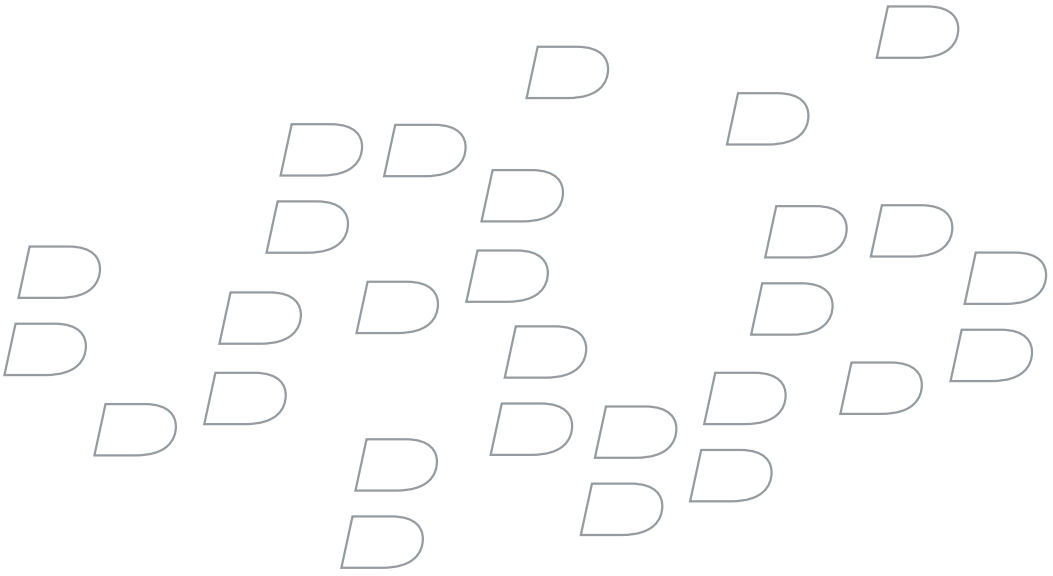

PGP Support Package for BlackBerry Devices

User Guide Supplement

BlackBerry 8707h Smartphone

PGP Support Package for BlackBerry Devices User Guide Supplement

Last modified: 28 June 2007

Document ID: 12063712-001

At the time of publication, this documentation is based on PGP Support Package for BlackBerry devices Version 4.2.2.

Send us your comments on product documentation: https://www.blackberry.com/DocsFeedback.

third-party. You are solely responsible for determining whether such third-party licenses are required and are responsible for acquiring any such licenses relating to Third-Party Information. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use Third-Party Information until all such applicable licenses have been acquired by you or on your behalf. Your use of Third-Party Information shall be governed by and subject to you agreeing to the terms of the Third-Party Information licenses. Any Third-Party Information that is provided with RIM's products and services is provided "as is". RIM makes no representation, warranty or guarantee whatsoever in relation to the Third-Party Information and RIM assumes no liability whatsoever in relation to the Third-Party Information even if RIM has been advised of the possibility of such damages or can anticipate such damages.

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

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

Published in Canada

Contents

1

PGP Support Package for BlackBerry devices installation

About the PGP Support Package for BlackBerry devices

The PGP® Support Package for BlackBerry devices is designed to permit you to send PGP messages from—and receive PGP messages on—your BlackBerry® device, if you are already sending PGP messages from and receiving PGP messages on your computer. The PGP Support Package for BlackBerry devices supports OpenPGP messages and, if your BlackBerry device is integrated with an account that uses BlackBerry Enterprise Server Version 4.1.2 or later, PGP/MIME messages.

PGP Support Package for BlackBerry devices prerequisites

- Verify that you have installed the BlackBerry® Desktop Software on your computer. The installer for the PGP® Support Package for BlackBerry devices uses components from the BlackBerry Device Software.
- Verify that you have installed and configured the PGP Universal™ Satellite or PGP Desktop client on your computer. Refer to the PGP documentation to determine the correct version for your configuration.
- Verify that you have obtained the installer for the PGP Support Package for BlackBerry devices from PGP Corporation or an authorized PGP reseller.
- Verify that your BlackBerry Enterprise Server supports the PGP Support Package for BlackBerry devices.

