

PGP Support Package

Release 4.1

White Paper

Contents

PGP Support Package	3
System requirements	3
System architecture	3
PGP Universal Server	4
Data transfer process	5
BlackBerry security	5
BlackBerry standard encryption	5
PGP security	5
PGP key types	6
PGP encryption	6
Storing PGP keys	8
PGP Universal Server storage	8
BlackBerry device storage	8
Searching for and validating PGP keys	10
LDAP PGP key servers	10
Searching external LDAP PGP key servers	11
Managing PGP keys	11
View PGP key details	11
Configure PGP key security options	12
Sending PGP protected messages	12
Message signing and encryption options	12
Fetch or import a PGP key from a received PGP protected message	13
Add an external LDAP PGP key server configuration from a received PGP protected message	14
PGP message icons	14
BlackBerry Enterprise Server IT policy rules for PGP	14
Related resources	15

This document describes the PGP Support Package, which is designed to offer extended security features for BlackBerry® devices.

PGP Support Package

The PGP Support Package is designed to provide an OpenPGP® (Request for Comments (RFC) 2440) implementation on the BlackBerry device. The implementation enables users who are already sending and receiving PGP protected messages using their desktop email program to send and receive PGP protected messages using their BlackBerry devices. The PGP Support Package is designed to work with PGP Universal version 2.0.2, with either PGP Universal Satellite version 2.0.2 or PGP Desktop Professional version 9.0.2.

The PGP Support Package includes tools for obtaining PGP keys and transferring them to the BlackBerry device. This means that messages that are encrypted using PGP can also be decrypted and read on the BlackBerry device. Users can sign, encrypt, and send PGP protected messages from their BlackBerry devices. Without the PGP Support Package, the user's BlackBerry device receives PGP protected messages as unreadable cipher text.

Within the PGP Universal Server environment, the PGP Universal Server operates as a network appliance. PGP Universal Server specifies secure email policies designed by the PGP Universal Server administrator. The BlackBerry device with the PGP Support Package installed enforces compliance with those policies for all email messages.

The PGP Support Package includes support for the following:

- PGP Universal Server
- encrypting and decrypting messages, including personal identification number (PIN) messages, verifying digital signatures, and digitally signing outgoing messages
- wireless fetching of PGP keys and PGP key status using either a PGP Universal Server or an external Lightweight Directory Access Protocol (LDAP) PGP key server

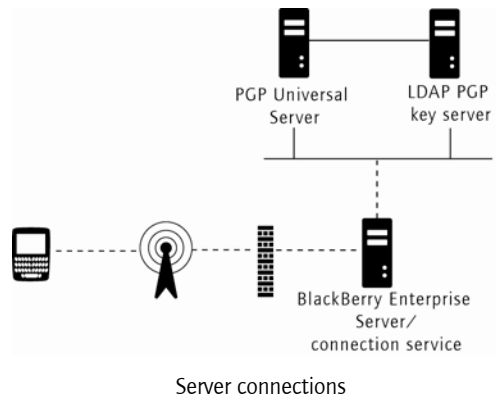
System requirements

The PGP Support Package version 4.1 supports the following messaging and collaboration servers, BlackBerry Enterprise Server software, BlackBerry Device Software, and BlackBerry devices.

Messaging and collaboration servers	BlackBerry Enterprise Server software	BlackBerry devices and BlackBerry device software
<ul style="list-style-type: none"> • Microsoft® Exchange 5.5, 2000 and 2003 Servers • IBM® Lotus® Domino® server version 5.0.3 or later (Research In Motion® (RIM®) recommends using 5.0.12 or later) 	<ul style="list-style-type: none"> • BlackBerry Enterprise Server version 4.0 Service Pack 2 or later for Microsoft Exchange • BlackBerry Enterprise Server version 4.1 for IBM Lotus Domino 	Java™-based BlackBerry devices that are running BlackBerry device software version 4.1 or later Note: Users must load the PGP Support Package on the BlackBerry device.

System architecture

The BlackBerry device is designed to connect to the PGP Universal Server and configured, external LDAP PGP key server(s) using the BlackBerry Mobile Data System™ (BlackBerry MDS™) Connection Service (connection service), which resides on the BlackBerry Enterprise Server®. The connection service uses a standard Internet protocol, such as HTTP or TCP/IP, to enable the BlackBerry device to pull PGP keys and PGP key status from the PGP Universal Server or an external LDAP PGP key server over the wireless network.



