

Does Exchange ActiveSync® (EAS) Solve All Your Mobile Data Needs?

WHITE PAPER

Version: 1.0

March 23, 2009

Table of Contents

1. Summary	3
2. Introduction	3
3. Supported Platforms	4
3.1. Exchange Data	4
3.2. Other Corporate Data	5
4. Supported Devices	5
4.1. Windows Mobile	5
4.2. Apple	6
4.3. Nokia	6
4.4. Sony Ericsson	6
4.5. Palm	7
4.6. BlackBerry	7
4.7. Laptops and Netbooks	7
4.8. Device Summary	7
5. Typical Microsoft Exchange ActiveSync Implementation	7
6. Alternatives to EAS	8
6.1. BlackBerry Enterprise Server (BES)	8
6.2. Good Technology Mobile Messaging	9
7. User Experience	10
7.1. Wireless Carrier Agnostic	10
7.2. True Push	10
7.3. Scalability	10
7.4. Network Efficiency	11
7.5. Battery Life	11
7.6. Easier for IT Managers	11
8. Security	11
8.1. Transport Security	11
8.2. Device Policies	12
9. Exchange Replacements	12
9.1. PostPath (Cisco)	12
9.2. Zimbra (Yahoo)	12
9.3. Open-Xchange	12
9.4. Scalix	12
9.5. Unison	13
9.6. Citadel	13
9.7. Lotus (IBM)	13
9.8. Novell Open Workgroup Suite (NOWS)	13
9.9. Openchange	13
9.10. The Future of Enterprise E-Mail	13
10. Conclusions	13
Bibliography	15

1. Summary

Exchange ActiveSync® (EAS) [1] enables mobile access to e-mail, schedules, contacts, tasks, and other Exchange Server data from Exchange ActiveSync-enabled mobile phones. Vendors who licensed Exchange ActiveSync from Microsoft include Apple, Nokia, Palm, Samsung, Sony Ericsson, and Symbian [2]. At first glance it appears that many phones from these vendors might support a BlackBerry-like mobile e-mail experience out of the box. This White Paper takes a closer look at this premise and concludes that EAS has severe limitations.

2. Introduction

EAS is a Microsoft Exchange synchronization protocol based on HTTP and XML, which lets mobile devices access an organization's information on a Microsoft Exchange server. These devices are either Microsoft Windows Mobile® powered devices or EAS-enabled mobile phones. EAS allows mobile users to access their e-mail, calendar, contacts, and tasks even while working offline.

EAS's basic architecture hasn't changed much since Exchange 2000 Server and Microsoft Mobile Information Server (MIS) 2002, which provided synchronization between Exchange 2000 and devices running Pocket PC 2002. Since Microsoft Exchange Server 2003, EAS support is built into the Exchange Server.

EAS is designed to synchronize users' mailbox data with configurable filtering and truncation settings, to deal with high-latency and low-bandwidth networks as well as low-capacity clients. E-mail support includes synchronization for individual folders on demand, and smart reply and forward including configurable attachment handling – e.g. attachments can be forwarded from the server without downloading them to the device. Meeting requests are supported, as are client-side deletions. Synchronizations are driven from the client either manually or scheduled through HTTP or HTTPS POST requests. The server responds to these POST requests with any required data, with most transactions using a compressed binary tag version of XML (WBXML) to reduce bandwidth.

The Exchange Server will supply identifiers for all objects to be synchronized, plus a key for each Exchange folder that determines the set of objects synchronized at that point. An EAS Client will typically maintain a database of these identifiers and will send the last known synchronization key to the Exchange Server on each synchronization request. This allows the server to assume knowledge of what objects the device contains without the need to receive a complete list of object identifiers each time. If a synchronization fails part way through – say, due to a network failure – then the client can resend the previous synchronization key to obtain any lost data.

EAS also includes functionality to work as a push-solution: Always-Up-To-Date (AUTD). Originally, AUTD synchronization was implemented using SMS-based notifications. This technology did not work properly in practice and it was eliminated from Microsoft Exchange Server 2007. The AUTD push mechanisms introduced in Microsoft Exchange Server 2003 Service Pack 2 (Direct Push) is based on an HTTP connection maintained by the device. The Exchange Server keeps the HTTP connection alive until an update occurs or a given timeout is reached, at which point it responds. If the response is a timeout rather than an update then the client has to re-submit the request for updates.

Several enhancements were introduced with Microsoft Exchange Server 2007 [3]. For example:

- Support for HTML messages.
- Support for follow-up flags.
- Support for fast message retrieval.
- Meeting attendee information.
- Enhanced Exchange search.
- Windows SharePoint Services and Windows file share document access.
- Password reset.
- Enhanced device security by using password policies.
- Autodiscover service for over-the-air provisioning.
- Support for Out of Office configuration.
- Support for Tasks synchronization.
- Direct Push.