Install the PGP Support Package for BlackBerry devices on your computer

1. Double-click the installer for the PGP® Support Package for BlackBerry® devices.
2. Complete the instructions on the screen.

Install the PGP Support Package for BlackBerry devices on your BlackBerry device

1. Connect your BlackBerry® device to your computer.
2. On the taskbar, click **Start** > **Programs** > **BlackBerry** > **Desktop Manager**.
3. Double-click the **Application Loader** icon.
4. Click **Next**.
5. Select the **BlackBerry PGP Support Package** check box.

6. Click **Next**.
7. Click **Finish**.

Enroll with the PGP Universal Server

1. After your BlackBerry® device has completed enterprise activation, at the prompt, click **Enroll Now**.
2. Type your email address or domain login information.
3. Click **OK**.
4. Click **OK** again.
5. To download PGP keys from the PGP Universal™ Server, click **Yes**.
6. Type the pass phrase to decrypt your private key.
7. Click **OK**.

Related topic

Legal notice (See page 29.)

2

PGP keys

About PGP keys

A PGP® key might contain several cryptographic keys, including a parent key to verify signatures and one or more subkeys to encrypt messages. PGP keys are generated in pairs, with a public key and a private key.

A PGP public key binds the identity and the public cryptographic information of the PGP public key user. A PGP public key is required to verify and encrypt messages. PGP public keys are shared and are accessible by both message senders and recipients.

A PGP private key is required to sign and decrypt messages. Private key information is never publicly available.

You can generate a PGP key using the PGP Universal™ Server or PGP Desktop client. If you generate the PGP key using the PGP Universal Server, the PGP Universal Server signs the key to verify that the key is trusted.

A PGP key might also contain an X.509 certificate, which is used to verify and encrypt Secure Multipurpose Internet Mail Extensions (S/MIME) messages. If you use the PGP Universal Server and you have installed the S/MIME Support Package for BlackBerry devices, you can use these certificates to send and receive S/MIME messages through the PGP Universal Server. Certificates that you obtain from PGP keys are stored in the key store and appear in the Certificates screen.

Related topics

About PGP key icons (See page 10.)

About digital signatures and encryption (See page 19.)

About the key store (See page 14.)

About PGP key icons

The following icons indicate the status of PGP® keys stored on your BlackBerry® device:

- **Key**: The PGP key has a corresponding private key on your device.
- **Check mark**: The PGP key is trusted, the PGP key revocation status is good, and the PGP key is valid.
- **Question mark**: The revocation status of the PGP key is unknown or the key is weak.
- **X**: The PGP key is not trusted, revoked, expired, not yet valid, or could not be verified.

Related topics

Check the status of a PGP key (See page 11.)

Download an updated PGP key (See page 11.)

Download a personal PGP key from the PGP Universal Server

1. In the device options, click **Security Options**.
2. Click **PGP**.
3. Click the trackwheel.
4. Click **Download Keys**.
5. Type your key store password.
6. Click **OK**.
7. Type the pass phrase to decrypt your private key.
8. Click **OK**.

Related topics

About PGP keys (See page 9.)

Send a PGP key to a contact (See page 12.)

Download another person's PGP key

1. In the device options, click **Security Options**.
2. Click **PGP keys**.
3. Click the trackwheel.
4. Click **Fetch PGP Keys**.
5. Select a Lightweight Directory Access Protocol (LDAP) server.
6. Type PGP® key subject information in one or more of the **First Name**, **Last Name**, or **Email** fields.
7. Click the trackwheel.
8. Click **Search**.
9. Click a PGP key.
10. Click **Add PGP Key to Key Store**.
11. Type your key store password.
12. Click **OK**.

Notes:

A selected check box beside a PGP key indicates that the PGP key is downloaded and stored in the key store on your BlackBerry® device.

If you use the PGP Universal™ Server, you might not be able to download PGP keys from an LDAP server.

Related topics

About PGP keys (See page 9.)

Set options for checking the status of a PGP key (See page 12.)

I cannot download another person's PGP key from an LDAP server (See page 15.)

Find PGP key information

1. In the device options, click **Security Options**.
2. Click **PGP keys**.
3. Click a PGP® key.
4. Click **Details**.

Related topics

PGP key information fields (See page 11.)