PGP Universal Server

The PGP Universal Server enables users to download PGP keys to their BlackBerry devices and verify the authenticity and status of the PGP keys. The BlackBerry device and the PGP Universal Server can use LDAP to search for and download PGP keys.

When a BlackBerry device user enrolls and authenticates with the PGP Universal Server, the following events occur:

- The BlackBerry device enables the user to wirelessly download their PGP keys to their BlackBerry device. The BlackBerry device stores keys in the PGP Key Store and the PGP Universal Key Cache.
- The BlackBerry device automatically fetches the secure email policy and required PGP keys from the PGP Universal Server on demand without additional user interaction.

Enrollment and authentication

When you set the PGP Universal Server Address IT policy rule, the BlackBerry Enterprise Server pushes the PGP Universal Server address to the BlackBerry device, which prompts the BlackBerry device user to enroll with that PGP Universal Server.

By default, the enrollment method requires the BlackBerry device user to send an email message. You can specify the preferred enrollment method (by domain user name and password authentication or by email address authentication) using the PGP Universal Enrollment Method IT policy rule.

Until the user completes the enrollment

- an Enroll with PGP Universal Server menu item appears on the PGP options screen
- the BlackBerry device prompts the user to enroll with PGP Universal Server when either of the following events occurs:
 - the user attempts to send a message from the BlackBerry device
 - the BlackBerry device completes a reset

After the user completes the enrollment, the BlackBerry device stores the long term authentication information included in the enrollment response. If the BlackBerry device resets, the stored authentication information automatically authenticates the BlackBerry device to the PGP Universal Server.

Secure email policy

The BlackBerry device is designed to use the secure email policy from the PGP Universal Server to determine whether to encrypt, sign, or sign and encrypt the messages it sends.

The BlackBerry device fetches the secure email policy data from the PGP Universal Server at a frequency set by the PGP Universal Policy Cache Timeout IT policy rule. By default, the BlackBerry device caches the secure email policy data for a maximum of 24 hours.

PGP key storage and retrieval

When a user sends a PGP protected message from the BlackBerry device, the PGP Universal Server fetches PGP public keys on the user's behalf for the intended message recipients, as needed, and validates the fetched keys before returning them to the user. See "PGP Universal Server storage" on page 8 for more information.

Data transfer process

1. The BlackBerry Enterprise Server pushes the PGP Universal Server Address policy rule to the BlackBerry device.
2. The BlackBerry device prompts the user to enroll with the PGP Universal Server.
3. The BlackBerry device user responds to the prompt and automatically enrolls with the PGP Universal Server.
4. The PGP Universal Server sends an enrollment response to the BlackBerry device.
5. The BlackBerry device stores the long term authentication information included in the enrollment response in the BlackBerry device flash memory.
6. The BlackBerry device refreshes the secure email policy data, if necessary, and then stores that data temporarily.
7. The BlackBerry device uses the secure email policy from the PGP Universal Server to determine how to encode each message. The BlackBerry device encrypts, signs, or signs and encrypts each message based on the minimum security requirements of the secure email policy and any additional security that the BlackBerry device user applies to the message when sending it.
8. The BlackBerry device contacts the PGP Universal Server each time the BlackBerry device user sends or receives a message. The PGP Universal Server obtains the PGP public keys as needed and validates them before returning them to the BlackBerry device user.
9. If the PGP Universal Server cannot provide the PGP keys that the BlackBerry device requests, the BlackBerry device uses the connection service to contact the configured, external LDAP PGP key server(s).

BlackBerry security

The BlackBerry Infrastructure uses symmetric key cryptography to encrypt the data that is sent between the BlackBerry Enterprise Server and the BlackBerry device. BlackBerry standard encryption encrypts data using the Triple Data Encryption Standard (Triple DES) or the Advanced Encryption Standard (AES) algorithm.

BlackBerry standard encryption

Before sending a message, the BlackBerry device compresses the message and then encrypts the message using the master encryption key, which is unique to that BlackBerry device.

