

April 2006

---

# PGP<sup>®</sup> Support Package for BlackBerry<sup>®</sup>

PGP Universal<sup>™</sup> 2.0

BlackBerry Enterprise Server<sup>™</sup> for Microsoft  
Exchange 4.1

Administrator's Guide  
Version 1.3



## Table of Contents

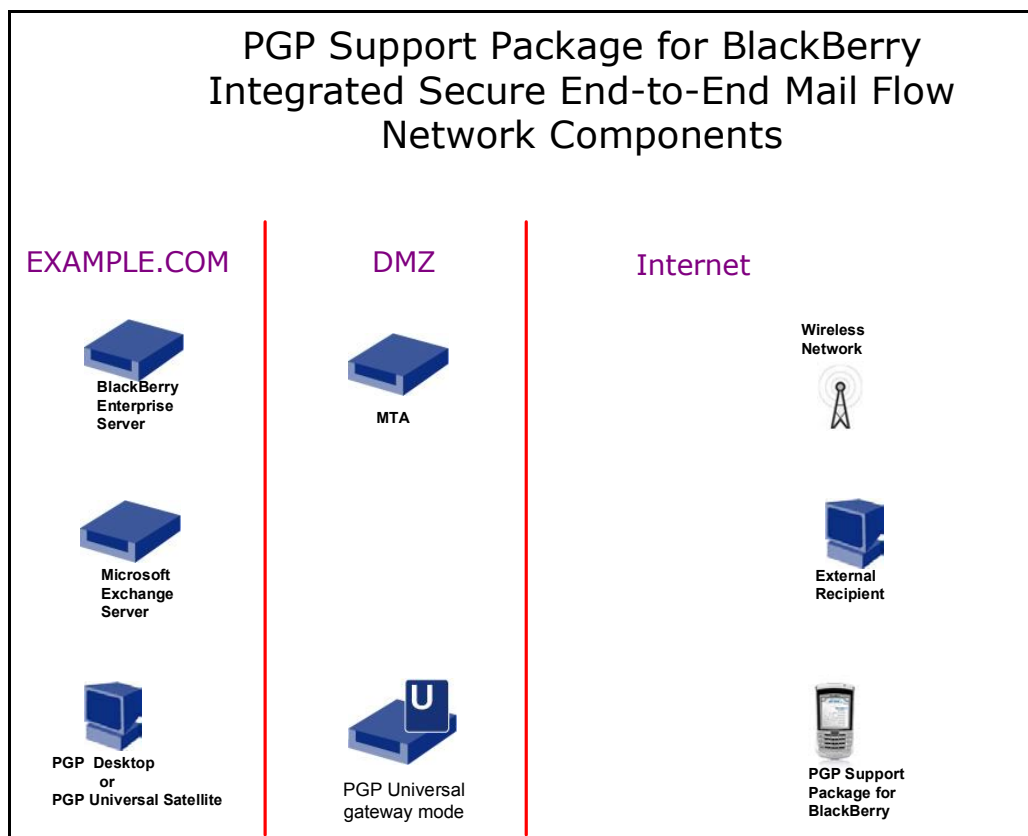
<b>INTRODUCTION</b> .....	<b>3</b>
<b>DESIGN &amp; REQUIREMENTS</b> .....	<b>3</b>
PGP UNIVERSAL ARCHITECTURE & SETUP REQUIREMENTS.....	4
CONFIGURATION REQUIREMENTS.....	4
TRANSACTIONS.....	5
<b>POLICY CONSIDERATIONS &amp; BLACKBERRY ENTERPRISE SERVER SETUP</b> .....	<b>6</b>
DEFAULT POLICY ATTRIBUTES.....	6
EDITING IT POLICIES.....	7
ENABLE BLACKBERRY ENTERPRISE SERVER SECURE EMAIL SUPPORT.....	9
MOBILE DATA SERVICE LDAP SETTINGS.....	10
PUSHING POLICY TO THE HANDHELD.....	11
ENFORCING POLICY TO MULTIPLE RECIPIENTS.....	11
<b>KEY CONDITIONING</b> .....	<b>12</b>
SKM KEY CONDITIONING.....	12
PGP UNIVERSAL: SKM EXPORT.....	13
PGP DESKTOP: SKM IMPORT.....	14
PGP DESKTOP: REMOVE PREFERRED KEYSERVER.....	14
REMOVE BZIP2 COMPRESSION.....	16
REMOVE UNSUPPORTED CIPHERS AND REMOVE KEY EXPIRATION.....	17
PGP DESKTOP: EXPORT KEYS.....	18
PGP UNIVERSAL: DELETE & IMPORT.....	19
GKM KEY CONDITIONING.....	22
<b>TROUBLESHOOTING</b> .....	<b>23</b>
BLACKBERRY ENTERPRISE SERVER LOG FILES.....	23
PGP UNIVERSAL LOGS.....	23
TROUBLESHOOTING ENROLLMENT.....	23
TRACING KEY & POLICY LOOKUP.....	24
USER CANNOT ENROLL WITH PGP UNIVERSAL.....	25
“YOUR PGP UNIVERSAL SERVER POLICY IS OUT OF DATE AND COULD NOT BE UPDATED”.....	26
EMAIL ON HANDHELD IS BLANK OR CANNOT BE DECRYPTED.....	26

## Introduction

The PGP Support Package for BlackBerry enables end-to-end PGP-encrypted email delivery from a wireless BlackBerry handheld to a PGP-enabled desktop. This guide illustrates the installation and configuration requirements for the PGP Universal Server and the BlackBerry Enterprise Server. These steps must be completed before BlackBerry handhelds can be configured. Handheld installation is described in the *PGP Support Package for BlackBerry User's Guide*.

## Design & Requirements

The necessary components and general topology described by this guide are shown in Figure 1. A state diagram outlining the progress of a secure message sent from the BlackBerry handheld to the desktop is shown in Figure 2 on page 5. The section entitled "Enforcing Policy to Multiple Recipients" on page 11 describes the implications of putting PGP Universal into various topologies.



**Figure 1: PGP RIM Topology**

## PGP Universal Architecture & Setup Requirements

PGP Universal should be installed before the PGP Support Package for BlackBerry is deployed on BlackBerry handhelds. This process will permit keys to be created and properly conditioned, as described in the “Key Conditioning” section beginning on page 12. There are many viable network configuration options, depending on the needs of the enterprise.

All desktops associated with BlackBerry handheld PGP users must be running PGP software on the desktop. The desktop software options are PGP® Desktop and PGP Universal™ Satellite. Users without PGP software can receive messages decrypted by PGP Universal operating in gateway mode, but decryption will occur on the PGP Universal Server rather than on the desktop. Also, BlackBerry handheld users not running PGP software on the desktop will not be able to read encrypted mail deposited into their Exchange-based “sent items” folder.

The PGP Universal Server should be placed in the DMZ. At a minimum, PGP Universal will be used for policy and key lookup. However, there is a compelling reason for placing PGP Universal into the mail flow, either directly or on a conditional basis, as described below.