Find PGP subkey information (See page 11.)

Find PGP subkey information

1. In the device options, click **Security Options**.
2. Click **PGP keys**.
3. Click a PGP® key.
4. Click **Details**.
5. Click **View Subkey**.

Related topics

PGP key information fields (See page 11.)

Find PGP key information (See page 10.)

PGP key information fields

- **Revocation Status**: The status of the PGP® key at a specified date and time.
- **Trust Status**: How the PGP key is trusted.
  - **Explicitly Trusted**: The PGP key itself is trusted.
  - **Implicitly Trusted**: A private key on your BlackBerry® device corresponds with the PGP key.
  - **Not Trusted**: The PGP key is not explicitly trusted and does not chain to a trusted PGP key on your device, and a chain of digital signatures to a trusted key does not exist.
- **Creation Date**: The date the key was generated.
- **Expiration Date**: The expiration date that is set by the PGP Universal™ Server.
- **Email Address**: The email address associated with the key. Multiple Email Address fields might appear.
- **Public Key Type**: The standard to which the public key complies. Your device supports Rivest Shamir Adleman (RSA), Digital Signature Algorithm (DSA), and Diffie-Hellman (DH) keys.
- **Key Usage**: Approved uses for the key.
- **Fingerprint**: The PGP key fingerprint in hexidecimal format.

Related topics

About PGP keys (See page 9.)

Find PGP key information (See page 10.)

Find PGP subkey information (See page 11.)

Check the status of a PGP key

1. In the device options, click **Security Options**.
2. Click **PGP Keys**.
3. Highlight a PGP® key.
4. Click the trackwheel.
5. Click **Fetch Status**.

Related topics

About PGP key icons (See page 10.)

Download an updated PGP key (See page 11.)

Download an updated PGP key

1. In the device options, click **Security Options**.
2. Click **PGP Keys**.
3. Highlight a PGP® key.
4. Click the trackwheel.
5. Click **Fetch Updated PGP Key**.

Related topics

About PGP keys (See page 9.)

About PGP key icons (See page 10.)

Check the status of a PGP key (See page 11.)

Set a PGP key to trusted

1. In the device options, click **Security Options**.
2. Click **PGP Keys**.
3. Highlight an untrusted PGP® key.
4. Click the trackwheel.
5. Click **Trust**.

Related topics

About PGP keys (See page 9.)

About PGP key icons (See page 10.)

Set a PGP key to not trusted (See page 12.)

Set a PGP key to not trusted

1. In the device options, click **Security Options**.
2. Click **PGP Keys**.
3. Highlight a trusted PGP® key.
4. Click the trackwheel.
5. Click **Distrust**.

Related topics

About PGP keys (See page 9.)

Revoke a PGP key (See page 13.)

Delete a PGP key (See page 13.)

Send a PGP key to a contact

1. In the device options, click **Security Options**.
2. Click **PGP Keys**.
3. Highlight a PGP® key.
4. Click the trackwheel.
5. Click **Send via Email** or **Send via PIN**.

Note:

When you send a PGP key, only the public key is sent and not the private key.

Related topic

Import a PGP key from a message (See page 20.)

Set options for checking the status of a PGP key

1. In the device options, click **Security Options**.
2. Click **PGP keys**.
3. Click the trackwheel.
4. Click **Fetch PGP Keys**.
5. Click the trackwheel.
6. Click **Options**.
7. Perform one of the following actions:
   - To always check the status of a PGP® key when you add it to the key store, set the **Fetch Status** field to **Yes**.
   - To be prompted to check the status of a PGP key when you add it to the key store, set the **Fetch Status** field to **Prompt**.
   - To never check the status of a PGP key when you add it to the key store, set the **Fetch Status** field to **No**.
8. Click the trackwheel.
9. Click **Save**.

Related topics

About the key store (See page 14.)

Check the status of a PGP key (See page 11.)

Use the common name when adding a PGP key to the key store

The common name is the name set for the key when it is generated. You can use the common name as a label for the key on your BlackBerry® device or you can set the label to one that has more meaning to you.

1. In the device options, click **Security Options**.

2. Click **PGP keys**.
3. Click the trackwheel.
4. Click **Fetch PGP Keys**.
5. Click the trackwheel.
6. Click **Options**.
7. Set the **Prompt for Label** field to **Yes**.
8. Click the trackwheel.
9. Click **Save**.