When the BlackBerry Enterprise Server receives the message from the BlackBerry device, the BlackBerry Enterprise Server decrypts the message using the BlackBerry device master encryption key and then decompresses the message.

See the *BlackBerry Security White Paper* for more information on standard BlackBerry encryption.

PGP security

If the user has installed the PGP Support Package on their BlackBerry device and completed enrollment with PGP Universal Server, messages that the user sends from the BlackBerry device are encrypted twice: once with PGP encryption and once with standard BlackBerry encryption.

From the time the BlackBerry device user sends a message until the BlackBerry Enterprise Server receives the message, the BlackBerry standard encryption encrypts the message. PGP technology is designed to enable sender-to-recipient authentication and confidentiality and help maintain data integrity and privacy from the time

that the originator of the message sends it over the wireless network until the message is decoded and read by the message recipient.

PGP technology relies on public key cryptography (using private and public key pairs) to provide the following:

- **Confidentiality:** PGP uses encryption to make sure that only the intended recipient can view the contents of the message.
- **Authenticity:** PGP uses digital signatures to permit the message recipient to identify and trust the message sender.
- **Integrity:** PGP uses digital signatures to verify that a third party has not altered the message data.

PGP key types

The PGP implementation of public key cryptography uses the following keys:

Key type	Description
PGP public key	The BlackBerry device uses the PGP public key to encrypt outgoing messages and verify digital signatures on received messages. The PGP public key binds the identity and the public cryptographic information of the PGP public key user. Both message senders and recipients can access the PGP public key (in other words, the PGP public key is shared).
PGP private key	The BlackBerry device uses the PGP private key to digitally sign outgoing messages and decrypt received messages. Private key information is never publicly available.

PGP encryption

If the PGP Support Package is installed on a BlackBerry device, when a BlackBerry device user sends a message, the BlackBerry device encrypts the message once with PGP encryption and once with standard BlackBerry encryption, using the following process:

1. The BlackBerry device encrypts the message with the message recipient's PGP public key.
2. The BlackBerry device uses standard BlackBerry encryption to encrypt the PGP data.
3. The BlackBerry device sends the encrypted data to the BlackBerry Enterprise Server.
4. The BlackBerry Enterprise Server removes the BlackBerry standard encryption and sends the PGP encrypted message to the recipient.

If the PGP Support Package is installed on a BlackBerry device, when the BlackBerry device receives a message, the PGP message is encrypted with standard BlackBerry encryption and then decrypted, using the following process:

1. The BlackBerry Enterprise Server receives the PGP protected message.
2. The BlackBerry Enterprise Server uses standard BlackBerry encryption to encrypt the PGP data.
3. The BlackBerry Enterprise Server sends the encrypted message to the BlackBerry device.
4. The BlackBerry device removes the BlackBerry standard encryption and stores the PGP data.
5. When the BlackBerry device user opens the message, the BlackBerry device decrypts the message and renders the message.

PGP encryption algorithms

RIM recommends using a strong algorithm for PGP encryption. The PGP Allowed Content Ciphers IT policy rule default setting specifies that the BlackBerry device can use any of the supported algorithms to encrypt PGP

messages. You can set the PGP Allowed Content Ciphers IT policy rule to encrypt PGP messages using any of AES (256-bit), AES (192-bit), AES (128-bit), CAST (128-bit), and Triple DES.

The message recipient's PGP key indicates which content ciphers the recipient can support, and the BlackBerry device is designed to use one of those ciphers. The BlackBerry device encrypts the message using Triple DES by default if the recipient's PGP key does not include a list of ciphers.

PGP public keys

When a user sends a message from the BlackBerry device, the BlackBerry device uses the message recipient's PGP public key to encrypt the message.

Recipients can verify the message signature if they have the sender's PGP public key. PGP public keys might contain multiple cryptographic keys, including a parent key that is typically used for digital signature verification, and zero or more subkeys that are typically used for encryption. The PGP parent key signs all of the other information (for example, the user identity information, the subkeys, and expiry information) in a PGP key.

PGP public key strength

The length (size) of a PGP public key determines its encryption strength. The parent key and the subkeys of a PGP public key can have different strengths.