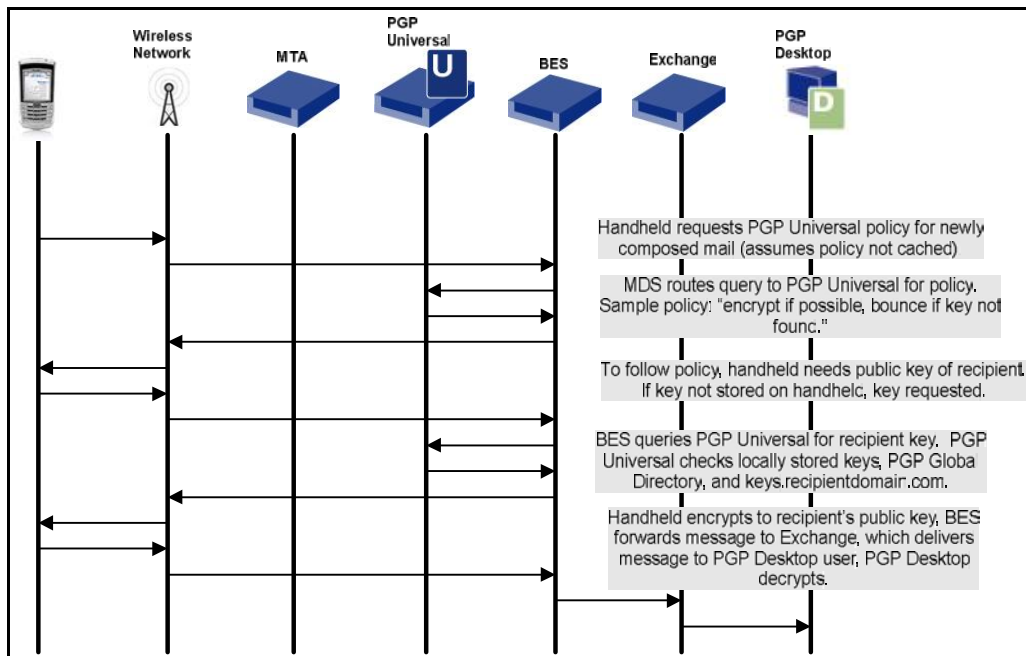
## Configuration Requirements

This configuration requires the following:

- PGP Universal 2.0.2 build 2433 or greater
- PGP key requirements (see the “Key Conditioning” section beginning on page 12 for details)
  - All handheld users are either in
    - Server Key Mode (SKM) *or*
    - Guarded Key Mode (GKM)
  - No “preferred keyserver” is specified
  - Twofish and IDEA ciphers are disabled
  - Bzip2 compression is disabled
- PGP-supported ciphers
  - AES (128-, 192-, and 256-bit)
  - CAST (128-bit)
  - TripleDES
- RIM requirements
  - BlackBerry Enterprise Server for Microsoft Exchange 4.0 SP2 or higher
  - BlackBerry Handheld Software v4.1 or greater
  - PGP Support Package for BlackBerry
- Desktop requirements
  - PGP Desktop 9.0 *or* PGP Universal Satellite
  - BlackBerry Desktop Manager 4.0 (to load PGP software onto the handheld)

## Transactions

Figure 2 details the transactions associated with the transmission of a message sent from a PGP-enabled handheld to a PGP-managed desktop inside the same enterprise. The BlackBerry Enterprise Server proxies requests to PGP Universal on behalf of the handheld and finally inserts the message into the user's Exchange mailbox.



**Figure 2: Message Flow – BlackBerry Handheld to Managed User**

### Considerations:

- The message is never sent or received by the externally facing mail transfer agent (MTA).
- The BlackBerry Enterprise Server requests to the BlackBerry infrastructure are stateful outbound TCP-based requests to port 3101 of the BlackBerry infrastructure.
- In this example, the recipient was an internal user, so the public key was found on the local PGP Universal Server.
- The flow of this message to an external domain would be very similar to the transactions shown in Figure 2. However, in the final step, the message would be passed from the Exchange server to the externally facing MTA for delivery to the recipient domain.

Log entries demonstrating the PGP Universal processing of a secure message sent from a BlackBerry handheld are shown in the "Troubleshooting" section beginning on page 23.

## Policy Considerations & BlackBerry Enterprise Server Setup

Both the PGP Universal Server and the BlackBerry Enterprise Server permit the administrator to define policy. PGP Universal enforces compliance from an email security perspective while the BlackBerry Enterprise Server controls the operation of the handheld connected to it. As such, the policies are considered to be separate entities. There may be some overlap in the policy items available to administrators. In all cases, when using a handheld, BlackBerry Enterprise Server IT policy will be enforced before PGP Universal policy is applied.

A user whose BlackBerry handheld is enrolled with the PGP Universal Server cannot send a message that violates PGP Universal policy. Consider these examples:

- The PGP Universal policy is set to “encrypt if key found, otherwise bounce message.” The handheld user may compose a message to a recipient without a key, but will receive an error when the message is sent.
- Similarly, the handheld user may compose a message using the plaintext “Send Using” option, but the PGP Universal policy prevails and the message is sent encrypted. The handheld user is informed as the message is sent.

PGP Universal policy will only prevail if the IT policy for “PGP Force Encrypted Messages” is set to “false.” This setting determines whether policy is handheld-based or PGP Universal Server-based and is further described in Table 1 on page 7.

Messages sent from the BlackBerry handheld to multiple recipients are subject to a variety of policy implications. Refer to “Enforcing Policy to Multiple Recipients” on page 11.

### Default Policy Attributes

Policy settings should be considered carefully. A post-deployment change to the PGP Universal Server Address will force the handheld user to re-enroll with the PGP Universal Server. Table 1 on page 7 shows PGP Universal policy attributes and their default values.

Attribute	Notes	Default Value
PGP Force Digital Signature	If "False," policy is dictated by the PGP Universal Server. If "True," messages composed on the handheld are always signed.	False
PGP Force Encrypted Messages	If "False," policy is dictated by the PGP Universal Server. If "True," messages composed on the handheld are forced to encrypt without consulting the PGP Universal Server. If no recipient key is found, an error is generated on the handheld.	False
PGP Blind Copy Address	Archival or administrative use. Should PGP-managed messages be blind copied (BCC'd) to a recipient specified by the BlackBerry Enterprise Server administrator? The BCC address is visible on the user's handheld.	False
PGP Allowed Content Ciphers	What ciphers are permitted to encrypt messages? A number in base 2 is displayed based on the selected ciphers.	AES (128-, 192-, 256-bit), CAST, TripleDES
PGP Minimum Strong RSA Key Length	The minimum key length before a user is warned about the length of the RSA key. The default RSA key length used by PGP Universal is 2048 bits.	1024
PGP Minimum Strong DH Key Length	The minimum key length before a user is warned about the length of the DH key.	1024
PGP Minimum Strong DSA Key Length	As above, for DSA key length.	1024
<b>PGP Universal Server Address</b>	Used by the handheld to look up policy and the recipient's public key.	None
PGP Universal Enrollment Method	0 = enroll by domain username / password 1 = enroll by email sent to user	1
PGP Universal Policy Cache Timeout	How many hours can the handheld cache policy after it is retrieved from PGP Universal? After cache timeout, the handheld requests policy the next time a message is sent.	24

Table 1: IT Policy Table

## Editing IT Policies

The IT policies for the PGP Support Package for BlackBerry are called the "PGP Application Policy Group." These policies should be modified to conform to corporate security practice. The policies articulated by this guide are recommended by PGP Corporation. Open the BlackBerry Manager on the BlackBerry Enterprise Server. Select the policy group by following the five steps shown in Figure 3 on page 8.