Related topics

Change the display name for a PGP key (See page 13.)

Add a contact when adding a PGP key to the key store (See page 14.)

Change the display name for a PGP key

1. In the device options, click **Security Options**.
2. Click **PGP keys**.
3. Highlight a PGP® key.
4. Click the trackwheel.
5. Click **Change Label**.
6. Type a new PGP key label.
7. Click **OK**.

Related topic

Use the common name when adding a PGP key to the key store (See page 12.)

Revoke a PGP key

1. In the device options, click **Security Options**.
2. Click **PGP Keys**.
3. Highlight a PGP® key.
4. Click the trackwheel.
5. Click **Revoke**.
6. Click **Yes**.
7. Press the **Space** key to set the **Reason** field to the appropriate revocation reason.
8. Click **OK**.

Note:

Other options that do not apply to your support package might appear in the dialog box.

Related topics

Revocation reasons (See page 13.)

Set a PGP key to not trusted (See page 12.)

Delete a PGP key (See page 13.)

Revocation reasons

- **Unknown**: The reason is unspecified.
- **Superseded**: A new PGP® key is replacing an existing PGP key.
- **Key Compromise**: A person who is not the key subject might have discovered the private key value.
- **Key Retired**: The PGP key is no longer used.
- **User ID Invalid**: The user information is no longer valid.

Related topic

Revoke a PGP key (See page 13.)

Delete a PGP key

1. In the device options, click **Security Options**.
2. Click **PGP keys**.
3. Highlight a PGP® key.
4. Click the trackwheel.
5. Click **Delete**.

Related topics

Revoke a PGP key (See page 13.)

Set a PGP key to not trusted (See page 12.)

Add a contact when adding a PGP key to the key store

You can add new contacts from PGP® keys to your address book automatically when you add a PGP key to the BlackBerry® device key store.

1. In the device options, click **Security Options**.
2. Click **Key Stores**.
3. Set the **Key Store Address Injector** field to **Enabled**.
4. Click the trackwheel.
5. Click **Save**.

Related topic

About the key store (See page 14.)

Set the service used to download PGP keys

Verify that your system administrator has provided you with the service record for the BlackBerry Mobile Data System™ (BlackBerry MDS™) Connection Service that your BlackBerry® device uses to download PGP® keys.

1. In the device options, click **Security Options**.
2. Click **Key Stores**.
3. Set the **Certificate Service** field to the correct service record.
4. Click the trackwheel.
5. Click **Save**.

Related topic

Download another person's PGP key (See page 10.)

About the key store

The key store on your BlackBerry® device stores the following items:

- Personal PGP® keys (public and private key pairs)
- PGP public keys downloaded from a Lightweight Directory Access Protocol (LDAP) server
- PGP public keys imported from a message
- Secure Multipurpose Internet Mail Extensions (S/MIME) certificates downloaded from an LDAP server
- S/MIME certificates imported from a message

The key store is protected by a key store password. Your device might prompt you to set the key store password the first time that you open the key store. You might need to type this password when adding items to or deleting items from the key store, or when an application tries to access your private key to sign or decrypt a message.

Related topics

Download a personal PGP key from the PGP Universal Server (See page 10.)

Download another person's PGP key (See page 10.)

Change the key store password

1. In the device options, click **Security Options**.
2. Click **Key Stores**.
3. Click the trackwheel.
4. Click **Change Password**.

Related topics

About the key store (See page 14.)

Set how long your key store password is remembered (See page 15.)

Set how long your key store password is remembered

After a password timeout occurs, you must type your password to access private keys.

1. In the device options, click **Security Options**.
2. Click **Key Stores**.
3. Set the **Private Key Password Timeout** field.
4. Click the trackwheel.
5. Click **Save**.

Related topics

About the key store (See page 14.)

Change the key store password (See page 14.)

Set how frequently the revocation status is refreshed

When your BlackBerry® device stores a PGP® key longer than the time limit specified in the Certificate Status Expires field, your device should download a new revocation status automatically the next time your device uses the PGP key.