You can configure the encryption key length by setting the minimum Rivest Shamir Adleman (RSA), Digital Signature Algorithm (DSA), and Diffie-Hellman (DH) algorithm key lengths using BlackBerry Enterprise Server IT policy rules. The following table lists the default minimum and maximum key lengths for the supported key generation algorithms.

Algorithm	Default minimum strong key length (bits)	Maximum key length (bits)
RSA	1024	4096
DSA	1024	1024
DH	1024	4096

RIM recommends using a strong PGP public key to protect messages by setting the following IT policy rules to 1024:

- PGP Minimum Strong DH Key Length
- PGP Minimum Strong DSA Key Length
- PGP Minimum Strong RSA Key Length

See "BlackBerry Enterprise Server IT policy rules for PGP" on page 14 for more information.

PGP private keys

When a user sends a message from the BlackBerry device, the BlackBerry device uses the message sender's PGP private key to digitally sign the message.

When a user receives a PGP protected message, the BlackBerry device uses the user's PGP private key to decrypt the message.

PGP private key strength

The public key length and the private key length are the same. The larger the PGP public key and the PGP private key, the stronger the PGP key pair.

Storing PGP keys

PGP Universal Server storage

PGP keys are stored on the PGP Universal Server in one of three ways: client key mode, guarded key mode, or server key mode. The key storage mode impacts the user's access to PGP public keys.

Key storage mode	Description	Impact on BlackBerry device user
server key mode	The PGP Universal Server stores the user's PGP public key and an unencrypted copy of the user's PGP private key.	The BlackBerry device user can download the PGP personal key without a passphrase prompt and automatically import the key into the BlackBerry device key store. The BlackBerry device user is prompted for the key store password when accessing PGP private keys in the key store to digitally sign or decrypt messages.
guarded key mode	The PGP Universal Server stores the user's PGP public key and a passphrase-protected copy of the user's PGP private key. Note: The user creates the passphrase when creating the PGP private key.	The BlackBerry device user can download the PGP public key and PGP private key pair (in other words, the PGP personal key). The BlackBerry device prompts the user for the passphrase to import the PGP personal key into the BlackBerry device key store. The BlackBerry device user is prompted for the key store password when accessing private keys in the key store to digitally sign or decrypt messages.
client key mode	The BlackBerry device user's PGP Desktop software stores and manages the user's PGP private keys. The PGP Universal Server stores only the user's PGP public key.	The BlackBerry device user cannot sign or decrypt messages unless that user exports the PGP private key to a file from the PGP Desktop software and then attaches the PGP private key to a self-addressed message.

The PGP Universal Server administrator can turn on either client key mode or guarded key mode for a BlackBerry device user in the PGP Universal Administration console. See the documentation that PGP Corporation provides for more information.

BlackBerry device storage

The PGP Universal Key Cache (a non-persisted, transient key store on the BlackBerry device) stores PGP public keys that the BlackBerry device fetches from the PGP Universal Server. The PGP Universal Key Cache stores the keys temporarily, for 24 hours, to be fetched again as needed.

The PGP key store, which is part of the BlackBerry device flash memory, stores the following keys:

- PGP public and private key pairs
- PGP public keys that the BlackBerry device fetches from external PGP key server(s) or imports from messages

Key store security

BlackBerry device users must supply the key store password to add and delete PGP public keys and PGP private keys stored on the BlackBerry device.

The BlackBerry device stores a Secure Hash Algorithm (SHA-256) hash of the key store password. The hash of the password is designed to protect the actual key store password by preventing the possibility of an attacker determining the password from the BlackBerry device memory contents. When the user types the key store password, the BlackBerry device performs a one-way hash function on the entered characters using SHA-256, and then compares the hashed input to the stored hashed password.

You can set BlackBerry Enterprise Server IT policy rules to configure the key store password. See the *Policy Reference Guide* for more information.