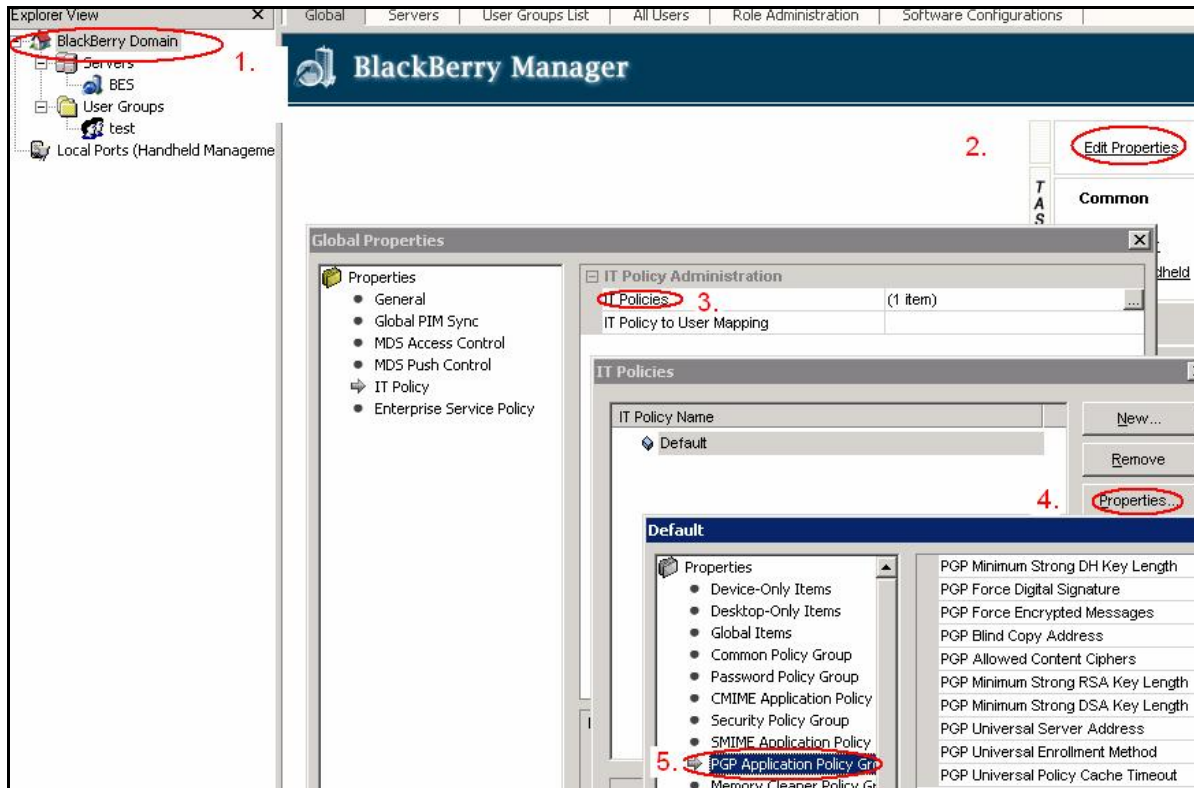


Figure 3: Selecting PGP Application Policy Group

With one exception, PGP Corporation recommends using the default values. The definition of each field is displayed when the field is selected. Table 1 on page 7 explains these fields. Modify the PGP Universal Server Address to correspond to your managed domain, as shown in Figure 4:

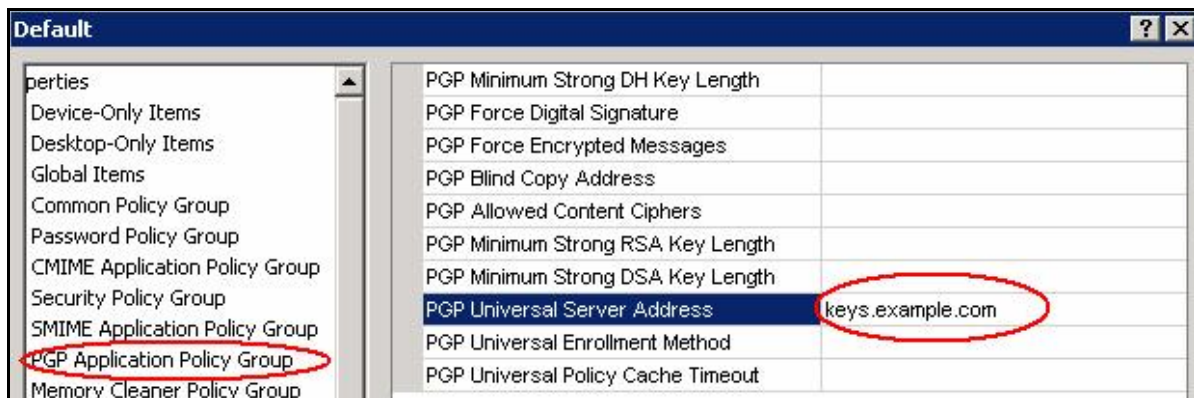


Figure 4: Editing IT Policy

## Enable BlackBerry Enterprise Server Secure Email Support

For BlackBerry Enterprise Server versions prior to 4.1, the PGP Support Package for BlackBerry will not be recognized by the handheld unless S/MIME encryption is enabled on the BlackBerry Enterprise Server. From the BlackBerry Enterprise Server, select "Properties." Select the "Message Options" tab and enable S/MIME Message Processing, as shown in Figure 5.

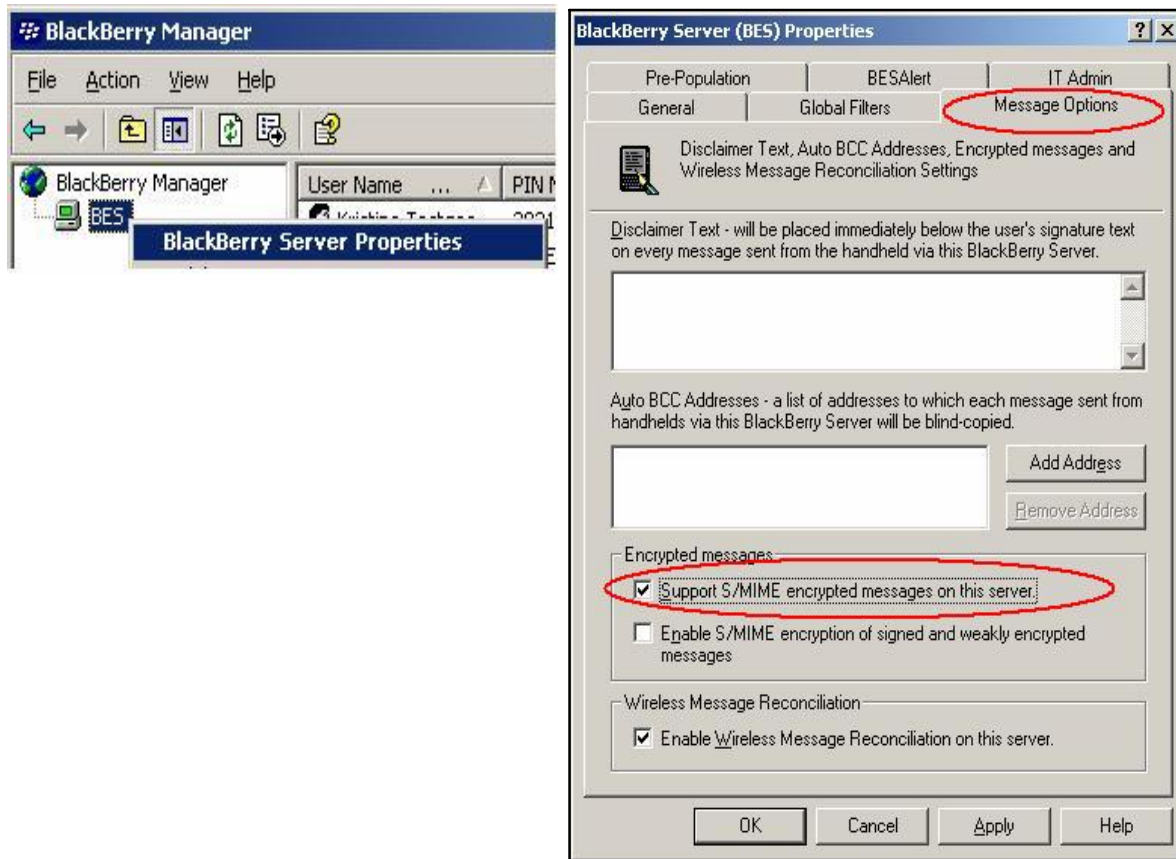


Figure 5: BlackBerry Enterprise Server 4.0 – Enable S/MIME

## Mobile Data Service LDAP Settings

The PGP Support Package for BlackBerry uses the PGP Universal Server Address specified on page 7 to look up the public key of the recipient when encryption is requested and the recipient's key is not available on the BlackBerry handheld. The Mobile Data Service (MDS) on the BlackBerry Enterprise Server proxies the key request for the handheld user to the PGP Universal Server. Optionally, an additional PGP Universal Server can be specified, as shown in Figure 6.

Set the secondary server used for key lookup by modifying the MDS Properties and selecting LDAP. Enter the name of the PGP Universal Server. In this example, **keys.emailrecipient.com** is specified as an alternate key lookup source. Note that the LDAP query "o=Searchable PGP Keys" is case-sensitive and must be entered precisely as shown, starting with a lower-case "o".

