click **Remove**.
7. Click **OK**.

Making installed BlackBerry MDS Runtime Applications unavailable on BlackBerry devices

Make an installed BlackBerry MDS Runtime Application unavailable on BlackBerry devices

You can quarantine a BlackBerry® MDS Runtime Application if you want to make it temporarily unavailable on BlackBerry devices. Quarantined applications appear on BlackBerry devices with a quarantine icon. Users cannot open quarantined applications on their BlackBerry devices.

1. In the BlackBerry Manager, in the left pane, expand a BlackBerry MDS Integration Service.
2. Click **Applications Installed**.
3. On the **Applications Installed** tab, click the BlackBerry MDS Runtime Application that you want to quarantine.
4. In the lower pane, click **Application Management**.
5. Click **Quarantine Application**.
6. Click **Yes**.

Make an installed BlackBerry MDS Runtime Application available on BlackBerry devices again

1. In the BlackBerry® Manager, in the left pane, expand a BlackBerry MDS Integration Service.
2. Click **Applications Installed**.
3. On the **Applications Installed** tab, click the BlackBerry® MDS Runtime Application that you want to make available again.
4. In the lower pane, click **Application Management**.

5. Click **Reinstate Application**.
6. Click **Yes**.

Removing BlackBerry MDS Runtime Applications and BlackBerry Browser Applications

If you want to prevent users from accessing a BlackBerry® MDS Runtime Application or BlackBerry® Browser Application, you can remove the application from the BlackBerry MDS Application Repository and from BlackBerry devices.

Make a BlackBerry MDS Runtime Application unavailable for installation

Remove a BlackBerry® MDS Runtime Application from the BlackBerry MDS Application Repository if you want to prevent users from discovering and installing the application using the BlackBerry MDS Control Center on their BlackBerry devices.

1. In the BlackBerry Manager, in the left pane, expand a BlackBerry MDS Integration Service.
2. Click **Application Registry**.
3. On the **Application Registry** tab, click the BlackBerry MDS Runtime Application that you want to remove.
4. In the lower pane, click **Application Management**.
5. Click **Delete Application**.
6. Click **Yes**.

After you finish: If you remove a BlackBerry MDS Runtime Application from the BlackBerry MDS Application Repository, the application still runs on the BlackBerry devices that it is installed on. If you do not want users to use an installed BlackBerry MDS Runtime Application, remove the application from the users' BlackBerry devices.

Remove an installed BlackBerry MDS Runtime Application from BlackBerry devices

1. In the BlackBerry® Manager, in the left pane, click a user group.
2. On the **View** menu, click **Choose Columns**. Add the **MDS Integration Service Server URL** column.
3. Click the **MDS Integration Service Server URL** column heading.
4. Click the users that are connected to the same BlackBerry MDS Integration Service.
5. On the **Group Configuration** tab, click **MDS Services**.
6. Click **Uninstall on Device**.
7. Click **Next**.
8. Click the BlackBerry® MDS Runtime Application that you want to remove.
9. In the **Group size for pushing** field, type the number of BlackBerry devices that you want to send the removal request to at the same time.

10. In the **Push interval (minute)** field, type an interval for the BlackBerry MDS Integration Service to send the removal request to BlackBerry devices.
11. To set a specific date to send the removal request on, click the **Schedule** check box. Specify the start date and end date.
12. Click **Next**.
13. Click **Finish**.

Remove an installed BlackBerry MDS Runtime Application from a specific BlackBerry device

1. In the BlackBerry® Manager, in the left pane, expand a BlackBerry MDS Integration Service.
2. Click **Applications Installed**.
3. On the **Applications Installed** tab, click the BlackBerry® MDS Runtime Application that you want to remove.
4. In the lower pane, click **Device Management**.
5. Click **Uninstall on Device**.
6. In the **Uninstall application on devices** drop-down list, click **with application installed**.
7. Clear the **Select all** check box.
8. Click the PIN of the BlackBerry device that you want to remove the application from.
9. Click **Next**.
10. To set a specific time to send the removal request, click the **Schedule** check box. Specify the start date and end date.
11. Click **Next**.
12. Click **Finish**.

Configuring a new connection between a BlackBerry MDS Integration Service and a BlackBerry MDS Connection Service

You can make a local or remote BlackBerry® MDS Connection Service available to a BlackBerry MDS Integration Service in the same BlackBerry Domain. You can make multiple instances of the BlackBerry MDS Connection Service available to the same BlackBerry MDS Integration Service.

You cannot use a proxy server to exchange data between a BlackBerry MDS Connection Service and a BlackBerry MDS Integration Service; a direct HTTP connection is required. You must configure your organization's BlackBerry MDS Connection Service proxy rules with the correct host name to use a direct connection to the BlackBerry MDS Integration Service.

Related topics

Configure multiple BlackBerry Enterprise Server instances to use the same BlackBerry MDS Integration Service, 26

Make a BlackBerry MDS Connection Service available to a BlackBerry MDS Integration Service

You can make a BlackBerry® MDS Connection Service available to any BlackBerry MDS Integration Service in the same BlackBerry Domain.

Before you begin: The BlackBerry MDS Connection Service that you specify must have a fully qualified domain name or IP address. The BlackBerry MDS Connection Service cannot use localhost or 127.0.0.1.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Integration Service.
2. On the **MDS Integration Services** tab, click **Edit Properties**.
3. In the left pane, click **Connection Service**.
4. Double-click **BlackBerry MDS Connection Service Definition**.
5. Click **New**.
6. Double-click **URL**.
7. Type the full web address or domain name and the port number of the BlackBerry MDS Connection Service.
8. Click **OK**.