1. In the device options, click **Security Options**.
2. Click **Key Stores**.
3. Set the **Certificate Status Expires After** field to the length of time that a revocation status can be stored before your device considers the status to be stale.
4. Click the trackwheel.
5. Click **Save**.

Related topic

Check the status of a PGP key (See page 11.)

Do not back up or restore items in the key store

The Allow Key Store Backup/Restore field determines whether items in the key store are backed up or restored when your BlackBerry® device is backed up or restored. Although the keys are encrypted on your computer, you might want to set this field to No if you do not want your private key backed up to your computer for security reasons.

1. In the device options, click **Security Options**.
2. Click **Key Stores**.
3. Set the **Allow Key Store Backup/Restore** field to **No**.
4. Click the trackwheel.
5. Click **Save**.

Related topic

About the key store (See page 14.)

Shortcuts for viewing PGP key information in the PGP Keys screen

To view the PGP® key label, press the **Space** key.

To view PGP key information, press the **Enter** key.

To view the security level of a private PGP key, press the **Alt** key and **L**.

To view the serial number for a PGP key, press the **Alt** key and **S**.

PGP key troubleshooting

I cannot download another person's PGP key from an LDAP server

I cannot download another person's PGP key from an LDAP server

Try performing the following actions:

- Verify that your organization permits you to download PGP® keys from an LDAP certificate server. For more information, contact your system administrator.
- If you changed the connection type that your BlackBerry® device uses to connect to the LDAP certificate server, try using the default connection type.

Related topic

LDAP certificate server options (See page 17.)

Certificate servers

About certificate servers

Your BlackBerry® device uses Lightweight Directory Access Protocol (LDAP) servers to search for and download PGP® keys.

If you use the PGP Universal™ Server, you might not be able to download PGP keys from an LDAP server.

Related topic

Add a certificate server (See page 17.)

Add a certificate server

1. In the device options, click **Security Options**.
2. Click **Certificate Servers**.
3. Click the trackwheel.
4. Click **New Server**.
5. Set the **Server Type** field.
6. Type the appropriate information for the server.
7. Click the trackwheel.
8. Click **Save**.

Related topics

LDAP certificate server options (See page 17.)

LDAP certificate server options

- **Friendly Name**: Type the common name that is associated with the server.
- **Server Name**: Type the network address of the server.
- **Base Query**: Type the base query information as it is configured in your LDAP server. Content appears in X.509 distinguished name (DN) syntax (for example, o=test.rim.net).
- **Port**: Type the port number as it is configured on your organization's network. The default port number is 389.
- **Authentication Type**: Set whether you require authentication credentials to connect to the server.
- **Connection Type**: Set whether your BlackBerry® device uses Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to connect to the server.

Related topic

Add a certificate server (See page 17.)

Change certificate server information

1. In the device options, click **Security Options**.
2. Click **Certificate Servers**.
3. Highlight a server.
4. Click the trackwheel.
5. Click **Edit**.
6. Edit the appropriate fields.
7. Click the trackwheel.

8. Click **Save**.

Related topics

LDAP certificate server options (See page 17.)

Delete a certificate server

1. In the device options, click **Security Options**.
2. Click **Certificate Servers**.
3. Highlight a server.
4. Click the trackwheel.
5. Click **Delete**.
6. Click **Yes**.

Related topic

Change certificate server information (See page 17.)

Send certificate server information to a contact

1. In the device options, click **Security Options**.
2. Click **Certificate Servers**.
3. Highlight a server.
4. Click the trackwheel.
5. Click **Email Server** or **PIN Server**.

Related topics

Send a PGP key to a contact (See page 12.)

Attach a PGP key to a message (See page 23.)

PGP messages

About digital signatures and encryption

You can digitally sign a message to help the recipient verify the authenticity and integrity of the message. When you digitally sign a message using your private key, the recipient uses your public key to verify that you sent the message and not someone who was pretending to be you, and that no one changed the message before it arrived.

You can encrypt a message to keep the message confidential. When you encrypt a message, your BlackBerry® device uses the recipient's public key to encrypt the message. Only the recipient's private key can decrypt the message and the recipient knows that no one else read the message.

Related topics

About encryption icons (See page 19.)
About signature icons (See page 20.)

About encryption icons

When you open an encrypted message, a lock icon represents the encryption status. Your system administrator sets an IT Policy that determines whether the encryption algorithm that the message uses is considered to be strong or weak.