Some of these enhancements require Microsoft Windows Mobile 6.0 or higher in the device.

With respect to the security configurations applicable to the server running EAS, an administrator can configure an authentication method [4]. By default the basic authentication with SSL is enabled. Microsoft recommends Digest authentication or Integrated Windows authentication. In addition, EAS for Exchange 2007 enables the administrator to create EAS mailbox policies to apply a common set of security settings to a collection of users. Some of these settings include:

- Requiring a password.
- Specifying the minimum password length.
- Requiring numbers or special characters in the password.
- Designating how long a device can be inactive before the user is required to reenter their password.
- Specifying that the device be wiped if an incorrect password is entered more than a specific number of times.

Furthermore, administrators can issue a remote wipe command from the Exchange Management Shell, or users can issue their own remote wipe commands from the Outlook Web Access user interface.

In summary, Microsoft claims that EAS technology delivers a rich mobile messaging experience on a breadth of mobile devices, while offering enhanced device security and management [5]. In this white paper we will examine those claims.

3. Supported Platforms

3.1. Exchange Data

With Microsoft Exchange 2003 and previous versions of Exchange the functionality provided by EAS was very limited in terms of data that can be synchronized and security settings. Basically, with Exchange 2003, only e-mail, contacts and calendar could be synchronized. The change in EAS protocol version from 1.0 to 2.0 made the devices supporting version 1.0, in practice, obsolete. Moreover, the changes in security settings and functionality introduced with Microsoft Exchange Server 2007 make only this latter version of Exchange worthwhile to consider for the purposes of this discussion.

With Microsoft Exchange 2007 and EAS, mobile users can synchronize e-mail messages, contacts, calendar and tasks. Mobile users cannot synchronize notes, but they can access Microsoft Office documents on a Windows SharePoint Services or Windows file share path, when using the latest Windows Mobile client.

If Microsoft Exchange Server 2007 Unified Messaging server role is deployed, voice mail and fax can be added to Exchange and therefore, through synchronization of their mailboxes, mobile users can have access to them.

3.2. Other Corporate Data

Any corporate data that is not available through Exchange cannot be accessed through EAS. In that case, a VPN connection with the device has to be provided. This prevents, for example, EAS access to non-Exchange corporate directories.

4. Supported Devices

4.1. Windows Mobile

Mobile devices with Windows Mobile software offer the greatest functionality when synchronizing with Exchange 2007. The table below shows some of the features that are available with different versions of Windows Mobile software [6][7].

Windows Mobile Software Feature Matrix					
		Windows Mobile 6.1	Windows Mobile 6.0	Windows Mobile 5.0 Plus Messaging & Security Feature Pack	All Windows Mobile powered devices
Productivity Enhancements	Direct Push	Yes	Yes	Yes	Yes
	HTML e-mail support	Yes	Yes	No	No
	Message flags	Yes	Yes	No	No
	Quick message retrieval	Yes	Yes	No	No
	Enhanced calendar views	Yes	Yes	No	No
	Meeting attendee information	Yes	Yes	No	No
	Out of Office management	Yes	Yes	No	No
	Exchange search	Yes	Yes	No	No
	Windows SharePoint Services and Windows file share (UNC) document access	Yes	Yes	No	No
	Synchronization of e-mail messages, calendar, and contact data	Yes	Yes	Yes	Yes

Windows Mobile Software Feature Matrix					
	Global address book lookup	Yes	Yes	Yes	No
	Task synchronization	Yes	Yes	Yes	No
Security Enhancements	Enforcement of Exchange ActiveSync mailbox policies	Yes	Yes	Yes	No
	Remote device wipe	Yes	Yes	Yes	No
	Certificate-based authentication	Yes	Yes	Yes	No
	S/MIME support (with Exchange 2007 SP1)	Yes	No	No	No
	Device storage card encryption	Yes	Yes	No	No
	Rights management support	Yes	Yes	No	No
	Secure Sockets Layer (SSL) encryption	Yes	Yes	Yes	Yes
	Basic authentication	Yes	Yes	Yes	Yes
	Integration with Internet Security and Acceleration (ISA) Server	Yes	Yes	Yes	Yes
Administration Enhancements	Detailed device monitoring	Yes	Yes	No	No
	Error reporting	Yes	Yes	No	No
	Microsoft Operations Manager integration and reporting	Yes	Yes	Yes	Yes
	Diagnostic tasks and health monitoring	Yes	Yes	Yes	Yes

4.2. Apple

The iPhone supports EAS, delivering push e-mail, calendar, and contacts over a 128-bit encrypted SSL connection.

