

## Information About BlackBerry Wireless Email to Plan for Disaster Recovery

Originally Posted: August 8, 2000

### Summary

Disaster recovery planning for Research In Motion's BlackBerry™ Wireless email solution is a natural extension of the planning that organizations must undertake for their Microsoft Windows NT® and Microsoft® Exchange environments. There are two architectural configurations that are in use today for BlackBerry deployments: those that are managed via user's individual desktop software (the BlackBerry Desktop Redirector) and those that are unified into a single administrative interface (the BlackBerry Enterprise Server).

Because Microsoft Exchange Server is a core component in the BlackBerry Desktop Redirector solution, a complete Exchange Server Disaster Recovery Plan (DRP) process should exist, be documented and tested regularly. In addition to requiring a DRP process for the Exchange Server, BlackBerry Enterprise Server installations will also require a DRP process for a Windows NT Server (this server hosts the BlackBerry Enterprise Server service).

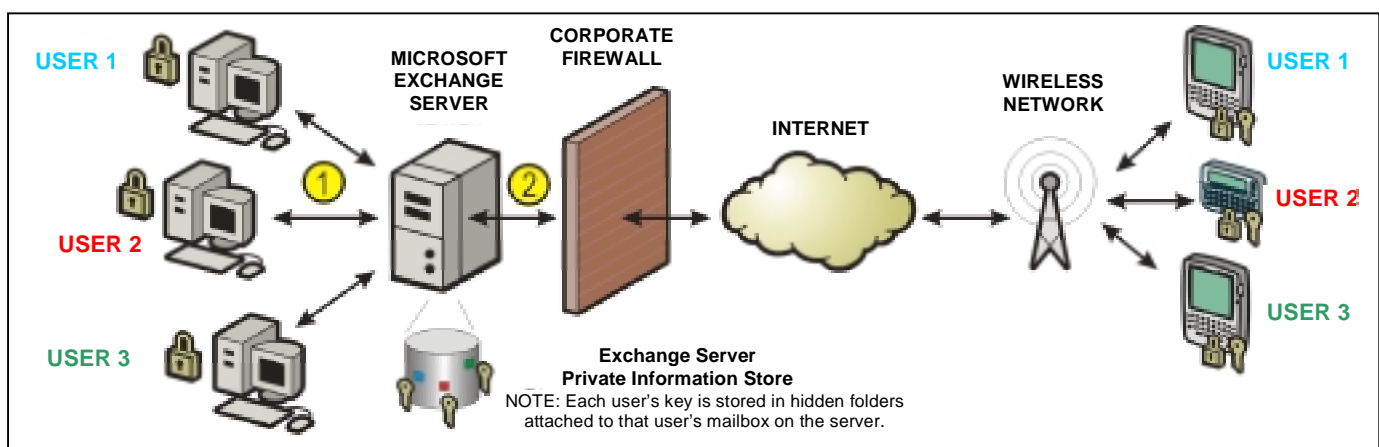
### Resolution

There are two recovery scenarios that will be examined in greater detail below. They are: a) BlackBerry Desktop Redirector disaster recovery plan and b) BlackBerry Enterprise Server disaster recovery plan.

#### Scenario A – BlackBerry Desktop Redirector DRP

In order to plan for disaster recovery for the Desktop Redirector scenario, it is necessary to understand at a high level how the Desktop Redirector performs the task of securely redirecting email to a user's handheld. The Desktop Redirector is a software component that is installed as part of the BlackBerry Desktop Software installation routine. When the user installs the desktop software, they will be prompted to choose whether the BlackBerry service will be run from their desktop or from a server provided by their IT department.

By configuring the desktop software to install the Desktop Redirector, the user is enabling their desktop to perform the compression/decompression, encryption/decryption and redirection of email to and from their handheld (assuming the user has not been added to a BlackBerry Enterprise Server by their administrator, in which case this option will not affect redirection at the server). Below is a simple diagram of how this service functions:



Individual desktops communicate with Exchange via MAPI – Microsoft's Messaging Application Programming Interface. Through this interface, the desktop redirector component is notified when new mail arrives at the Exchange Server. Upon notification, the desktop will retrieve a copy of the message from the Exchange Server in order to apply the user's forwarding rules and filters. If the message meets the user's rules for forwarding to the handheld, then the first 2 KB of the

message will be compressed and encrypted with the user's Triple DES encryption key. This encrypted payload will then be sent to the wireless network via the Internet using the SMTP capabilities provided by Microsoft Exchange Server.