Make a BlackBerry MDS Connection Service unavailable to a BlackBerry MDS Integration Service

If you want to prevent a BlackBerry® MDS Integration Service from accessing a BlackBerry MDS Connection Service, you can remove the BlackBerry MDS Connection Service from the list available to the BlackBerry MDS Integration Service.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Integration Service.
2. On the **MDS Integration Services** tab, click **Edit Properties**.
3. In the left pane, click **Connection Service**.
4. Double-click **BlackBerry MDS Connection Service Definition**.
5. Click the web address for a BlackBerry MDS Connection Service.
6. Click **Remove**.
7. Click **OK**.

Managing how users access enterprise applications and web content

20

Restricting user access to content on web servers

You can prevent users from accessing specific web servers using the BlackBerry® Browser or applications on their 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.

Restrict requests for content on web servers from BlackBerry devices

Turn on pull authorization for the BlackBerry® MDS Connection Service to restrict the web addresses that users can request when connecting to the Internet or your organization's intranet from their BlackBerry devices.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. In the left pane, click **Access Control**.
4. Click **Pull Authorization**.
5. In the drop-down list, click **True**.
6. Click **OK**.

Users cannot access web content on their BlackBerry devices until you allow access to certain web servers using pull rules.

After you finish: To allow users to access certain web servers, specify allowed web address patterns and assign them to a pull rule, and then assign the pull rule to a user or user 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 then 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 allowed or restricted on BlackBerry devices. After you create a pull rule, you must assign it to user accounts or user groups.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. In the left pane, click **Access Control**.

4. Double-click **URL Patterns**.
5. Click **New**.
6. Double-click **URL pattern**.
7. Type the web address pattern of the web server that the pull rule controls access to.
8. Click **Service Name**.
9. In the drop-down list, click the service that the web address pattern is bound to.
10. Click **OK**.

After you finish: Create web address patterns that match each web server that you want to allow users to access. Create a pull rule that allows access to web servers that match the web address patterns.

Create a pull rule

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. In the left pane, click **Access Control**.
4. Double-click **Pull Rules**.
5. Click **New**.
6. Double-click **Name**.
7. Type a name for the pull rule.
8. Click **OK**.

After you finish: Assign web address patterns to the pull rule.

Restrict or allow web address patterns using a pull rule

Before you begin: Create a pull rule.

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. In the left pane, click **Access Control**.
4. Double-click **URL Pattern Rules**.
5. In the left pane, click the pull rule that you created.
6. In the right pane, perform any of the following actions:
   - To prevent users from accessing web servers that match a specified web address pattern, select the **Deny** check box.
   - To allow users to access web servers that match a specified web address pattern, select the **Allow** check box.

7. Click **OK**.

After you finish: Assign the pull rule to a user group or to a specific user.

Assign a pull rule to a user group

Before you begin: Create a pull rule. Assign web address patterns to the pull rule.

1. In the BlackBerry® Manager, in the left pane, click a user group.
2. On the **Group Configuration** tab, click **Edit Group Template**.
3. In the left pane, click **Access Control**.
4. Double-click **Pull Rule Set**.
5. Select the check box of the pull rule that you want to assign to the user group.
6. Click **OK**.
7. Select the **Pull Rule Set** check box.
8. Click **Reapply Template**.
9. Click **Yes**.
10. Click **OK**.

Assign a pull rule to a specific user

Before you begin: Create a pull rule. Assign web address patterns to the pull rule.

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. In the left pane, click **Access Control**.
4. Double-click **User Rules**.
5. In the left pane, click a pull rule.
6. In the right pane, click a user.
7. Click **OK**.

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 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), through the BlackBerry® Browser and other applications on the BlackBerry device.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **Media Content Management**.
4. Double-click **Media Content Types**.
5. Click **New**.
6. In the **Media Content Type** field, type the media type and subtype, using standard definitions for MIME media types. Use the format *<type/subtype>*.
7. In the **Disallow content** drop-down list, click **True**.
8. Click **OK**.

Configure a maximum file size for media types

You can configure the BlackBerry® MDS Connection Service to prevent users from accessing specific media file types that exceed a maximum size.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **Media Content Management**.
4. Double-click **Media Content Types**.
5. Click **New**.
6. In the **Media Content Type** field, type the media type and the subtype, using standard definitions for MIME media types. Use the format *<type>/<subtype>*.
7. In the **Maximum KB/Connection** field, type the maximum file size.
8. In the **Disallow content** drop-down list, click **False**.
9. Click **OK**.

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 allow only authenticated push applications to send push requests to applications on BlackBerry® devices.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Click **Access Control**.
4. Click **Push Authentication**.
5. In the drop-down list, click **True**.
6. Click **OK**.

After you finish: To authenticate and allow certain 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 allowed to send push requests to applications on BlackBerry® devices. For push initiators to work, you must have push authentication turned on 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 development environment allows it. Make sure that the authorization HTTP header in push requests from server-side push applications matches the push principal name and password that you specify for the push initiator.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. In the left pane, click **Access Control**.
4. Double-click **Push Initiators**.
5. Click **New**.
6. Double-click **Push Principal Name**.
7. Type the name of the server-side application that you want to allow to send push requests to BlackBerry devices.
8. Double-click **Credentials**.
9. Type the password for the server-side push application.
10. Click **OK**.

After you finish: Create a push initiator for each server-side push application that you want to allow to send push requests to BlackBerry devices. To specify which users can receive push requests from authenticated push applications, turn on push authorization, and then create push rules.

Turn on push authorization

If you turned on push authentication and created push initiators to specify which push applications are permitted to send push requests, you can create push rules to specify which users are allowed to receive authenticated push requests. The BlackBerry® MDS Connection Service can only apply push rules 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 Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Click **Access Control**.
4. Click **Push Authorization**.
5. In the drop-down list, click **True**.
6. Click **OK**.

After you finish: Create a push rule.