4.3. Nokia

Nokia offers Mail for Exchange on 43 of their devices[8], enabling users to access their e-mail, calendar and contacts, tasks and company directory through EAS.

4.4. Sony Ericsson

Since 2007, Sony Ericsson has offered EAS as standard on all mid-level and high end handsets. Users can synchronize their e-mail, calendar, and contacts.

4.5. Palm

Palm Treo incorporated the Windows Mobile OS and Direct Push.

4.6. BlackBerry

Through third-party applications, e.g. AstraSync[9], support for EAS can be added to BlackBerry devices.

4.7. Laptops and Netbooks

Laptops and netbooks are not supported by EAS. They use the standard Outlook client which does not allow for background synchronization. For example, when a user enters a hotel room his or her BlackBerry is already up-to-date because new e-mail was pushed to the device while the user traveled. To work with e-mail on the laptop, on the other hand, the user has to first turn on the laptop, setup network connectivity, establish a VPN connection, start Outlook and wait for Outlook to synchronize with the Exchange server.

4.8. Device Summary

In summary, the Microsoft Exchange team claims that over 200 smart phones support EAS out of the box[10]. However the best user experience is only achieved with Window mobile devices, from which there are around 140 [11]. This number is less than 10% of all devices sold, which count for 1,332 [12], and it is also less than 10% of smart phones market. In comparison, RIM has 41% of smart phones market.

5. Typical Microsoft Exchange ActiveSync Implementation

The following figure shows a typical deployment [13] of Exchange Server with ActiveSync capability enabled to support mobile access.

Since direct push technology requires an established connection between the server and the client, the maximum length of the connection is determined by the lowest network timeout in the path between the device and the server. Setting the appropriate timeout in the firewall is an important parameter to minimize the number of times the device reconnects to the server, and therefore maximize the battery life of the device.