IT policy rule	Recommendation
Minimum Password Length	Set a key store password that is between 4 and 12 alphanumeric characters in length.
Forbidden Passwords	Specify weak passwords to prevent.
Key Store Password Maximum Timeout	Specify the maximum length of time (0, 1, 2, 5, 10, 20, 30 minutes, or 1 hour) that the key store remains unlocked after the BlackBerry device user types the correct key store password.
Disable Key Store Backup	Configure this policy rule to prevent the back up of PGP private keys in the key store.
Minimal Signing Key Store Security Level	Set to one of the following levels: <ul style="list-style-type: none"> • 2 (high security): The BlackBerry device prompts the user for their key store password each time an application attempts to access their private key • 3 (medium security): The BlackBerry device prompts the user for their key store password when an application attempts to access their private key for the first time or when their private key password timeout expires
Minimal Encryption Key Store Security Level	Set to one of the following levels: <ul style="list-style-type: none"> • 2 (high security): The BlackBerry device prompts the user for their key store password each time an application attempts to access their private key • 3 (medium security): The BlackBerry device prompts the user for their key store password when an application attempts to access their private key for the first time or when their private key password timeout expires

Users can configure additional key store security on their BlackBerry devices (**Security Options > Key Stores**).

Setting	Description
Allow Key Store Backup/Restore	Specify whether to back up and restore PGP keys (private keys and public keys) and symmetric keys in the key store.
Private Key Password Timeout	Specify the maximum amount of time that the key store remains unlocked after the BlackBerry device user types the correct key store password. Note: The value that you specify for this rule cannot be greater than the value that the Key Store Password Maximum Timeout IT policy rule specifies.
Certificate Service	Define the connection service that the PGP key search uses to fetch a PGP key status.
Certificate Status Expires After	Specify the maximum amount of time (1, 2, 4, or 12 hours, 1 day, 1 week, 1 month, or 6 months) for which the PGP key revocation

Setting	Description
	status remains valid.
Change Password	Type a new key store password.

Memory cleaning

The memory cleaning function is designed to remove unreferenced, decrypted content from the BlackBerry device (for example, from the PGP application, key store, content protection and address book caches, PGP key search, and BlackBerry device clipboard).

You can configure the memory cleaning function to run automatically when the

- user synchronizes the BlackBerry device with the desktop computer
- user locks the BlackBerry device
- BlackBerry device locks after a specified amount of idle time
- user changes the time or time zone on the BlackBerry device

Scenario	Recommendation
Remove decrypted content from BlackBerry device memory when the BlackBerry device is holstered.	Set the Force Memory Clean When Holstered policy rule to True.
Remove decrypted content from BlackBerry device memory when the BlackBerry device is idle.	Set the Force Memory Clean When Idle policy rule to True.
Start the memory cleaner after the time specified has elapsed.	Set the Memory Cleaner Maximum Idle Time policy rule to 1 (minute).

See the *Policy Reference Guide* for more information.

Users can configure the memory cleaning function to run when their BlackBerry devices are holstered, or when their BlackBerry devices remain idle for a configured period of time (2, 5, 10, 20, 30 minutes, or 1 hour).

Searching for and validating PGP keys

You must turn on the connection service to enable wireless synchronization of PGP keys and their status from external LDAP PGP key servers.

LDAP PGP key servers

LDAP servers can store information about PGP keys. If the PGP Universal Server cannot provide the BlackBerry device with a user's PGP keys, the BlackBerry device searches for PGP keys on the external LDAP servers that you or the BlackBerry device user configure.

If the PGP Universal Server does not have information about a user's PGP key, that user might not have uploaded the key to the PGP Universal Server, might have revoked the key and uploaded the key to an external LDAP PGP key server, or might have uploaded the key to an external LDAP PGP key server without first revoking the key. The connection service can contact these configured, external LDAP PGP key servers to fetch and verify the authenticity and status of a PGP key.

The BlackBerry device user must manually validate the fingerprint of PGP keys that the BlackBerry device obtains from external LDAP PGP key servers.

Configure an external LDAP server

1. In the BlackBerry Manager, in the left pane, click a BlackBerry Enterprise Server.

2. Click the **Connection Service** tab.
3. Click **Edit Properties**.
4. Click **LDAP**.
5. Set the following fields:

Field	Description
Host Name	Type the name of the default LDAP server.
Port	Type the port on which the default LDAP server listens. Note: If you typed a host name, you must type a port number.
Default Server Base Query	Type the default base query for the default LDAP server. Note: Each LDAP server can host multiple domains but can only search in one domain at a time. You must set a default base query.
Query Limit	Type the maximum number of entries to return for each query.
Enable Data Compression	In the drop-down list, click True to compress results from an LDAP lookup.