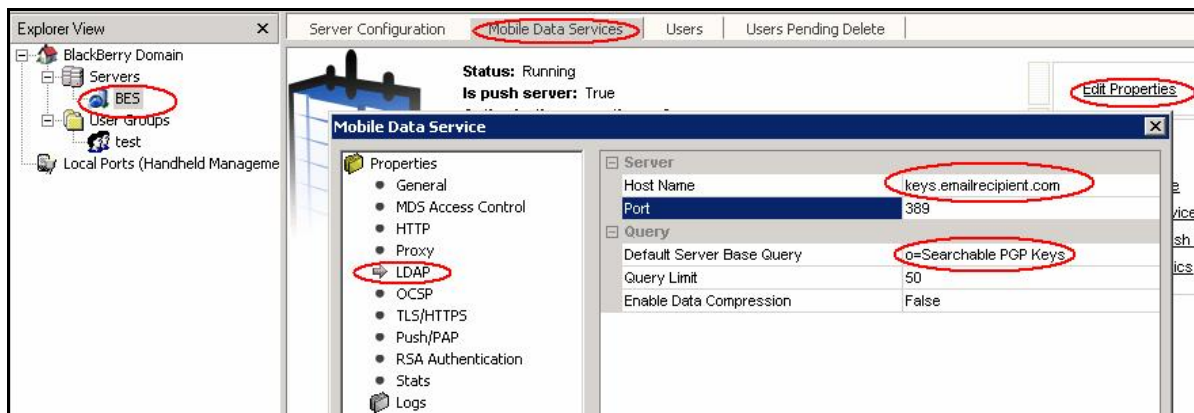


Figure 6: MDS LDAP Settings

Users may also look up keys on an ad-hoc basis using the "PGP Key Search" module that resides on the BlackBerry handheld. This key search is also proxied for the handheld user by the BlackBerry Enterprise Server.

## Pushing Policy to the Handheld

- **MDS** – Mobile Data Service (MDS) settings are stored on the BlackBerry Enterprise Server. MDS changes are realized on the handheld whenever MDS-related services are requested.
- **BlackBerry Enterprise Server Properties** – Changes to BlackBerry Enterprise Server properties are sent to the handheld on a regular basis, approximately every 3–5 minutes, depending on server load.
- **IT Policy** – New policies are pushed out after they are created. Modifications to the policy groups are sent every 3–5 minutes, depending on server load. Modifications to IT policy may force handheld users to re-enroll.
- **PGP Universal** – PGP Universal policy is requested by, not pushed to, the handheld. PGP Universal policy changes are requested by the handheld after the policy cache has timed out and a new message is sent. The cache timer is set by IT policy on the BlackBerry Enterprise Server. An unscheduled policy update can be requested by resetting the handheld.

## Enforcing Policy to Multiple Recipients

The BlackBerry handheld never transmits more than one copy of a given email message. This behavior preserves bandwidth on wireless networks and simplifies message management on the handheld. A message addressed to multiple recipients will always be transmitted as a single message to the BlackBerry Enterprise Server. If all recipients have keys on the handheld or keys that can be discovered by PGP Universal, the message is encrypted on the BlackBerry handheld. However, messages with multiple recipients will likely be addressed to some recipients with keys and some recipients without keys.

If the PGP Universal “key not found” policy is to bounce messages sent to recipients without keys, the handheld user is prompted to remove the recipient without a key from the distribution list, cancel the message, or supply a key. For all other PGP Universal “key not found” policies, a message addressed to recipients with **and** without keys will **not** be PGP-encrypted by the BlackBerry handheld. RIM standard AES encryption will protect the message from the BlackBerry handheld to the BlackBerry Enterprise Server, but PGP Universal must be placed in the mail flow to enforce end-to-end policy.

To secure the message internally, “TLS required” should be configured on the BlackBerry Enterprise Server, the Exchange server, and PGP Universal’s outbound mail proxy. For other “key not found” policies such as “Web Messenger” and “Smart Trailer,” the PGP Universal Server will transmit multiple copies of the message, as appropriate.

It is possible to put PGP Universal directly in the external mail flow so that all messages leaving or entering the enterprise are processed by PGP Universal. For large installations, messages are often relayed to PGP Universal on a conditional basis. There are many PGP-supported configuration guides available from PGP Corporation to assist with the setup of conditional relay environments.

## Key Conditioning

If the user's private key is held without an individual passphrase on the PGP Universal Server, the user is said to be in Server Key Mode (SKM). All SKM keys can be conditioned centrally using the PGP Universal administrative interface and PGP Desktop. If the desktop user and the PGP Universal Server hold a user passphrase-protected copy of the key (called Guarded Key Mode [GKM]), the administrator will have to visit every GKM client and condition each user's GKM key. Privately held keys not on the PGP Universal Server (called Client Key Mode [CKM]) are possible, but are not supported in this configuration.

PGP MIME-encoded messages cannot be read on the BlackBerry handheld. The "preferred server" attribute should be cleared from each user's keypair before the keypair is downloaded to the handheld. When a sender locates a key without this attribute, the sender will not encode the message using PGP MIME.

Bzip2 is an open source data compression algorithm. Bzip2 is not supported on the BlackBerry handheld, so Bzip2-compressed messages cannot be viewed on the handheld. To lessen the likelihood of receiving a Bzip2-compressed message, each user's key should exclude Bzip2 compression. Only keys created on PGP Desktop for the Macintosh will have Bzip2 enabled by default.

The supported ciphers on the BlackBerry handheld are AES256, AES192, AES128, CAST, and TripleDES. Mail encrypted by other ciphers (such as IDEA or Twofish) cannot be deciphered on the handheld. Support for IDEA and Twofish should be removed from all keys of all BlackBerry handheld users.

After these operations are completed, users may still receive unreadable encrypted messages or attachments if external users encrypt to a copy of the old, unconditioned key. In this case, the user will have to read the message at the desktop. The recipient or administrator should make the modified key available to the sender.

## SKM Key Conditioning

During an email outage window, the administrator exports private and public keys from the PGP Universal Server to a PGP Desktop host. After the keys are exported, PGP Desktop is used to change the attributes of the keys. The original key is removed from the PGP Universal Server, the public key and email key cache are cleared, and the conditioned key is re-imported into the PGP Universal Server.

An outage window is required during the brief period between the deletion of the original key and the importation of the newly conditioned key. When no key is present, outgoing mail detected by PGP Universal triggers the generation of a new keypair. The outage prevents the generation of this second keypair.

## PGP Universal: SKM Export

This procedure should also be followed for all new users. Use one computer to access both PGP Universal and PGP Desktop, if possible. From PGP Universal, export the first 20 users, as shown in Figure 7.

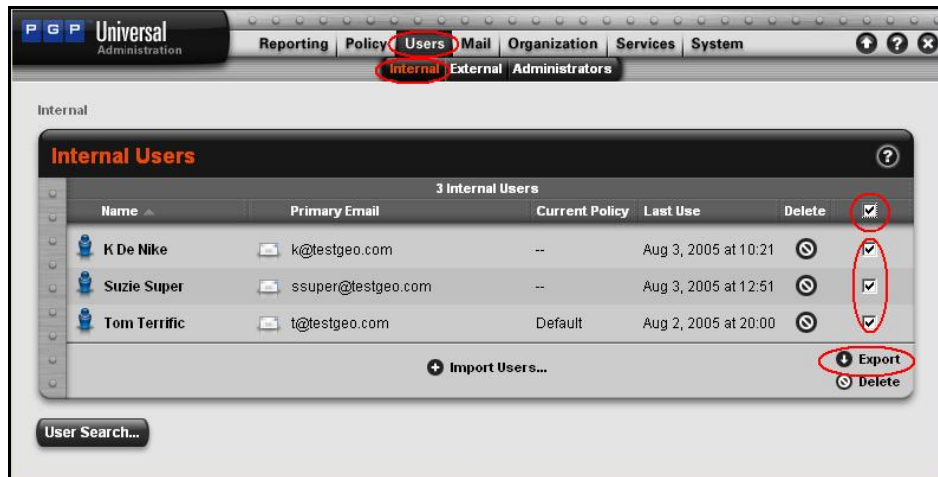


Figure 7: Export SKM Users

If more than 20 users are managed by the PGP Universal Server, export multiple sets of 20 users one screen at a time, each with a unique PGP Armored file name.