- **Lock**: The message is strongly encrypted.
- **Lock with a question mark**: The message is weakly encrypted.

Related topic

About signature icons (See page 20.)

About signature icons

When you open a digitally signed message, a ribbon icon represents the verification status of the digital signature.

- **Ribbon with a check mark**: Your BlackBerry® device verified the digital signature.
- **Ribbon with an X**: Your device could not verify the digital signature.
- **Ribbon with a question mark**: Your device requires more data to verify the digital signature.

The icon after the ribbon icon represents the status of the sender's PGP® key.

- **Certificate with a check mark**: The sender's PGP key is trusted.
- **X**: The sender's PGP key cannot be found on your device, is revoked, is not trusted, or cannot be verified, or the sender's email address does not match the email address in the key.
- **Question mark**: Your device requires more data to verify the trust status, or it considers the key status to be stale.
- **Clock**: The sender's PGP key has expired.

Related topic

About encryption icons (See page 19.)

About message classifications

If your BlackBerry® device is integrated with an account that uses BlackBerry Enterprise Server Version 4.1.2 or later and your system administrator turns on message classifications, the BlackBerry Enterprise Server applies a minimum set of security actions to each message that you compose, forward, or reply to, based on the classification that you assign to the message. Your system administrator configures the set of message classifications that you can use.

If you receive a message that uses message classifications, your can view the abbreviated classification in the subject line of the message and the full description of the classification in the body of the message. The abbreviated classification and description also appear in messages in your Sent Items folder.

Related topic

Digitally sign or encrypt an email message (See page 21.)

Download a sender's PGP key

1. In an open PGP® message, highlight the digital signature or trust status icon.
2. Click the trackwheel.
3. Click **Fetch Sender's PGP key**.

Notes:

The Fetch Sender's PGP key menu item appears only if the sender's PGP key is not included in your BlackBerry® device key store or the sender's message.

If you use the PGP Universal™ Server, you might not be able to download the sender's PGP key, or your device might download the sender's key from the PGP Universal Server automatically.

Related topics

Download another person's PGP key (See page 10.)

I cannot add a PGP key to the key store from an email or PIN message (See page 25.)

Import a PGP key from a message

1. In an open message, highlight the digital signature or trust status icon.
2. Click the trackwheel.
3. Click **Import PGP Key**.
4. Type your key store password.

5. Click **OK**.
6. Type a PGP® key label.
7. Click **OK**.

Note:
If you use the PGP Universal™ Server, you might not be able to import PGP keys from messages.

Related topics

Download a sender's PGP key (See page 20.)

Download another person's PGP key (See page 10.)

I cannot add a PGP key to the key store from an email or PIN message (See page 25.)

Import a PGP key from an attachment

1. In an open message, click the PGP® key attachment icon.
2. Click **Retrieve PGP Attachment**.
3. Click the PGP key.
4. Click **Import PGP Key**.

Note:
If you use the PGP Universal™ Server, you might not be able to import PGP keys from message attachments.

Related topics

Download a sender's PGP key (See page 20.)

Download another person's PGP key (See page 10.)

I cannot add a PGP key to the key store from an email or PIN message (See page 25.)

Import certificate server information from a message

1. In an open message, highlight a PGP® server icon.
2. Click the trackwheel.
3. Click **Import Server**.

Note:
If you use the PGP Universal™ Server, you might not be able to import certificate server information from messages.

Related topics

Add a certificate server (See page 17.)

I cannot add a PGP key to the key store from an email or PIN message (See page 25.)

Forward or reply to a PGP message

1. In an open message, click the trackwheel.
2. Click **Forward** or **Reply**.

Related topics

Digitally sign or encrypt an email message (See page 21.)

I cannot see all signing or encryption options (See page 24.)

Digitally sign or encrypt an email message

1. In an unsent message, perform one of the following actions:
   - To apply the default encoding recommended by the PGP Universal™ Server, set the **Encoding** field to **PGP Universal Default**.
   - To attach a digital signature, set the **Encoding** field to **Sign**.
   - To encrypt the message, set the **Encoding** field to **Encrypt**.
   - To attach a digital signature and encrypt the message, set the **Encoding** field to **Sign and Encrypt**.
2. If required, set the **Classification** field.