See the *BlackBerry Enterprise Server Administration Guide* for more information.

Users can add and configure external LDAP servers from the BlackBerry device. See the *PGP Support Package User Guide Supplement* for more information.

Searching external LDAP PGP key servers

The PGP Support Package includes a PGP key search feature. BlackBerry device users can query configured, external LDAP PGP key servers and download PGP keys from the search results. BlackBerry device users can perform searches based on the PGP key subject's first name, last name, or email address.

PGP key revocation status

Users can perform PGP key revocation status checks from the BlackBerry device when they receive a signed or signed and encrypted message, and before they send a message to the subject of a PGP key. Users can also check the revocation status of a PGP key from the BlackBerry device key store and from the PGP Key Search screen.

The BlackBerry device uses the connection service to request and retrieve either the PGP key revocation status or an updated PGP key (if the PGP key revocation status has expired) from a configured, external LDAP PGP key server. If the BlackBerry device retrieves an updated PGP key, it updates the BlackBerry device key store.

On the BlackBerry device, in the PGP Key Search Options screen, users can set whether they are prompted to fetch the PGP key revocation status when they try to add a PGP key to the BlackBerry device key store.

Managing PGP keys

View PGP key details

To view PGP key details on a BlackBerry device, click **Security Options > PGP keys > Details**.

Detail	Description
Revocation Status	displays the status of the PGP key at a specified date and time
Trust Status	displays the status of the PGP key trust level

	<ul style="list-style-type: none"> • Explicitly trusted: the PGP key is trusted • Implicitly trusted: the PGP key corresponds to a PGP private key on the BlackBerry device or a chain of digital signatures to a trusted key exists • Not trusted: the PGP key is not explicitly trusted, does not correspond to a trusted PGP private key on the BlackBerry device, and a chain of digital signatures to a trusted key does not exist
Fingerprint	displays the PGP fingerprint in hexadecimal format, which the BlackBerry device user can use to validate the authenticity of the PGP public key

Configure PGP key security options

Users can configure PGP key security options on a BlackBerry device (in **Security Options > PGP keys**).

Action	Procedure
Trust the PGP key.	Click Trust .
Remove the trust associated with the PGP key.	Click Distrust .
Invalidate the status of a PGP key.	Click Revoke .
Remove a PGP key from the BlackBerry device key store.	Click Delete .
Send a PGP key in an email message.	Click Send via Email .
Send a PGP key in a PIN message.	Click Send via PIN .
Download the status of the PGP key.	Click Fetch Status .
Download updated PGP keys from an LDAP server.	Click Fetch Updated PGP Key .

See the *PGP Support Package User Guide Supplement* for more information.

Sending PGP protected messages

By default, with the PGP Support Package installed, the BlackBerry device automatically applies the secure email policies designed by the PGP Universal Server administrator to all email that the user sends. The BlackBerry device automatically encrypts, signs, or signs and encrypts messages based on the secure email policy.

If the BlackBerry device cannot retrieve PGP keys for one or more message recipients and the BlackBerry device user sends the message to the PGP Universal Server, the PGP Universal Server can further process the message, using the default secure email policy to determine what action to take on the message. See the documentation that PGP Corporation provides for more information.

You can configure digital signing and encryption options on the BlackBerry device using IT policy. See "BlackBerry Enterprise Server IT policy rules for PGP" on page 14 for more information.

Message signing and encryption options

The PGP Support Package includes digital signing and encryption options that the user can specify on the BlackBerry device when they send a message. When the user selects an option on the BlackBerry device to send an encrypted or signed and encrypted PGP message, one of the following conditions occurs:

- If the BlackBerry device has an appropriate PGP key (in other words, a key that has a strong public key and is trusted, not revoked, and not expired) for the recipient, the BlackBerry device sends the message.
- If the BlackBerry device does not have an appropriate PGP key for the recipient, the BlackBerry device automatically consults the PGP Universal Server (and possibly the user's configured, external LDAP servers) to search for an appropriate key. If the BlackBerry device does not find an appropriate PGP key for the intended recipient, the BlackBerry device prompts the user to do one of the following:

- not send the message
- manually fetch an appropriate PGP key
- send the message in unencrypted form

Manually fetching a PGP key

If the user responds to the BlackBerry device prompt by choosing to manually fetch an appropriate PGP key for the intended recipient, a Certificate Search application appears on the BlackBerry device. The user can refine search parameters in the Certificate Search application before the BlackBerry device attempts to fetch an appropriate PGP key from a configured, external LDAP PGP key server. If it finds an appropriate PGP key, the BlackBerry device sends the message.