To export the entire keypair, select "Export Private Key," as shown in Figure 8



Figure 8: Export SKM Keypair

## PGP Desktop: SKM Import

After all keys have been exported, move the PGP Armored file to the desktop of the PGP Desktop machine. Double-click on the file and import all keys, as shown in Figure 9:

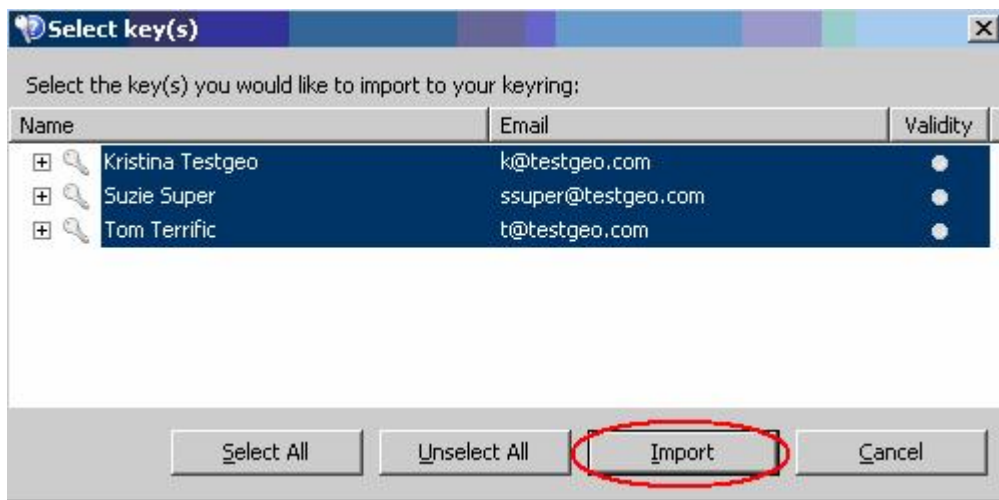


Figure 9: Import SKM Keys

## PGP Desktop: Remove Preferred Keyserver

Open PGP Desktop. As shown in Figure 10, select "PGP Keys," "All Keys." Press Ctrl-A to select all keys. Right-click and select "Key Properties" (not shown).

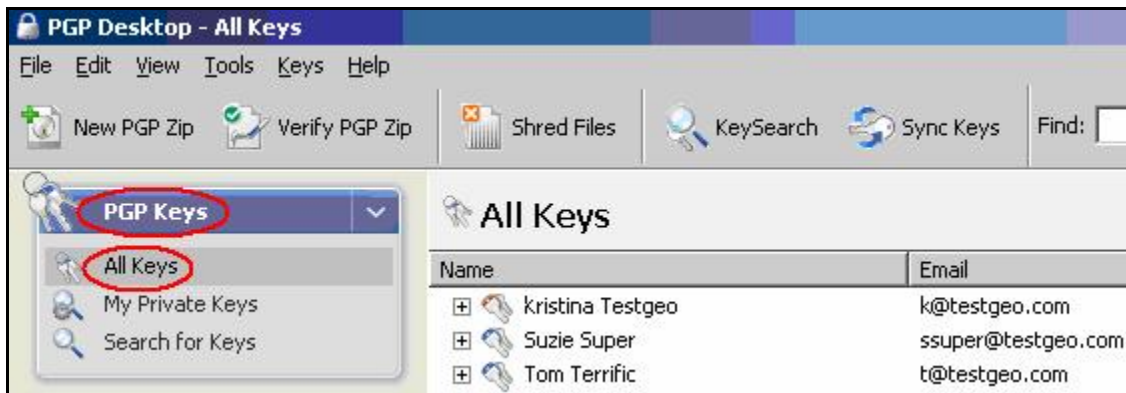


Figure 10: Remove Preferred Keyserver – Step 1

An individual pop-up screen displays the properties for each user, as shown in Figure 11. Click on the “Keyserver” attribute.

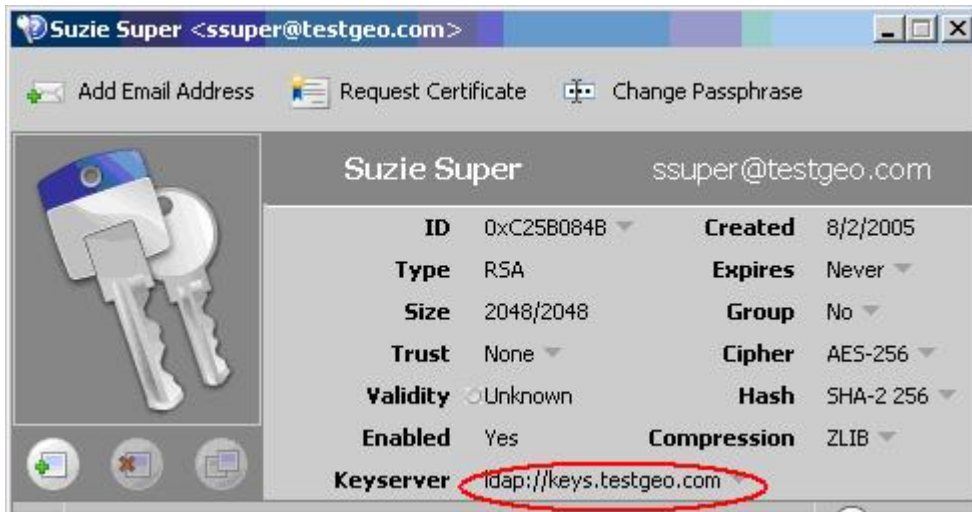


Figure 11: Remove Preferred Keypair – Step 2

Delete the contents of the “Server” field and press “OK,” as shown in Figure 12:

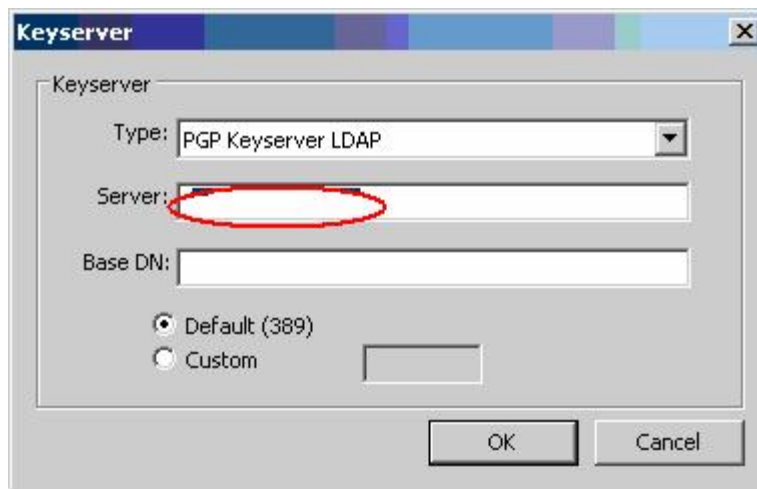


Figure 12: Remove Preferred Keypair – Step 3

## Remove Bzip2 Compression

Bzip2 is not supported on the BlackBerry handheld. By default, keys that are generated by PGP Universal or PGP Desktop for the PC do not have Bzip2 compression enabled. To ensure Bzip2 is not enabled on each user's key, select the "Compression" attribute shown in Figure 13 and make sure that Bzip2 is unchecked.