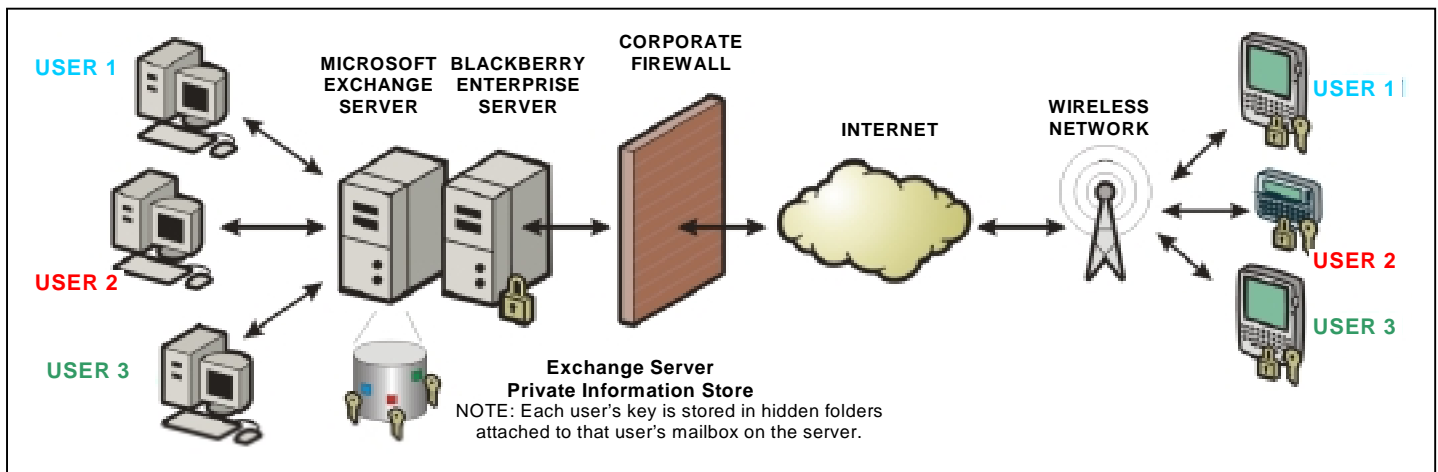
When the message is delivered to the handheld, the Triple DES encryption key stored on the handheld will decrypt the message and the user will be notified. If the user chooses to respond to the message, it will once again be compressed and encrypted and will follow the same path back to the Exchange Server. The message will then be delivered to the user's Inbox where it will be decrypted and decompressed by the Desktop Redirector. The message is then placed in the user's Outbox from where the message will be sent to the intended recipient.

All of the user's configuration information as well as their Triple DES encryption key, are stored in hidden folders added to each user's individual private information store on the Microsoft Exchange Server. Therefore, in the case of a disaster, both the user's desktop and the Exchange Server would need to be fully recovered in order to restore e-mail flow to and from a user's handheld. The desktop would have to be restored, because it is the component performing the compression/decompression, encryption/decryption in addition to the forwarding through Exchange Server via SMTP. The Exchange Server(s) would also need to be restored and the user's mailbox would need to be recovered as of the most recent backup. A new mailbox created with the same name would not be enough, as all of the user's configuration information as well as their encryption key would have been lost. Additionally, the Exchange Server Internet connection must be re-established and its Internet Mail Service (IMS) fully functional.

Therefore, in the case of the desktop redirector scenario – the key to disaster recovery will be to ensure that the user's local machine and Microsoft Exchange Server are both fully accounted for in a disaster recovery plan. For further information on disaster recovery of an Exchange environment, see the Microsoft Exchange Disaster Recovery White Paper (Document version 4.0).

## Scenario B – BlackBerry Enterprise Server DRP

When the BlackBerry wireless email solution is deployed with a BlackBerry Enterprise Server, additional steps need to be taken in order to ensure an appropriate disaster recovery procedure is in place. To shed some light on these additional steps, it is important to review the architecture of a server-based BlackBerry installation.