Related topics

Restrict push applications from sending data to BlackBerry devices, 138

Create a push rule

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. In the left pane, click **Access Control**.
4. Double-click **Push Rules**.
5. Click **New**.
6. Double-click **Name**.
7. Type a name for the push rule.
8. Click **OK**.

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® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. In the left pane, click **Access Control**.
4. Double-click **Push Initiator Rules**.
5. In the left pane, click a push rule.
6. In the right pane, select the push initiators for the applications that you want to assign to the push rule.
7. Click **OK**.

After you finish: Assign the push rule to users.

Related topics
Create push initiators for push applications, 138

Assign a push rule to a user group

Before you begin:
- Create a push rule.
- Assign push initiators to the push rule.

1. In the BlackBerry® Manager, in the left pane, click a user group.
2. On the **Group Configuration** tab, click **Edit Group Template**.
3. In the left pane, click **Access Control**.
4. Double-click **Push Rule Set**.
5. Select the check box of the push rule that you want to assign to the user group.
6. Click **OK**.
7. Select the **Push Rule Set** check box.
8. Click **Reapply Template**.
9. Click **Yes**.
10. Click **OK**.

Assign a push rule to a specific user

Before you begin:
- Create a push rule.

- Assign push initiators to the push rule.

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. In the left pane, click **Access Control**.
4. Double-click **User Rules**.
5. In the left pane, click a push rule.
6. In the right pane, click a user.
7. Click **OK**.

Encrypt push requests that push applications send to BlackBerry devices

You can configure the 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 Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Click **Access Control**.
4. Click **Push Encryption**.
5. In the drop-down list, click **True**.
6. Click **OK**.

After you finish: To turn off encryption for push requests, in the **Push Encryption** drop-down list, click **False**.

Associate a push initiator with the BlackBerry MDS Integration Service

You can specify the push initiator that you want the BlackBerry® MDS Integration Service to use to communicate with the BlackBerry MDS Connection Service.

Before you begin:

- Turn on push authentication to restrict the push applications that can send push requests to BlackBerry devices.
- Create a push initiator for the BlackBerry MDS Integration Service to communicate with the BlackBerry MDS Connection Service.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Integration Service.
2. On the **MDS Integration Services** tab, click **Edit Properties**.
3. In the left pane, click **Connection Service**.
4. Double-click **BlackBerry MDS Connection Service Definition**.
5. Click **New**.

6. In the left pane, click **Connection Service Details**.
7. Double-click **URL**.
8. Type the full web address or domain name and port number of the BlackBerry MDS Connection Service that is associated with the push initiator.
9. In the **Push Initiator** drop-down list, click the push initiator that you want to associate with the BlackBerry MDS Integration Service.
10. Click **OK**.

Related topics
Create push initiators for push applications, 138

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 Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. In the left pane, click **Push/PAP**.
4. Double-click **Device Ports Enabled for Reliable Pushes**.
5. Type the device port number. To separate multiple port numbers, use commas.
6. Click **OK**.
7. Click **Restart Service**.

Store push application requests in the BlackBerry Configuration Database

To manage memory and system resources in your organization's environment, you can configure the 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 Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Click **Push/PAP**.
4. Click **Store Push Submissions**.
5. In the drop-down list, click **True**.
6. Click **OK**.
7. Click **Restart Service**.

After you finish: Configure the settings for storing push requests in the BlackBerry Configuration Database.

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 Manager, in the left pane, click **BlackBerry Domain.**
2. On the **Global** tab, click **Edit Properties**.
3. Click **Push Control**.
4. Double-click **Maximum Stored Push Messages**.
5. Type the maximum number of push requests that you want the BlackBerry Configuration Database to store.
6. Double-click **Maximum Push Message Age**.
7. 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.
8. Click **OK**.
9. Click **Restart Service**.

Configure the maximum number of active connections that the BlackBerry MDS Connection Service can process

You can configure the maximum number of push connections that the 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 Manager, in the left pane, click a BlackBerry MDS Connection Service.

2. On the **Connection Service** tab, click **Edit Properties**.
3. Click **Push/PAP**.
4. Double-click **Maximum number of Active Connections**.
5. Type a number.
6. Click **OK**.
7. Click **Restart Service**.

Configure the maximum number of queued connections that the 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 the BlackBerry MDS Connection Service can queue. The BlackBerry MDS Connection Service sends a "service unavailable" message to BlackBerry devices for pending push connections that exceed this limit.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Click **Push/PAP**.
4. Double-click **Maximum number of Queued Connections**.
5. Type a number.
6. Click **OK**.
7. Click **Restart Service**.

Delete requests from the push request queue manually

An automated process runs daily to delete outstanding requests from the push request queue on a Microsoft® SQL Server®. To delete requests from the push request queue manually, you can run the RIMPurgeMDSMsg<*database_name*> process from the Microsoft SQL Server management console.

1. Perform one of the following actions:
   - If you use the Microsoft SQL Server Enterprise Manager, navigate to Console Root\Microsoft SQL Servers\SQL Server Group\<*BlackBerry_Configuration_Database_server*>\Management\SQL Server Agent\Jobs.
   - If you use the Microsoft SQL Server Management Studio, navigate to SQL Server Agent\Jobs.
2. Start the RIMPurgeMDSMsg<*database_name*> process.

Monitoring a BlackBerry Domain 21

How the BlackBerry Controller monitors the BlackBerry Enterprise Server components

The BlackBerry® Controller detects when activity stops and restarts the appropriate BlackBerry® Enterprise Server services, which enables the BlackBerry Enterprise Server to continue to run in the event of nonresponsive threads or inactive services.