Note:
If you set the Encoding field to indicate that the message should be encrypted and keys are not available for all recipients, you might be able to send the message to the PGP Universal Server for further processing. In this case, you have the option to click Send to Server.

If you use the PGP Universal Server and your system administrator has specified a minimum set of actions, the PGP Universal Server might encrypt or sign your message even if you did not select these actions.

Related topics

Select your default PGP key (See page 23.)

Select encryption algorithms for PGP messages (See page 23.)

I cannot see all signing or encryption options (See page 24.)

Digitally sign or encrypt a PIN message

In an unsent message, perform one of the following actions:

- To attach a digital signature, set the **Encoding** field to **Sign**.
- To encrypt the message, set the **Encoding** field to **Encrypt**.
- To attach a digital signature and encrypt the message, set the **Encoding** field to **Sign and Encrypt**.

Note:
To send an encrypted personal identification number (PIN) message, the recipient must appear in your contact list with an associated PIN and email address. Your BlackBerry® device uses the email address in your contact list to locate a PGP® key for the recipient.

Related topics

Select your default PGP key (See page 23.)

I cannot see all signing or encryption options (See page 24.)

View an attachment in a signed message

1. In an open message, click the attachment.
2. Click **Open Attachment**.

Related topic

Import a PGP key from an attachment (See page 21.)

Search the message list

1. In a message list, click the trackwheel.
2. Click **Search**.
3. Set the search criteria.
4. Perform one of the following actions:
   - To search only plain text and signed messages, set the **Include Encrypted Messages** field to **No**.
   - To search plain text, signed, and encrypted messages, set the **Include Encrypted Messages** field to **Yes**.
5. Click the trackwheel.
6. Click **Search**.

Note:
If you set the Include Encrypted Messages field to Yes and the security level for your private key is set to medium or high, your BlackBerry® device might prompt you to type your key store password before search results appear.

Related topic

Set how long your key store password is remembered (See page 15.)

Encrypt a PGP message with a pass phrase

For conventional encryption, your BlackBerry® device uses a pass phrase instead of your PGP® key to encrypt the message.

1. In an unsent message, set the **Encoding** field to one that uses encryption.
2. Click the trackwheel.
3. Click **Options**.
4. Set the **Use Conventional Encryption** field to **Yes**.
5. Click the trackwheel.
6. Click **Save**.
7. Type your message.
8. Click the trackwheel.
9. Click **Send**.
10. Type a pass phrase to encrypt the message.
11. Confirm the pass phrase.
12. Click **OK**.

Using a secure method, let the recipient know what the pass phrase is.

Related topics

Select your default PGP key (See page 23.)

Digitally sign or encrypt an email message (See page 21.)

Attach a PGP key to a message

1. In an unsent message, click the trackwheel.
2. Click **Attach PGP Keys**.
3. Highlight a PGP® key.
4. Click the trackwheel.
5. Click **Continue**.

Related topic

Send a PGP key to a contact (See page 12.)

Display small status icons for PGP messages

1. In the device options, click **Security Options**.
2. Click **PGP**.
3. Set the **Message Viewer Icons** field to **Small**.
4. Click the trackwheel.
5. Click **Save**.

Related topics

About encryption icons (See page 19.)

About signature icons (See page 20.)

Select your default PGP key

Your BlackBerry® device uses the default PGP® key to sign messages and to encrypt messages in the Sent folder.

1. In the device options, click **Security Options**.
2. Click **PGP**.
3. Set the **Default Key** field.
4. Click the trackwheel.
5. Click **Save**.

Related topic

Digitally sign or encrypt an email message (See page 21.)

Select encryption algorithms for PGP messages

If a message has multiple recipients, your BlackBerry® device uses the first selected algorithm that all recipients are known to support.

1. In the device options, click **Security Options**.
2. Click **PGP**.
3. Select all content ciphers that you want available for encrypting messages.

4. Click the trackwheel.
5. Click **Save**.

Related topic

Digitally sign or encrypt an email message (See page 21.)

Set the default security options that you use to send messages

Your BlackBerry® device uses the default encoding for contacts to whom you have not previously sent a message.