When a BlackBerry Enterprise Server is introduced into the environment, it will serve as a centralized point for all redirection, compression and encryption thus removing the need for users to run the Desktop Redirector. The BlackBerry Enterprise Server is installed on a Windows NT Server as an NT Service. This service will access the Microsoft Exchange Server via MAPI through a MAPI profile on the local machine. The Exchange account the MAPI profile uses is given "Service Account Admin" privileges over the Exchange site and hence will have access to the requisite user mailboxes. Once a message arrives for a particular user, the BlackBerry Enterprise Server will be notified via a MAPI event, that a new message has arrived. The BlackBerry Enterprise Server will then apply the user's filters and rules to determine if the message should be forwarded to the user's BlackBerry. If the forwarding criteria are met, then the BlackBerry Enterprise Server will compress, Triple DES encrypt and forward the encrypted message to the wireless network, via direct connection over the Internet.



There are several components which must be in place for the server to function correctly. First, the NT Service running on the BlackBerry Enterprise Server requires configuration parameters, which are stored in the registry. Second, the service will require a validated security context (in other words, the ability to log onto a functioning Windows NT Domain) such that it will be able to gain access to the Microsoft Exchange Server. Finally, it requires a MAPI profile (provided by either Exchange 5.0 client or Outlook 97/98/2000) that is tied to an Exchange account with Service Account Admin privilege within the Exchange domain. This is all in addition to a fully restored Microsoft Exchange Server environment as all of the configuration information for the BES is stored in the administrative mailbox created on the Exchange Server. Additionally, user's individual configuration options like filters and rules as well as their encryption keys, are stored in their individual mailboxes as occurs with the Desktop Redirector scenario discussed above. Therefore, to plan for a disaster recovery scenario when a BlackBerry Enterprise Server is in place, one will require the following components:

- A Windows NT domain that will provide authentication services for the appropriate accounts
- An Exchange Server with a fully recovered private information store with a current backup of all BlackBerry enabled mailboxes as well as the administrative mailbox for the BlackBerry Enterprise Server
- A Windows NT Server with a full registry backup for the service configuration information
- A MAPI profile on the Windows NT Server which access the administrative mailbox on the Exchange Server through an account with Service Account Admin permissions

When compared with the steps required for a Desktop Redirector disaster recovery plan, an additional Windows NT Server with several particular components is required. It is important to note that this "restored" Windows NT Server could be provided either by a server recovered through standard disaster recovery procedures (i.e. restoring the most recent backups) or through a "hot spare" machine. However, a hot spare machine would need to be stored at a location off site in order to fully serve the purpose of providing true disaster recovery. The use of a "hot spare" machine will be further explored in Technical Advisory # STAE-0006.

## Affected Software Versions

- BlackBerry Enterprise Server versions 1.6, 1.6 with Service Pack 1, 1.6 with Service Pack 2, 2.0 and 2.0 with Service Pack 1
- BlackBerry Desktop Software versions 1.6, 1.6 with Service Pack 1, 1.6 with Service Pack 2, 2.0 and 2.0 with Service Pack 1

## Additional Information Required

Not Applicable

## Obtaining Support on this Issue

Support for this issue can be obtained by contacting BlackBerry Technical Support at 1-877-255-2377

## Revisions

- Aug 8, 2000: Advisory Created

©2000 Research In Motion Limited. All rights reserved. Research In Motion, BlackBerry, the BlackBerry logo and the "envelope in motion" symbol are trademarks of Research In Motion Limited. RIM, Research In Motion - Registered U.S. Patent and Trademark Office. All other brands, product names and company names mentioned herein may be trademarks or registered trademarks of their respective holders.

RESEARCH IN MOTION LIMITED (RIM) MAKES NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION OR GRAPHICS CONTAINED IN THIS ADVISORY FOR ANY PURPOSE. THE CONTENT CONTAINED IN THIS DOCUMENT, INCLUDING RELATED GRAPHICS, ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. RIM HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THIS INFORMATION, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL RIM BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION CONTAINED HEREIN. THIS DOCUMENT, INCLUDING ANY GRAPHICS CONTAINED WITHIN THE DOCUMENT, MAY CONTAIN TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. UPDATES ARE PERIODICALLY MADE TO THE INFORMATION HEREIN AND RIM MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED HEREIN AT ANY TIME.