The BlackBerry Controller monitors the following BlackBerry Enterprise Server components:

- BlackBerry Attachment Service
- BlackBerry Collaboration Service
- BlackBerry Instant Messaging Connector for Microsoft® Office Live Communications Server
- BlackBerry Dispatcher
- BlackBerry MDS Connection Service
- BlackBerry MDS Integration Service
- BlackBerry Messaging Agent
- BlackBerry Policy Service
- BlackBerry Router
- BlackBerry Synchronization Service

Changing how the BlackBerry Controller monitors the BlackBerry Enterprise Server components and restarts services

Registry keys determine how the BlackBerry® Controller monitors the BlackBerry® Enterprise Server components and restarts the associated services. You can change the default behavior of the BlackBerry Controller by creating new registry keys and changing the default values.

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 Dump application that is included in the Microsoft® OEM Support Tools.

1. On the computer that hosts the BlackBerry® Enterprise Server, open the 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. Click **Controller**.
4. Perform any of the following tasks:

Task	Steps
Change how the BlackBerry Controller restarts the BlackBerry Messaging Agent.	a. Create a DWORD value that is named **RestartAgentsOnCrash**. b. Double-click the new DWORD value. c. In the **Value data** field, type **0**.
Change the maximum number of times that the BlackBerry Messaging Agent restarts daily.	a. Create a DWORD value that is named **MaxAgentRestartsPerDay**. b. Double-click the new DWORD value. c. In the **Value data** field, type a value. The default maximum number of restarts that can occur daily is 10.
Change the maximum number of missed health checks that can occur before the BlackBerry Messaging Agent restarts.	a. Create a DWORD value that is named **WaitToRestartAgentOnHung**. b. Double-click the new DWORD value. c. In the **Value data** field, type a value that is greater than 4. This provides the BlackBerry Controller sufficient time to monitor thread health checks before it restarts the BlackBerry Messaging Agent. The default value is 6. Health checks occur every 10 minutes. If the health check does not receive a response from the thread that is being monitored, 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
Prevent the BlackBerry Controller from restarting the BlackBerry Messaging Agent when a nonresponsive thread occurs.	a. Create a DWORD value that is named **WaitToRestartAgentOnHung**. b. Double-click the new DWORD value. c. In the **Value data** field, type **0**.

Task	Steps
	The default value is 6.
Prevent the BlackBerry Controller from restarting the BlackBerry Messaging Agent for a specified time range if it detects a nonresponsive thread.	a. Create a DWORD value that is named **RestartAgentOnHungBlackoutFrom**. b. In the Properties for the new DWORD value, in the **Base** section, select the **Decimal** option. c. Double-click the new DWORD value. d. In the **Value data** field, type the lower boundary of the time range. The values range from 0 to 23, where 0 is 12:00 AM and 23 is 11:00 PM. e. Create a DWORD value that is named **RestartAgentOnHungBlackoutTo**. f. In the Properties for the new DWORD value, in the **Base** section, select the **Decimal** option. g. Double-click the new DWORD value. h. In the **Value data** field, type the upper boundary of the time range. For example, if the RestartAgentOnHungBlackoutFrom value is set to 8 and the RestartAgentOnHungBlackoutTo value is set 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, change the **RestartAgentOnHungBlackoutFrom** and **RestartAgentOnHungBlackoutTo** value fields to **0**.
Restart the BlackBerry Messaging Agent without creating a user.dmp file when the BlackBerry Controller detects nonresponsive threads.	a. Create a DWORD value that is named **RestartAgentOnHung**. b. Double-click the new DWORD value. c. In the **Value data** field, type **0**. The default value is 1. If you changed the default value for the **WaitToRestartAgentOnHung** DWORD value, that value takes precedence over the **RestartAgentOnHung** value.
Change the maximum number of user.dmp files that are created daily for each BlackBerry Enterprise Server	a. Create a DWORD value that is named **MaxUserDumpPerDay**. b. Double-click the new DWORD value. c. In the **Value data** field, type a value. The default value is 3.

Task	Steps
before the BlackBerry Controller restarts the BlackBerry Messaging Agent.	
Change the number of 10-minute intervals that the BlackBerry Controller waits for a successful health check before it restarts the BlackBerry Messaging Agent.	a. Create a DWORD value that is named **MissedHeartbeatThreshold**. b. Double-click the new DWORD value. c. In the **Value data** field, type a value. The default value is 2. If you set the MissedHeartbeatThreshold value to 3, the BlackBerry Controller waits for 30 minutes before it restarts the BlackBerry Messaging Agent.
Prevent the BlackBerry Messaging Agent from restarting if the BlackBerry Controller does not receive health checks from it.	a. Create a DWORD value that is named **MissedHeartbeatThreshold**. b. Double-click the new DWORD value. c. In the **Value data** field, type **0**.

5. Click **OK**.

Change how the BlackBerry Controller restarts the BlackBerry Enterprise Server services

By default, the BlackBerry® Controller restarts the BlackBerry® Enterprise Server services if they stop responding.

1. On the computer that hosts the BlackBerry Enterprise Server component that you want to change, open the 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. Click **Controller**.
4. Perform any of the following tasks:

Task	Steps
Prevent the BlackBerry Dispatcher from restarting if it stops responding.	a. Create a DWORD value that is named **RestartDispatcherOnCrash**. b. Double-click the new DWORD value. c. In the **Value data** field, type **0**. The default value is 1.