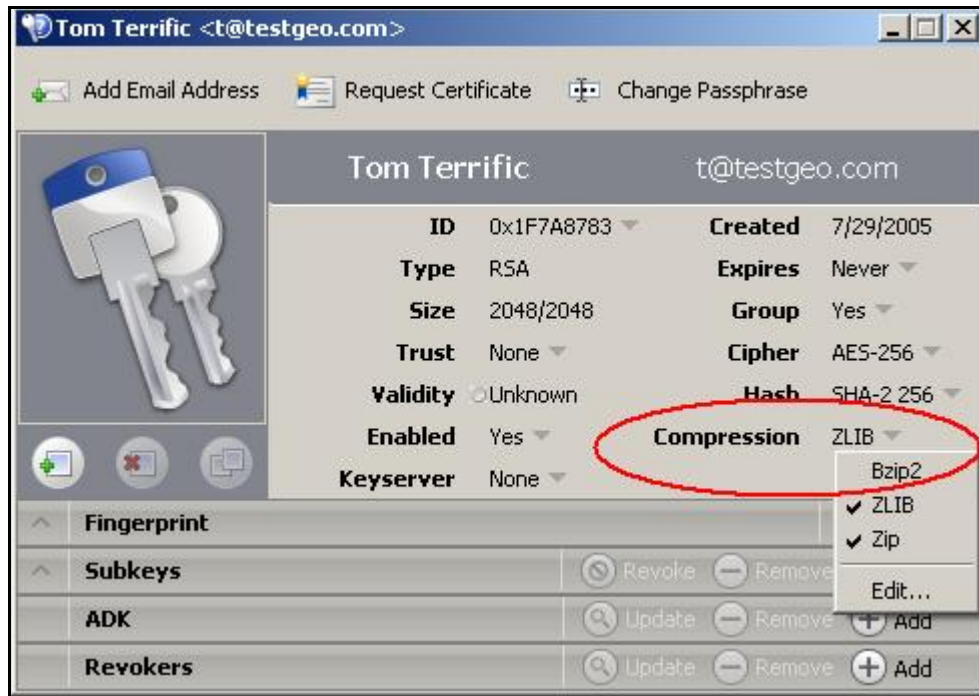


Figure 13: Remove Bzip2 Compression

## Remove Unsupported Ciphers and Remove Key Expiration

IDEA and Twofish should be grayed out, as shown in Figure 14. If not, select the “Edit” button and uncheck IDEA and Twofish. On page 14, the “Preferred Keyserver” attribute was removed. Keys without this attribute do not automatically renew. Ensure that the expiration date of the key is set to “Never”.

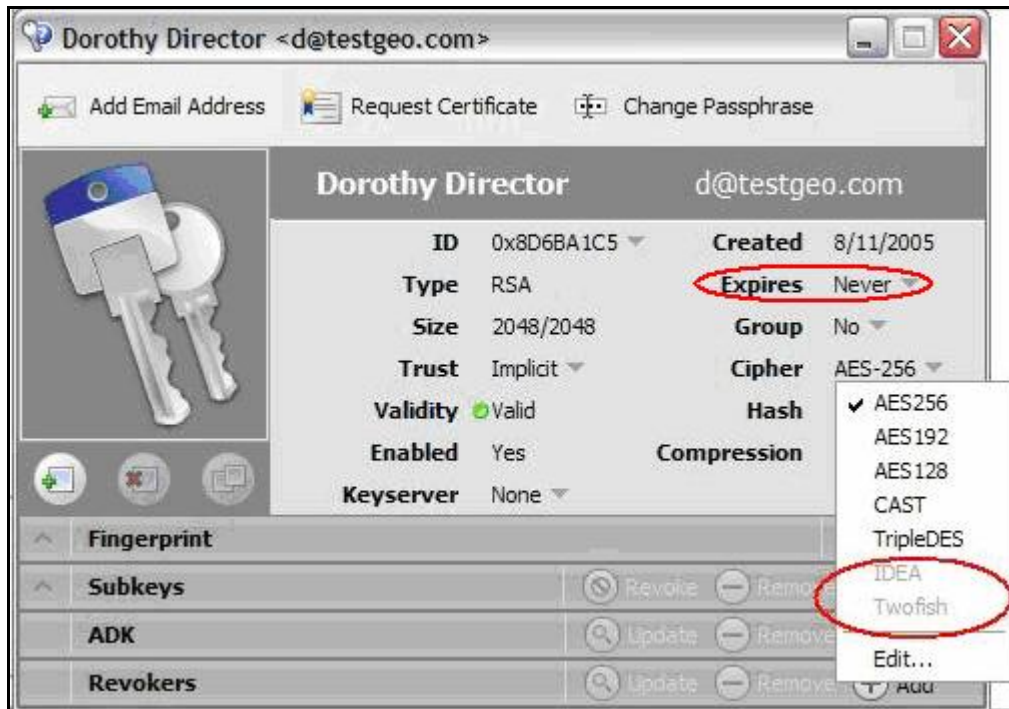


Figure 14: Remove Unsupported Ciphers, No Expiration Date

## PGP Desktop: Export Keys

Once you have conditioned each key, select the keys you have conditioned and export the private and public keyring, as shown in Figure 15:

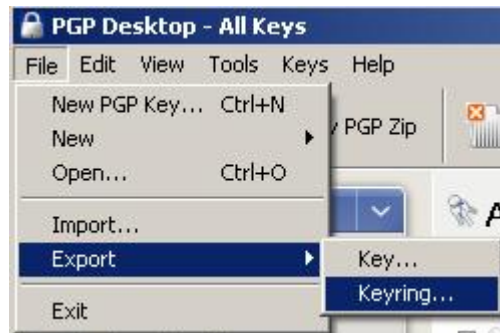


Figure 15: Export Keyrings

PGP Desktop will automatically create one file for the public keys and one for the private keys. The default names are **pubring** and **secring**, respectively. The file can be placed on the desktop by selecting the ellipse, as shown in Figure 16:



Figure 16: Save Exported Keyrings

## PGP Universal: Delete & Import

Initiate an email outage so that no messages are sent to PGP Universal. Login to PGP Universal. As shown in Figure 17, delete all internal users that are to be replaced with a newly conditioned key:

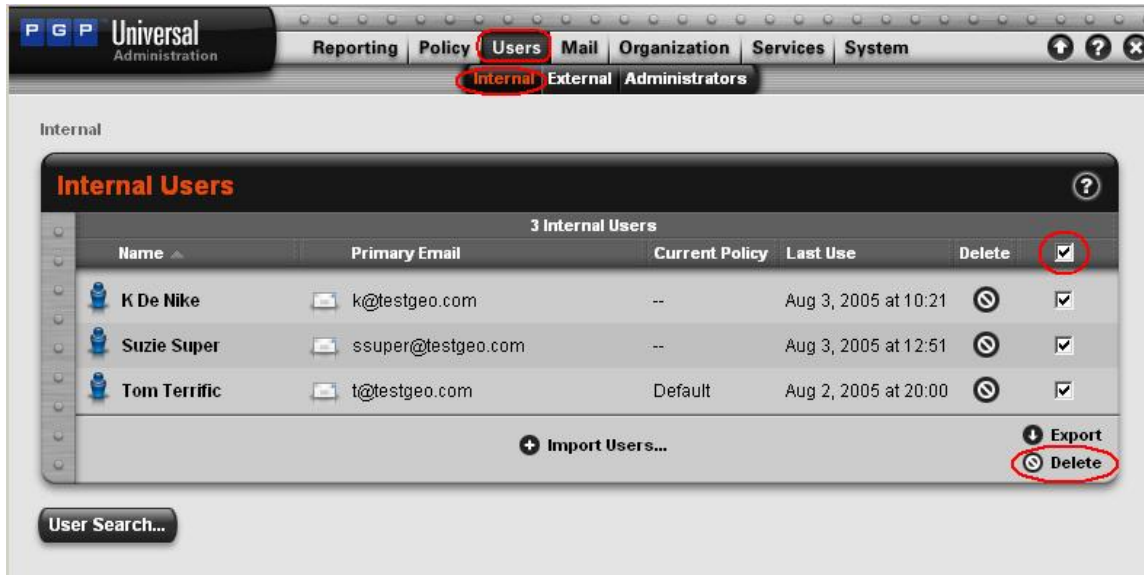


Figure 17: Delete Internal Users – Step 1

Clear the cache of the PGP Universal Server to prevent the attribution of old key attributes to new messages. Access the "Cache Settings" screen, as shown in Figure 18:

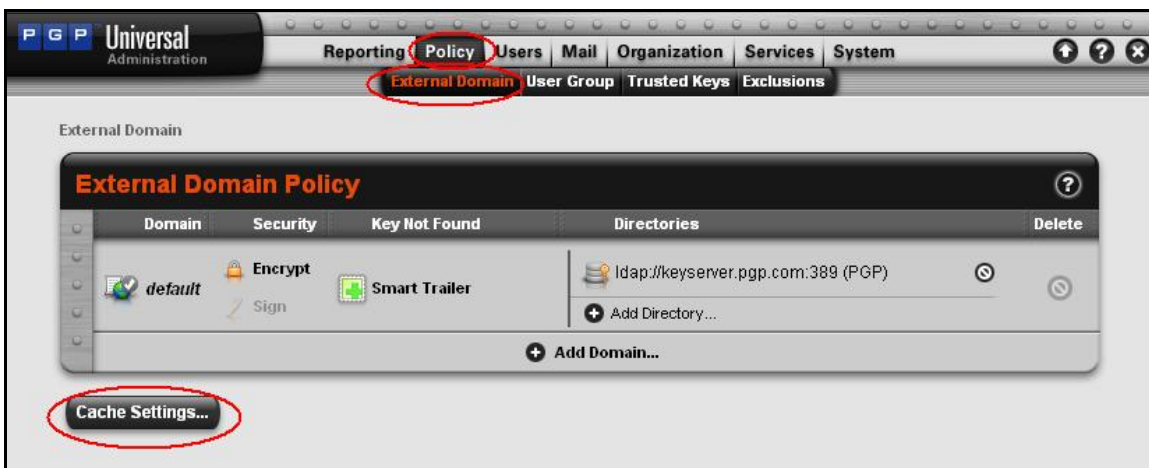


Figure 18: Delete Internal Users – Step 2

Purge the public key cache and then purge the email key cache, as shown in Figure 19:

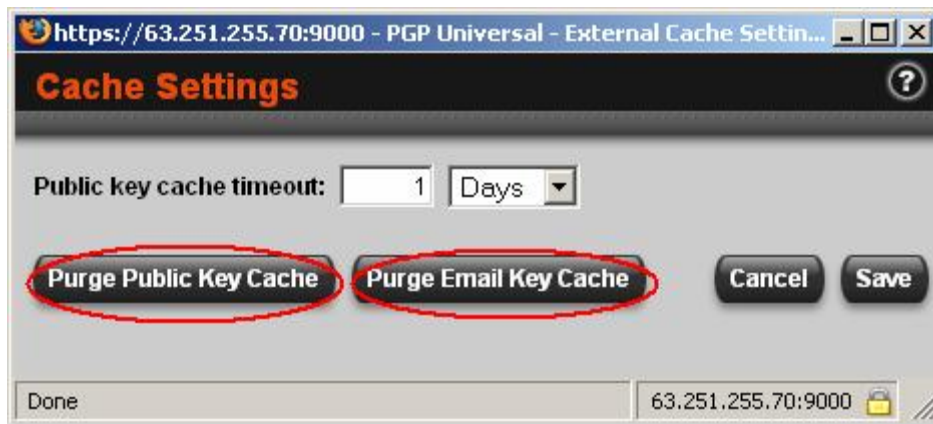


Figure 19: Delete Internal Users – Step 3

Import the newly conditioned users, as shown in Figure 20:

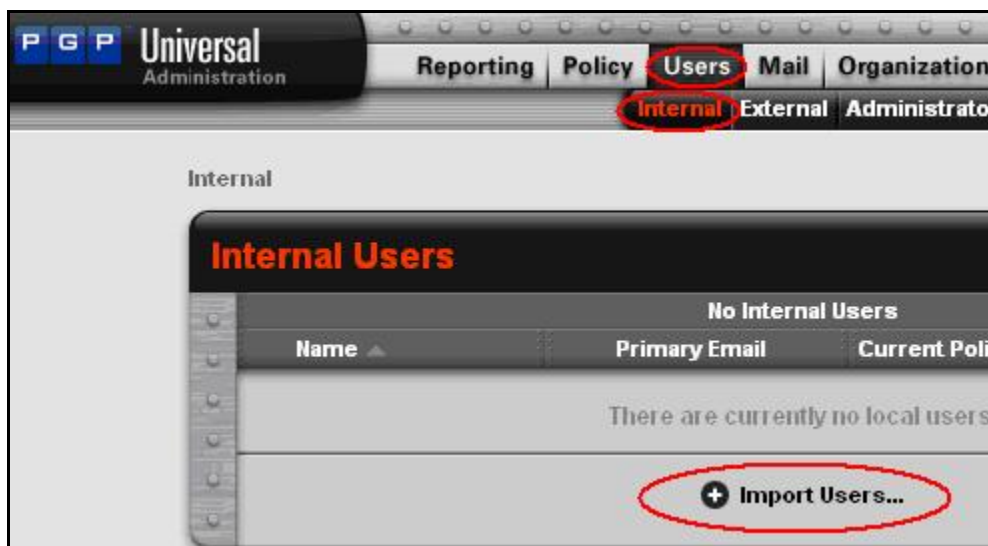


Figure 20: Import Internal Users – Step 1

Select the **pubring** file you saved earlier. You may receive a warning that the keys were only partially imported, as shown in Figure 21. You can ignore this message.



Figure 21: Import Internal Users – Step 2

Now, import the private keyring called **secring.pkr**. You may need to refresh the page. The icons should return to a solid blue man group, as shown in Figure 22, indicating that the users are now SKM.

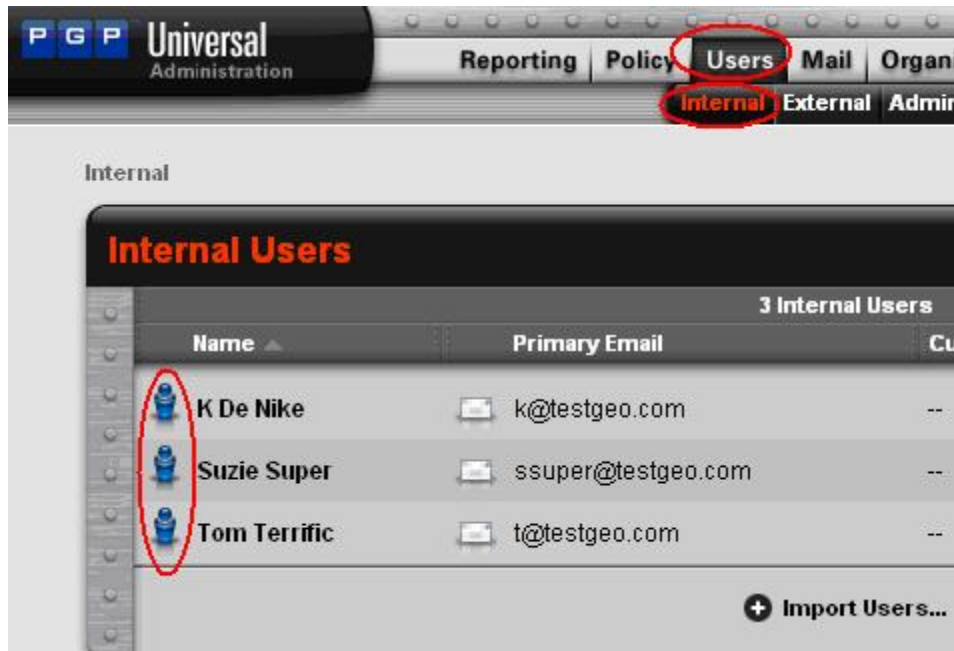


Figure 22: Import Internal Users – Step 3

It is important to securely delete the private keyring file. If the same machine was used to perform all work, the keyring files should now be placed into the PGP Shredder.

This step completes the key conditioning operation.



## GKM Key Conditioning

GKM keys are secured by a passphrase known only to the holder of the private key. GKM keys are conditioned directly on the client, then exported and loaded into PGP Universal.

The user will enter the private passphrase that secures the keypair before it is conditioned, saved locally, and exported for eventual import into PGP Universal. With a single user in mind, follow the general technique for SKM Key Conditioning starting with the section entitled, "PGP Desktop: Remove Preferred Keyserver" on page 14.

## Troubleshooting

### BlackBerry Enterprise Server Log Files

The BlackBerry Enterprise Server logs provide a wealth of information. The logs can be found in this directory:

\Program Files\Research In Motion\BlackBerry Enterprise Server\Logs

A separate directory is created for each day of activity. Ten log files are created by default.

### PGP Universal Logs

PGP Universal logs are broken into nine distinct sections. The most useful log for troubleshooting BlackBerry Enterprise Server configurations is the “Client” log.