Sending a message in unencrypted form

When composing a message, users can select the following options:

- attach PGP keys from the BlackBerry device key store and send the keys as .asc file attachments
- use conventional encryption to encrypt the PGP message with a passphrase
- send the message as plain text

By default, the PGP Support Package permits BlackBerry device users to send and receive plain text email and PIN messages. You can configure BlackBerry Enterprise Server IT policy rules to prevent users enabled for PGP from sending plain text messages.

Scenario	Recommendation
Force all PGP-enabled users to send signed, encrypted, or signed and encrypted PGP email messages.	Set the Disable Message Normal Send IT policy rule to True. Warning: If you apply this IT policy rule, you might overrule secure email policy settings configured on the PGP Universal Server.
Force all PGP-enabled users to send signed, encrypted, or signed and encrypted PGP PIN messages.	Set the Disable Peer-to-Peer Normal Send IT policy rule to True. Warning: If you apply this IT policy rule, you might overrule secure email policy settings configured on the PGP Universal Server.

See the *PGP Support Package User Guide Supplement* for more information.

Fetch or import a PGP key from a received PGP protected message

1. On the BlackBerry device, in the messages list, click a received PGP protected message.
2. Perform one of the following actions:

Action	Procedure
Retrieve a PGP key from the external LDAP PGP key server. (The sender's PGP key is not on the recipient's BlackBerry device and is not included in the message.)	> Click Fetch Sender's PGP Key .
Add the sender's PGP key to the BlackBerry device. (The sender's PGP key is included in the message but not in the recipient's BlackBerry device key store.)	> Click Import PGP Key .

See the *PGP Support Package User Guide Supplement* for more information.
















Add an external LDAP PGP key server configuration from a received PGP protected message

Import the LDAP PGP key server attachment included in the message to configure a new, external LDAP PGP key server (in **Security Options > Certificate Servers**).

1. On the BlackBerry device, in the messages list, click a received PGP protected message.
2. Click **Import Server**.

PGP message icons

PGP protected messages appear in the messages list. The messages appear with security icons that represent additional information about the validity of the source and the confidentiality of the content.

Icon	Description
	The message is strongly encrypted.
	The message is weakly encrypted.
	The BlackBerry device has verified the message signature.
	The BlackBerry device could not verify the message signature.
	The BlackBerry device requires more data to verify the message signature.
	Please wait for the operation to finish.
	The PGP key is trusted.
	The trust status of the PGP key is unknown.
	There was an error determining the trust status of the PGP key.
	The PGP key has expired.
	The PGP key has been revoked or is not trusted.
	A PGP key is included in the message.
	Several PGP keys are included in the message.
	The message contains an LDAP server attachment.
	A PGP key is attached to the message.

BlackBerry Enterprise Server IT policy rules for PGP

The following BlackBerry Enterprise Server IT policy rules apply only to BlackBerry devices on which the PGP Support Package is installed. Verify that any IT policy rules you configure using the BlackBerry Manager are not in conflict with your secure email policy on the PGP Universal Server.

IT policy rule	Description
PGP Allowed Content Ciphers	specifies the content ciphers that the BlackBerry device can use to