Task	Steps
Prevent the BlackBerry Policy Service from restarting if it stops responding.	a. Create a DWORD value that is named **RestartPolicyServerOnCrash**. b. Double-click the new DWORD value. c. In the **Value data** field, type **0**. The default value is 1.
Prevent the BlackBerry Router from restarting if it stops responding.	a. Create a DWORD value that is named **RestartRouterOnCrash**. b. Double-click the new DWORD value. c. In the **Value data** field, type **0**. The default value is 1.
Prevent the BlackBerry Synchronization Service from restarting if it stops responding.	a. Create a DWORD value that is named **RestartSyncServerOnCrash**. b. Double-click the new DWORD value. c. In the **Value data** field, type **0**. The default value is 1.
Prevent the BlackBerry MDS Connection Service from restarting if it stops responding.	a. Create a DWORD value that is named **RestartMDSOnCrash**. b. Double-click the new DWORD value. c. In the **Value data** field, type **0**. The default value is 1.
Prevent the BlackBerry MDS Integration Service from restarting if it stops responding.	a. Create a DWORD value that is named **RestartMDSServicesOnCrash**. b. Double-click the new DWORD value. c. In the **Value data** field, type **0**. The default value is 1.
Prevent the BlackBerry Attachment Service from restarting if it stops responding.	a. Create a DWORD value that is named **RestartAttachmentServerOnCrash**. b. Double-click the new DWORD value. c. In the **Value data** field, type **0**. The default value is 1.
Prevent the BlackBerry Collaboration Service from restarting if it stops responding.	a. Create a DWORD value that is named **RestartBBIMOnCrash**. b. Double-click the new DWORD value. c. In the **Value data** field, type **0**. The default value is 1.

Task	Steps
Prevent the BlackBerry Instant Messaging Connector for the Microsoft® Office Live Communications Server from restarting if it stops responding.	a. Create a DWORD value that is named **RestartLCSOnCrash**. b. Double-click the new DWORD value. c. In the **Value data** field, type **0**. The default value is 1.

5. Click **OK**.

Monitoring the BlackBerry MDS Integration Service notification messages

You can monitor the message traffic between the BlackBerry® MDS Integration Service and BlackBerry devices, and the message traffic that BlackBerry® MDS Runtime Applications generate. An excessive number of messages from a specific BlackBerry MDS Runtime Application or messages of a specific type might indicate that a problem exists with a BlackBerry device, a BlackBerry MDS Runtime Application, or the web services.

Set up monitoring of the BlackBerry MDS Integration Service notification messages for a BlackBerry device

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Integration Service.
2. On the **MDS Integration Services** tab, click **Edit Properties**.
3. Click **Message Monitors**.
4. Double-click **BlackBerry MDS Integration Service Monitor Definition**.
5. Click **New**.
6. In the **PIN** field, type the PIN of the BlackBerry device that you want to monitor.
7. In the **Application** drop-down list, click the BlackBerry MDS Runtime Application that you want to monitor.
8. Click **OK**.

If you restart the BlackBerry MDS Integration Service, you must re-create your message monitors.

Monitor the BlackBerry MDS Integration Service notification messages for a BlackBerry device

Before you begin: To monitor the notification messages, you must set up monitoring of the BlackBerry® MDS Integration Service notification messages for a BlackBerry device.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Integration Service.

2. Click **Monitor Messages**.
3. On the **Monitor Messages** tab, in the **Device** field, type the PIN of the BlackBerry device that you want to view notification messages for.
4. In the **Application** drop-down list, click the BlackBerry MDS Runtime Application that you want to monitor.
5. To monitor the traffic between the BlackBerry MDS Integration Service and a BlackBerry device, click **Search**.

Filter the BlackBerry MDS Integration Service notification messages by date and time

Before you begin: To filter the notification messages, you must set up monitoring of the BlackBerry® MDS Integration Service notification messages for a BlackBerry device.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Integration Service.
2. Click **Monitor Messages**.
3. On the **Monitor Messages** tab, type the PIN of the BlackBerry device that you want to filter notification messages for.
4. In the **Application** drop-down list, click the application.
5. In the **Start time** drop-down list, click the date.
6. Click the numbers in the time field and use the arrow buttons to set the time in hours, minutes, and seconds.
7. To set a date and time after which messages are not displayed, in the **End time** field, select the check box.
8. In the **End time** drop-down list, click the date.
9. Click the numbers in the time field and use the arrow buttons to set the time in hours, minutes, and seconds.
10. Click **Search**.

Block notification messages from a web services host

You can create filters to block the BlackBerry® MDS Integration Service notification messages if web services hosts send the notification messages too frequently. When you create a filter for a specific host, the BlackBerry MDS Integration Service does not process or send the notification messages from that web services host to the BlackBerry® Enterprise Server and the BlackBerry devices.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Integration Service.
2. On the **BlackBerry MDS Integration Services** tab, click **Edit Properties**.
3. Click **Filters**.
4. Double-click the **Filters** field.
5. Click **New**.
6. In the **Host/Address** field, type the name of the web services host (for example, *<hostname>.<domain>*), or the IP address of the web services host.
7. Click **OK**.

After you finish: To permit notification messages from a blocked web services host, delete the filter.

Remove all notification messages for the BlackBerry MDS Integration Service

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Integration Service.
2. Click **Monitor Messages**.
3. On the **Monitor Messages** tab, click **Clear**.

Monitoring PIN messages, SMS text messages, and calls

Change the default location for the PIN message, SMS text message, and phone log files

CAUTION: The PIN message, SMS text message, and phone log files store confidential information in plain-text format. To protect the information, you must limit read and write controls to the location of the log files.

By default, the log files are stored in the root directory that is defined in the BlackBerry® Configuration Database. You can choose to store the log files in a location that is different from where the BlackBerry® Enterprise Server component log files are stored.

1. In the BlackBerry Manager, in the left pane, click the name of the BlackBerry Enterprise Server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. Click **Sync Server**.
4. Double-click **Audit Root Directory**.
5. Type the absolute path to the location where you want to save the log files.
6. Click **OK**.

Monitor PIN messages

You use the log files for PIN messages to monitor the time and frequency at which users send PIN messages from their BlackBerry® devices. By default, the logging of PIN messages is turned off. The log files are named using the format PINLog_<*yyyymmdd*>.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click a policy.
6. Click **Properties**.
7. Click **PIM Synchronization Policy Group**.
8. Click **Disable PIN Messages Wireless Synchronization**.

9. In the drop-down list, click **False**.
10. Click **OK**.
11. On the computer that hosts the BlackBerry Synchronization Service, in the Windows® Services, restart the BlackBerry Synchronization Service.