### Troubleshooting Enrollment

Figure 23 catalogs the successful PGP enrollment of a user. The five log entries read from the bottom up and are translated as follows:

1. The Mobile Data Service (MDS) (10.214.0.66) logs in on behalf of the user.
2. The PGP enrollment request is received.
3. The user is recognized as a managed PGP Desktop 9.0 user.
4. The keypair is sent to the MDS so it can be delivered to the handheld.
5. The connection is closed.

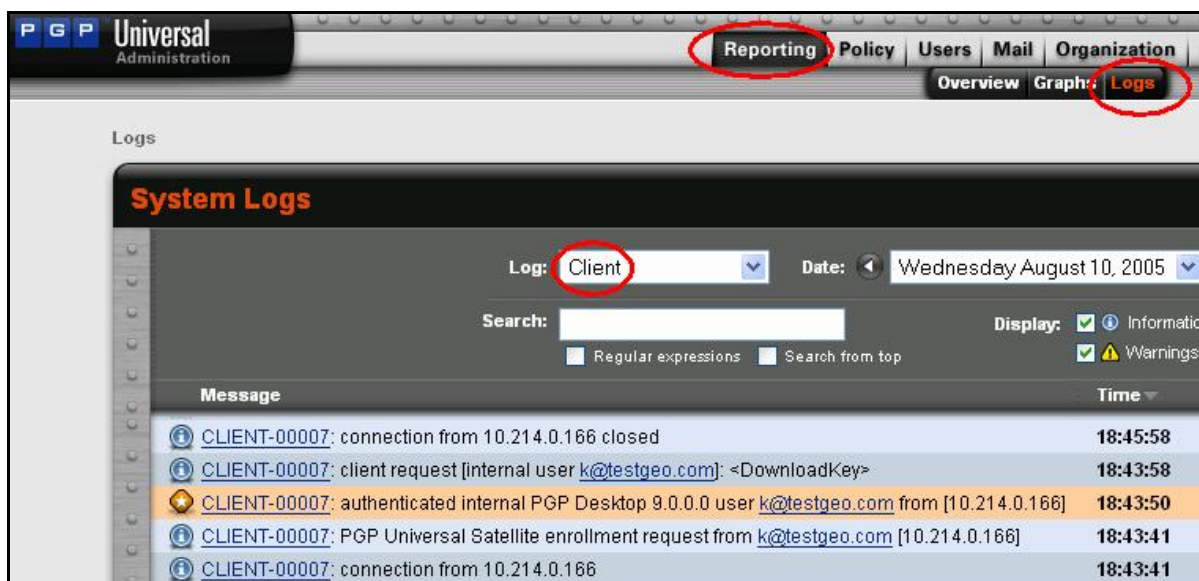


Figure 23: Successful User Enrollment

## Tracing Key & Policy Lookup

Figure 24 traces a successful policy and key lookup. Reading from the bottom up:

1. The MDS connects to PGP Universal.
2. The connection is on behalf of the handheld. The handheld user in this example is sending a message to pgp.com, which is external and not managed by this server. What policy should be applied when the handheld user is sending to an external unmanaged domain?
3. Three seconds later: The reply sent by PGP Universal was “encrypt if you can find a key.” However, the public key is not stored on the BlackBerry handheld. The BlackBerry handheld requires a key, and the MDS proxies this key request to PGP Universal.
4. Five seconds later: This PGP Universal Server queried **keys.pgp.com**. **keys.pgp.com** returned the public key of the recipient. This key is sent to the MDS, which sends it to the handheld, which then encrypts and sends the message.

The screenshot displays the PGP Universal Administration System Logs interface. The top navigation bar includes 'Reporting', 'Policy', 'Users', 'Mail', 'Organization', 'Services', and 'System'. The 'Reporting' tab is selected, and the 'Logs' sub-tab is active. The 'System Logs' section shows a list of log messages with filters for 'Log' (Client), 'Date' (Thursday August 11, 2005), and 'Time' (hh:mm). The 'Display' options are checked for Information, Notice, Warnings, and Errors. The log messages are as follows:

Message	Time
CLIENT-00000: key search <rfenerty@pgp.com> [keys.pgp.com]: found key "Robert Fenerty <rfenerty@pgp.com>" (Key ID: 0x8052C5D2)	11:11:37
CLIENT-00000: client request [internal user k@testgeo.com]: <GetKeyByEmail>	11:11:32
CLIENT-00000: client request [internal user k@testgeo.com]: <GetPolicy>	11:11:29
CLIENT-00000: connection from 10.214.0.166	11:11:29

Figure 24: Successful Policy & Key Lookup

## User Cannot Enroll with PGP Universal

- **MDS availability** – Can the user browse to a common Internet site? If not, the MDS may not be set up properly.
- **PGP Universal availability** – Verify that the BlackBerry Enterprise Server can make an outbound connection to the PGP Universal Server on port 443.
- **PGP Universal user** – Check to see if the email address matches the name of the user listed in PGP Universal's list of "Internal Users" and that **two** key icons are present. The padlock icon shown in Figure 25 indicates that Tom Terrific is a GKM user.

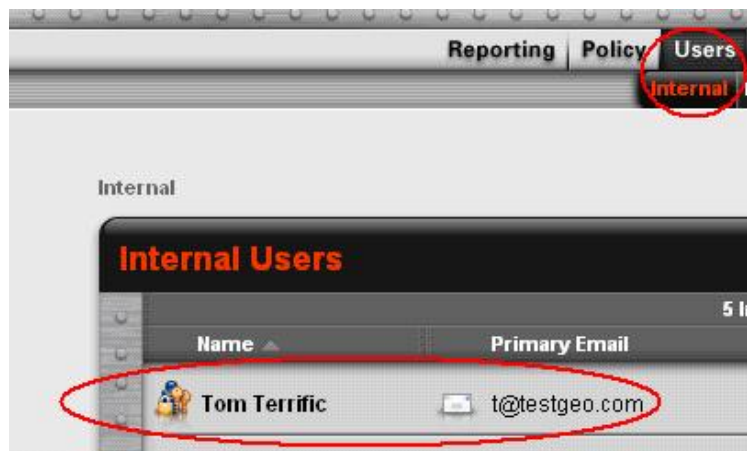


Figure 25: Validate Name & Keypair

If the handheld is unable to enroll successfully, ensure that:

- The handheld has successfully completed Enterprise Activation.
- The BlackBerry Enterprise Server displays the user's PIN and "running" status, as shown in Figure 26:



Figure 26: Active BlackBerry Enterprise Server User

## “Your PGP Universal Server policy is out of date and could not be updated”

This message indicates that the handheld user's key has expired. Condition the key so that the expiration date is set to “Never,” as shown in the “Key Conditioning” section of this guide, beginning on page 12.

## Email on Handheld is Blank or Cannot be Decrypted

The attributes associated with a user's public key are used by the sender to determine the appropriate options to secure a message. This negotiation process ensures a sender does not encrypt a message in a way that is unreadable by the recipient.

If a user is unable to read a message on the BlackBerry handheld, but can read the message using PGP Desktop or PGP Universal Satellite, it is likely the recipient's key is not properly conditioned.

Ensure that the key:

- Does **not** have a “Preferred Keyserver” set
- Only supports the AES256, AES192, AES128, CAST, and TripleDES ciphers
- Does **not** support Bzip2 compression

For details on how to change and publish these attributes, see the “Key Conditioning” section of this guide, beginning on page 12.

If these steps have already been taken, it is possible the sender is using an old copy of the recipient's key. Determine the source of the key and send a new copy of the conditioned public key to the sender.

**PGP Corporation**

3460 West Bayshore Road

Palo Alto, CA 94303 USA

Tel: +1 650 319 9000

Fax: +1 650 319 9001

Sales: +1 877 228 9747

Support: [www.pgpsupport.com](http://www.pgpsupport.com)

[www.pgp.com](http://www.pgp.com)

© 2006 PGP Corporation

All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form by any means without the prior written approval of PGP Corporation.

The information described in this document may be protected by one or more U.S. patents, foreign patents, or pending applications.

PGP and the PGP logo are registered trademarks of PGP Corporation. Product and brand names used in the document may be trademarks or registered trademarks of their respective owners. Any such trademarks or registered trademarks are the sole property of their respective owners.

**The information in this document is provided “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.**

This document could include technical inaccuracies or typographical errors.

Changes to this document may be made at any time without notice.