IT policy rule	Description
	encrypt PGP messages
PGP Blind Copy Address	specifies an email address that is added as a BCC recipient to all outgoing PGP encrypted messages
PGP Force Digital Signature	specifies whether all outgoing PGP messages are digitally signed Warning: If you apply this IT policy rule, you might overrule secure email policy settings configured on the PGP Universal Server.
PGP Force Encrypted Messages	specifies whether all outgoing PGP messages are encrypted Warning: If you apply this IT policy rule, you might overrule secure email policy settings configured on the PGP Universal Server.
PGP Minimum Strong DH Key Length	specifies the minimum DH key size, in bits, that you consider strong, for use with PGP
PGP Minimum Strong DSA Key Length	specifies the minimum DSA key size, in bits, that you consider strong, for use with PGP
PGP Minimum Strong RSA Key Length	specifies the minimum RSA key size, in bits, that you consider strong, for use with PGP
PGP Universal Enrollment Method	specifies the method by which BlackBerry device users must enroll with the PGP Universal Server
PGP Universal Policy Cache Timeout	specifies the maximum amount of time, in hours, that the BlackBerry device caches the PGP Universal Server policy before fetching it from the PGP Universal Server again
PGP Universal Server Address	specifies the URL of a PGP Universal Server

See the *Policy Reference Guide* for more information.

Related resources

Guide	Information
<i>BlackBerry Enterprise Server System Administration Guide</i>	<ul style="list-style-type: none"> generating and changing master encryption keys enabling encryption managing security
<i>BlackBerry Security White Paper</i>	<ul style="list-style-type: none"> preventing the decryption of information at an intermediate point between the BlackBerry device and the BlackBerry Enterprise Server or company Local Area Network (LAN) managing security settings for all BlackBerry devices protecting data in transit between the BlackBerry device and BlackBerry Enterprise Server. understanding the algorithms provided by the RIM cryptographic application programming interface (Crypto API) understanding the Transport Layer Security (TLS) and Wireless Transport Layer Security (WTLS) standards that the RIM Crypto API currently supports understanding the memory scrub process that occurs on the BlackBerry device when content protection is

Guide	Information
	enabled
<i>Policy Reference Guide</i>	<ul style="list-style-type: none">• using BlackBerry Enterprise Server IT policies
<i>PGP Support Package User Guide Supplement</i>	<ul style="list-style-type: none">• installing the PGP Support Package• managing PGP keys on the BlackBerry device• setting PGP options for digitally signing and encrypting messages• sending and receiving PGP protected messages

Part number: SWD_X_BES(EN)-162.002

© 2005 Research In Motion Limited. All rights reserved. The BlackBerry and RIM families of related marks, images and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, 'Always On, Always Connected', BlackBerry, and BlackBerry Enterprise Server are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

IBM, Lotus, and Domino are either registered trademarks or trademarks of International Business Machines Corporation in the United States, other countries, or both. Java is either a registered trademark or trademark of Sun Microsystems, Inc. in the United States or other countries. Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. PGP is either a registered trademark or trademark of PGP Corporation in the United States and other countries. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

The BlackBerry device and, or associated software are protected by copyright, international treaties, and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in various countries around the world. Visit www.rim.com/patents.shtml for a current list of RIM [as hereinafter defined] patents.

This document is provided "as is" and Research In Motion Limited and its affiliated companies ("RIM") assume no responsibility for any typographical, technical, or other inaccuracies in this document. RIM reserves the right to periodically change information that is contained in this document; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this document to you in a timely manner or at all. RIM MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR COVENANTS, EITHER EXPRESS OR IMPLIED (INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, MERCHANTABILITY, DURABILITY, TITLE, OR RELATED TO THE PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE REFERENCED HEREIN OR PERFORMANCE OF ANY SERVICES REFERENCED HEREIN). IN CONNECTION WITH YOUR USE OF THIS DOCUMENTATION, NEITHER RIM NOR ITS RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, OR CONSULTANTS SHALL BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER BE THEY DIRECT, ECONOMIC, COMMERCIAL, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR INDIRECT DAMAGES, EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF BUSINESS REVENUE OR EARNINGS, LOST DATA, DAMAGES CAUSED BY DELAYS, LOST PROFITS, OR A FAILURE TO REALIZE EXPECTED SAVINGS.

This document might contain references to third-party sources of information, hardware or software, products or services and, or third-party web sites (collectively the "Third-Party Information"). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third-Party Information. The inclusion of Third-Party Information in this document does not imply endorsement by RIM of the Third-Party Information or the third-party in any way. Installation and use of Third-Party Information with RIM products and services may require one or more patent, 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 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.

Certain features outlined in this document require a minimum version of BlackBerry Enterprise Server software and/or BlackBerry Device Software and may require use of specific models of BlackBerry devices, additional development or third party products and/or services for access to corporate applications.