After you finish: To turn off the logging of PIN messages, change the value for **Disable PIN Messages Wireless Synchronization** to **True**.

Monitor SMS text messages

You use the log files for SMS text messages to monitor the time and the frequency at which users send SMS text messages from their BlackBerry® devices. By default, the logging of SMS text messages is turned off. The log files are named using the format SMSLog_*yyyymmdd*.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click a policy.
6. Click **Properties**.
7. Click **PIM Synchronization Policy Group**.
8. Click **Disable SMS Messages Wireless Synchronization**.
9. In the drop-down list, click **False**.
10. Click **OK**.
11. On the computer that hosts the BlackBerry Synchronization Service, in the Windows® Services, restart the BlackBerry Synchronization Service.

After you finish: To turn off the logging of SMS messages, change the value for **Disable SMS Messages Wireless Synchronization** to **True**.

Turn off call logging

You use the call log files to monitor the time and frequency at which users make calls from their BlackBerry® devices. By default, the logging of calls is turned on. The log files are named using the format PhoneCallLog_<*yyyymmdd*>.csv.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.

5. Click a policy.
6. Click **Properties**.
7. Click **PIM Synchronization Policy Group**.
8. Click **Disable Phone Call Log Wireless Synchronization**.
9. In the drop-down list, click **True**.
10. Click **OK**.
11. On the computer that hosts the BlackBerry Synchronization Service, in the Windows® Services, restart the BlackBerry Synchronization Service.

After you finish: To turn on the logging of calls, change the value for **Disable Phone Call Log Wireless Synchronization** to **False**.

Log files for the BlackBerry Enterprise Server components

The BlackBerry Enterprise Server creates a log file for each BlackBerry® Enterprise Server component and saves the log files in *<drive>*:\Program Files\Research In Motion\BlackBerry Enterprise Server\Logs. The BlackBerry Enterprise Server component writes the log files to folders that are created daily and organized by date.

By default, the log files are named *<server_name>_<component_identifier>_<instance>_<yyyymmdd>_<log_number>*.txt (for example, BBServer01_MAGT_01_20070120_0001.txt). An event that is written to a log file uses a five-digit number, where the first digit represents the logging level. For example, the following log file entry indicates that level 3, informational level events, are being logged: **[30000]** (03/12 14:03:42.315):{0x18CC} [ENV] Computer Host Name: *host name-VM4*.

Changing where the BlackBerry Enterprise Server components write log files

Change the location where the BlackBerry Enterprise Server components write log files

1. On the computer that hosts the BlackBerry® Manager, on the taskbar, click **Start > Programs > BlackBerry Enterprise Server > BlackBerry Server Configuration**.
2. Click the **Logging** tab.
3. Click **Browse**.
4. Browse to a location on a local drive where you want to save the log files.
5. Click **OK**.
6. On the computers that host the BlackBerry® Enterprise Server components that you changed, in the Windows® Services, restart the BlackBerry Enterprise Server services.

Store all of the BlackBerry Enterprise Server component log files in one folder

You can store all of the BlackBerry® Enterprise Server component log files in one folder instead of organizing the folders by date.

1. On the computer that hosts the BlackBerry Manager, on the taskbar, click **Start** > **Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. Click the **Logging** tab.
3. Clear the **Create daily log folder** check box.
4. Click **OK**.
5. On the computers that host the BlackBerry Enterprise Server components that you changed, in the Windows® Services, restart the BlackBerry Enterprise Server services.

Changing how the BlackBerry Enterprise Server components create log files

Add a prefix to the file names of all the BlackBerry Enterprise Server component log files

1. On the computer that hosts the BlackBerry® Manager, on the taskbar, click **Start** > **Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. Click the **Logging** tab.
3. In the **Log file prefix** field, type a prefix.
4. Click **OK**.
5. On the computers that host the BlackBerry® Enterprise Server components that you changed, in the Windows® Services, restart the BlackBerry Enterprise Server services.

Configure the maximum size for a BlackBerry Enterprise Server component log file

If you turned on the Debug log auto-roll feature, a new log file is created when the log file size reaches the maximum. If you did not turn on the Debug log auto-roll feature, the existing file is overwritten when the log file size reaches the maximum.

1. On the computer that hosts the BlackBerry® Manager, on the taskbar, click **Start** > **Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. Click the **Logging** tab.
3. In the **BlackBerry Service Log Settings** pane, click **Debug log size** for the BlackBerry® Enterprise Server component that you want to set the log file size for.
4. Type a value in MB for the maximum log file size.
5. Click **OK**.
6. On the computers that host the BlackBerry Enterprise Server components that you changed, in the Windows® Services, restart the appropriate BlackBerry Enterprise Server services.

Change the logging level for a BlackBerry Enterprise Server component

You can change the logging level for a BlackBerry® Enterprise Server component to write more detailed information to the log files, or to minimize the amount of information that is written to the log files.

1. On the computer that hosts the BlackBerry Manager, on the taskbar, click **Start** > **Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. Click the **Logging** tab.
3. In the **BlackBerry Service Log Settings** pane, click **Debug log level** for the BlackBerry Enterprise Server component that you want to change the logging level for.
4. In the **Setting** column, double-click the current value.
5. In the drop-down list, click one of the following logging levels:
   - **1: Error**: This level logs error messages to the log files.
   - **2: Warning**: This level logs warning messages to the log files.
   - **3: Information**: This level logs daily activities to the log files.
   - **4: Debug**: This level logs additional information to the log files that can help you troubleshoot issues in the BlackBerry Enterprise Server environment.
   - **5: Verbose**: This level logs all events that are associated with a BlackBerry Enterprise Server component to the log files.
6. Click **OK**.
7. On the computers that host the BlackBerry Enterprise Server components that you changed, in the Windows® Services, restart the appropriate BlackBerry Enterprise Server services.