1. In the device options, click **Advanced Options**.
2. Click **Message Services**.
3. Set the **Default Encoding** field.
4. Click the trackwheel.
5. Click **Save**.

Related topic

About digital signatures and encryption (See page 19.)

Set the default message classification that you use to send messages

Verify that your system administrator has set up message classifications.

Your BlackBerry® device uses the default message classification for contacts to whom you have not previously sent a message.

1. In the device options, click **Advanced Options**.
2. Click **Message Services**.
3. Set the **Default Classification** field.
4. Click the trackwheel.
5. Click **Save**.

Related topic

About message classifications (See page 20.)

Turn off the prompt that appears when you use a PGP key that is not recommended for use

By default, a prompt appears when you try to send a message using a PGP® key that is not recommended for use (for example, a weak or expired PGP key).

1. In the device options, click **Security Options**.
2. Click **PGP**.
3. Set the **Warn about problems with my PGP keys** field to **No**.
4. Click the trackwheel.
5. Click **Save**.

To receive a prompt again, set the **Warn about problems with my PGP keys** field to **Yes**.

PGP message troubleshooting

I cannot see all signing or encryption options

I cannot add a PGP key to the key store from an email or PIN message

I cannot see all signing or encryption options

Try performing one of the following actions:

- Verify that the current message classification supports the signing or encryption options that you want. Try using a different message classification.
- Verify that your message service is configured to support all signing and encryption options.

Related topic

About message classifications (See page 20.)

I cannot add a PGP key to the key store from an email or PIN message

Verify with your system administrator that your configuration permits you to download PGP® keys from an LDAP server.

Memory cleaning

About memory cleaning

Your BlackBerry® device turns on the memory cleaning application automatically when you turn on content protection or when you install the S/MIME Support Package for BlackBerry devices or the PGP® Support Package for BlackBerry devices on your device.

The memory cleaning application on your device is designed to clear sensitive content from memory. Examples of sensitive content include sensitive web content in the browser cache, unencrypted email content, Lightweight Directory Access Protocol (LDAP) authentication passwords, and information from certificate and key searches.

The device memory is designed to be cleared automatically when your device:

- is inserted in the holster
- remains idle for a configured period of time
- is synchronized with your computer
- has its time or time zone changed
- is locked

Set how frequently the memory cleaning application runs

1. In the device options, click **Security Options**.
2. Click **Memory Cleaning**.
3. Perform any of the following actions:
   - To clear the BlackBerry® device memory every time you insert your device in the holster, set the **Clean When Holstered** field to **Yes**.
   - To clear the device memory after your device remains idle for a specified period of time, set the **Clean When Idle** field to **Yes**. Set the **Idle Timeout** field.
4. Click the trackwheel.
5. Click **Save**.

Related topics

About memory cleaning (See page 27.)

Clear the device memory (See page 27.)

Clear the device memory

1. In the device options, click **Security Options**.
2. Click **Memory Cleaning**.
3. In the **Registered Cleaners** section, click an application.
4. Perform one of the following actions:
   - To clear sensitive content for all applications, click **Clean Now**.
   - To clear sensitive content for the highlighted application, click **Clean <Application>**. Click **OK**.

Related topics

About memory cleaning (See page 27.)

Set how frequently the memory cleaning application runs (See page 27.)

View the memory cleaning icon on the Home screen

1. In the device options, click **Security Options**.
2. Click **Memory Cleaning**.
3. Set the **Show Icon on Home Screen** field to **Yes**.
4. Click the trackwheel.
5. Click **Save**.

Related topic

About memory cleaning (See page 27.)

Legal notice

trademark, or copyright licenses in order to avoid infringement of the intellectual property rights of others. Any dealings with Third-Party Information, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third-party. You are solely responsible for determining whether such third-party licenses are required and are responsible for acquiring any such licenses relating to Third-Party Information. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use Third-Party Information until all such applicable licenses have been acquired by you or on your behalf. Your use of Third-Party Information shall be governed by and subject to you agreeing to the terms of the Third-Party Information licenses. Any Third-Party Information that is provided with RIM's products and services is provided "as is". RIM makes no representation, warranty or guarantee whatsoever in relation to the Third-Party Information and RIM assumes no liability whatsoever in relation to the Third-Party Information even if RIM has been advised of the possibility of such damages or can anticipate such damages.