Create a new BlackBerry Enterprise Server component log file when the current log file reaches the maximum size

1. On the computer that hosts the BlackBerry® Manager, on the taskbar, click **Start** > **Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. Click the **Logging** tab.
3. In the **BlackBerry Service Log Settings** pane, click **Debug log auto-roll** for the BlackBerry® Enterprise Server component that you want to change.
4. In the **Setting** column, double-click the current value.
5. In the drop-down list, click **Yes**.
6. Click **OK**.
7. On the computers that host the BlackBerry Enterprise Server components that you changed, in the Windows® Services, restart the appropriate BlackBerry Enterprise Server components.

Change the identifier for a BlackBerry Enterprise Server component log file

1. On the computer that hosts the BlackBerry® Manager, on the taskbar, click **Start** > **Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. Click the **Logging** tab.
3. In the **BlackBerry Service Log Settings** pane, click **Debug log identifier** for the BlackBerry® Enterprise Server component that you want to change.
4. In the **Setting** column, double-click the current value.
5. Type a new identifier name for the BlackBerry Enterprise Server component log file.
6. Click **OK**.
7. On the computers that host the BlackBerry Enterprise Server components that you changed, in the Windows® Services, restart the appropriate BlackBerry Enterprise Server components.

Prevent a BlackBerry Enterprise Server component from creating a daily log file

1. On the computer that hosts the BlackBerry® Manager, on the taskbar, click **Start** > **Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. Click the **Logging** tab.
3. In the **BlackBerry Service Log Settings** pane, click **Debug daily log file** for the BlackBerry® Enterprise Server component that you want to change.
4. In the **Setting** column, double-click the current value.
5. In the drop-down list, click **No**.
   The log file name does not include the date.
6. Click **OK**.
7. On the computers that host the BlackBerry Enterprise Server components that you changed, in the Windows® Services, restart the appropriate BlackBerry Enterprise Server components.

Configure when to delete BlackBerry Enterprise Server component log files

1. On the computer that hosts the BlackBerry® Manager, on the taskbar, click **Start** > **Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. Click the **Logging** tab.
3. In the **BlackBerry Service Log Settings** pane, click **Debug log maximum daily file age** for the BlackBerry® Enterprise Server component that you want to change.
4. In the **Setting** column, double-click the current value.
5. Type the number of days after which you want to delete the BlackBerry Enterprise Server component log files.

6. Click **OK**.
7. On the computers that host the BlackBerry Enterprise Server components that you changed, in the Windows® Services, restart the appropriate BlackBerry Enterprise Server components.

Changing how the BlackBerry MDS Connection Service creates a log file

Change the logging level for the BlackBerry MDS Connection Service

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Double-click **Logs**.
4. Click **Destination**.
5. In the **File** section, click **Log Level**.
6. In the drop-down list, click one of the following logging levels:
   - **1: Error**: This level logs error messages to the log files.
   - **2: Warning**: This level logs warning messages to the log files.
   - **3: Information**: This level logs daily activities to the log files.
   - **4: Debug**: This level logs additional information to the log files that can help you troubleshoot the BlackBerry MDS Connection Service.
7. Click **OK**.

Change the location where the BlackBerry MDS Connection Service writes log files

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Double-click **Logs**.
4. Click **Destination**.
5. In the **File** section, double-click **Location**.
6. Browse to a location on a local drive where you want to save the log files.
7. Click **OK**.

Change the interval at which the BlackBerry MDS Connection Service writes information to the log file

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Connection Service.

2. On the **Connection Service** tab, click **Edit Properties**.
3. Double-click **Logs**.
4. Click **Destination**.
5. In the **File** section, double-click **Log Timer Interval**.
6. Type the interval value in milliseconds.
   The default value is 30000.
7. Click **OK**.

Change the logging level for the UDP log file

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Double-click **Logs**.
4. Click **Destination**.
5. In the **UDP** section, double-click **Log Level**.
6. In the drop-down list, click the level of logging that you want to write to the UDP log file.
7. Click **OK**.

Change the port number that the BlackBerry MDS Connection Service connects to when sending UDP log file messages

The SNMP agent for the BlackBerry® Enterprise Server receives UDP log file messages on the same port number that the BlackBerry MDS Integration Service connects to when sending UDP log messages.

1. In the BlackBerry Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Double-click **Logs**.
4. Click **Destination**.
5. In the **UDP** section, click **Location**.
6. Type the host name and port number using the format *<hostname>:<portnumber>*.
7. Click **OK**.

Change the logging level for the TCP log file

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Double-click **Logs**.

4. Click **Destination**.
5. In the **TCP** section, click **Log Level**.
6. Click the logging level that you want to use.
7. Click **OK**.

Change the port number that the BlackBerry MDS Connection Service connects to when sending TCP log file messages

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Double-click **Logs**.
4. Click **Destination**.
5. In the **TCP** section, double-click **Location**.
6. Type the host name and port number using the format *<hostname>:<portnumber>*.
7. Click **OK**.

Change the logging level for the Event log file

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. Double-click **Logs**.
4. Click **Destination**.
5. In the **EventLog** section, click **Log Level**.
6. Click the logging level that you want to use.
7. Click **OK**.

Change which BlackBerry MDS Connection Service activities are written to the log file

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry MDS Connection Service.
2. On the **Connection Service** tab, click **Edit Properties**.
3. In the left pane, click **Logs**.
4. Perform any of the following tasks:

Task	Steps
Monitor activity at the SRP network layer.	a. Click **SRP logging enabled**. b. In the drop-down list, click **True**.
Monitor activity at the IPPP network layer.	a. Click **IPPP logging enabled**. b. In the drop-down list, click **True**.
Monitor activity at the UDP network layer.	a. Click **UDP logging enabled**. b. In the drop-down list, click **True**.
Monitor activity at the GME network layer.	a. Click **GME logging enabled**. b. In the drop-down list, click **True**.
Monitor HTTP headers for response messages that are sent from the web server when users retrieve content from the Internet and intranet on their BlackBerry devices.	a. Click **HTTP logging enabled**. b. In the drop-down list, click **True**.
Monitor HTTP headers and the body of response messages that are sent from the web server when users retrieve content from the Internet and intranet on their BlackBerry devices.	a. Click **Verbose HTTP logging enabled**. b. In the drop-down list, click **True**.
Monitor encrypted data that the BlackBerry device and the origin web server send between them using TLS.	a. Click **TLS logging enabled**. b. In the drop-down list, click **True**.
Monitor the certificate revocation status that the BlackBerry device retrieves from the OCSP server.	a. Click **OCSP logging enabled**. b. In the drop-down list, click **True**.
Monitor requests from the BlackBerry device to access a user profile or certificate from the LDAP directory.	a. Click **LDAP logging enabled**. b. In the drop-down list, click **True**.
Monitor CRLs that the BlackBerry device retrieves from the CRL server.	a. Click **CRL logging enabled**. b. In the drop-down list, click **True**.
Monitor PGP® key status and revocation information that the BlackBerry device retrieves from the PGP server.	a. Click **PGP logging enabled**. b. In the drop-down list, click **True**.

5. Click **OK**.

Change which BlackBerry Collaboration Service activities are written to the log file

1. In the BlackBerry® Manager, in the left pane, click a BlackBerry Collaboration Service.
2. On the **Collaboration Service** tab, click **Edit Properties**.
3. In the left pane, click **Logs**.
4. Perform any of the following tasks:

Task	Steps
Do not monitor activity at the BlackBerry instant messaging network layer.	a. Click **BBIM logging enabled**. b. In the drop-down list, click **False**.
Do not monitor activity at the SRP network layer.	a. Click **SRP logging enabled**. b. In the drop-down list, click **False**.
Monitor activity at the GME network layer.	a. Click **GME logging enabled**. b. In the drop-down list, click **True**.

5. Click **OK**.

Managing a BlackBerry Domain

22

Managing multiple BlackBerry Domain instances

You can manage a different BlackBerry® Domain by connecting the BlackBerry Manager to the BlackBerry Configuration Database for that BlackBerry Domain.

Connect the BlackBerry Manager to a different BlackBerry Domain

1. In the BlackBerry® Manager, on the **Tools** menu, click **Options**.
2. In the left pane, click **Database**.
3. Double-click **Database Server Name**.
4. Type the name of the database server that the BlackBerry Configuration Database is located on.
5. Double-click **Database Name**.
6. Type the BlackBerry Configuration Database name.
7. In the **Authentication** drop-down list, click an authentication type.
8. In the **Log Database Calls** drop-down list, click **True**.
9. Click **OK**.
10. Close the BlackBerry Manager.
11. Open the BlackBerry Manager.

Managing CAL keys

CAL keys control how many user accounts can exist on a BlackBerry® Enterprise Server at the same time. When you exceed the number of licensed user accounts, the BlackBerry Manager informs you that you require more CAL keys.

If you use a temporary evaluation version of a CAL key and the CAL key expires, the BlackBerry Dispatcher turns off automatically, stopping all synchronization between the BlackBerry Enterprise Server and BlackBerry devices. You must purchase a new CAL key before you can restart the BlackBerry Dispatcher. If you use a temporary evaluation CAL key, you cannot reuse that CAL key after you purchase a permanent CAL key.

To help you transfer CAL keys to computers in other BlackBerry Domain instances, or to troubleshoot CAL key issues, you can copy the CAL keys from the BlackBerry Manager to a text file.

Add or delete a CAL key

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Account**.
3. Click **License Management**.
4. Perform one of the following actions:
   - To add a CAL key, type the new information for the license key. Click **Add License**.
   - To delete a CAL key, right-click the license key that you want to delete. Click **Remove License Key**.
5. Click **Close**.

Copy a license key to a text file

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Account**.
3. Click **License Management**.
4. Right-click a license key. Click **Copy Key**.
5. Open a text editor.
6. Paste the CAL key into the file.
7. Save the file.

Glossary

23

AES
Advanced Encryption Standard

ASCII
American Standard Code for Information Interchange

BCC
blind carbon copy

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 CAL
A BlackBerry® Client Access License (BlackBerry CAL) limits how many users you can add to a BlackBerry® Enterprise Server.

CMIME
Compressed Multipurpose Internet Mail Extensions

CRL
certificate revocation list

DES
Data Encryption Standard

DOM
Document Object Model

GAL
Global Address List

GME
The gateway message envelope (GME) 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.

HTML
Hypertext Markup Language

HTTP
Hypertext Transfer Protocol

HTTPS
Hypertext Transfer Protocol over Secure Sockets Layer

IPPP
Internet Protocol Proxy Protocol

LAN
local area network

LDAP
Lightweight Directory Access Protocol

LTPA
Lightweight Third-Party Authentication

messaging server

MIME
Multipurpose Internet Mail Extensions

NTLM
NT LAN Manager

OCSP
Online Certificate Status Protocol

PAP
Push Access Protocol

PIM
personal information management

PIN
personal identification number

S/MIME
Secure Multipurpose Internet Mail Extensions

SMS

Short Message Service

SNMP
Simple Network Management Protocol

SRP
Server Routing Protocol

SSL
Secure Sockets Layer

TCP
Transmission Control Protocol

TLS
Transport Layer Security

Triple DES
Triple Data Encryption Standard

UDP
User Datagram Protocol

Legal notice

24

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.

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

Research In Motion UK Limited
Centrum House
36 Station Road
Egham, Surrey TW20 9LF
United Kingdom

Published in Canada