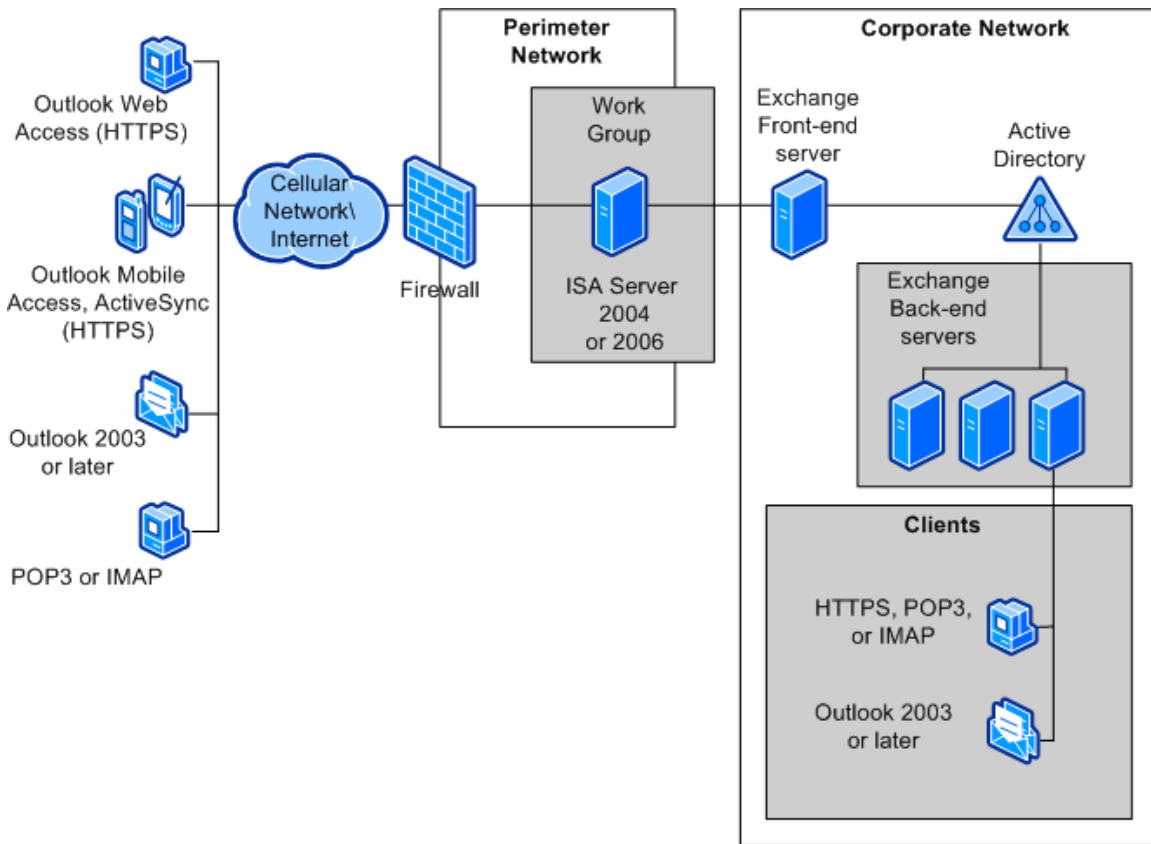


Figure 1: Typical Configuration Mobile Access to Exchange Server with ActiveSync

In addition, secure communication between the device and the server SSL encryption requires port 443 for incoming traffic in the firewall to be open.

In order to increase security and control of the devices, last year Microsoft introduced the System Center Mobile Device Manager (MDM) [14]. This software only works with Windows Mobile 6.1 and controls access to the corporation by establishing a mobile VPN connection.

6. Alternatives to EAS

At the enterprise level there are only two alternatives to EAS, which are described below.

6.1. BlackBerry Enterprise Server (BES)

The following figure shows the typical architecture of a BES deployment [15].

The BlackBerry Enterprise Server (number 1 in the figure) is placed behind the corporate firewall and includes all the modules necessary to access internal corporate data.

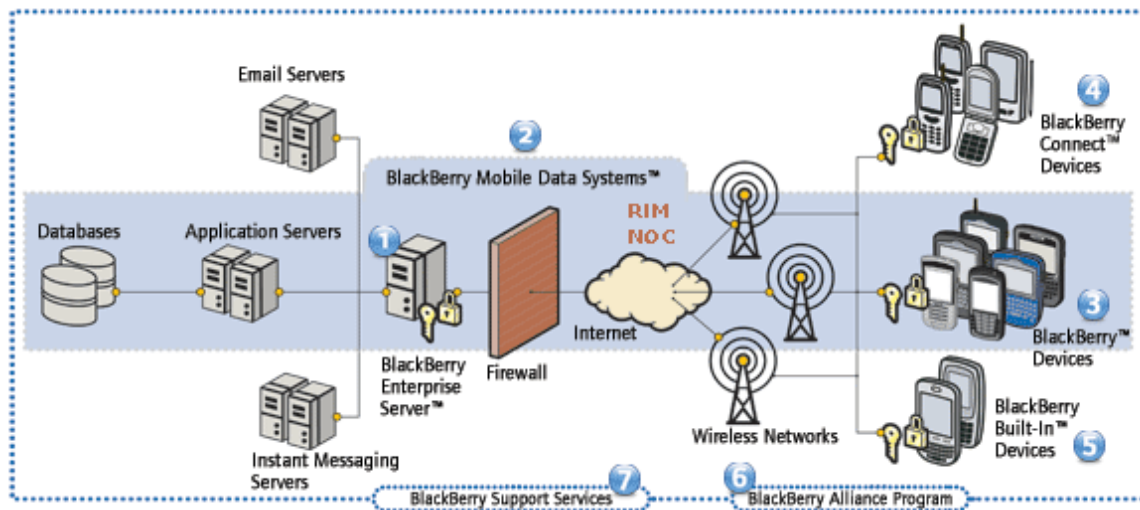


Figure 2: Typical BES (BlackBerry Enterprise Server) implementation.

The RIM Network Operation Center (RIM NOC) is a key part of the BlackBerry BES solution. This center operates from Canada and is the point where the BlackBerry device and the BES can find each other and communicate. The NOC takes care of handling individual BlackBerry connections and also queues up data that is destined for a BlackBerry when it is out of coverage or turned off. For a corporation, the only connection being used for all communication is the one that is established between BES and NOC. The traffic and uptime to the devices is handled by the NOC.

Every BES has a unique address called a Server Relay Protocol (SRP) ID, which allows the BES to log and identify itself to the NOC. This same SRP ID is included in the BlackBerry Service Book. When the BlackBerry is turned on, it registers with the RIM NOC using its PIN number, which refers to the SRP ID. Thus, since the RIM NOC is aware of both the BlackBerry and the BES, it allows them to communicate with one another via the RIM NOC.

During the activation of the BlackBerry device to the respective BES, which is done at the corporation, encryption keys are interchanged and then used for all communication.

6.2. Good Technology Mobile Messaging

Good Technology, which was recently acquired by Visto, offers a solution which is similar to BlackBerry. The following figure shows the Good Technology solution [16].

The Good Messaging Server resides inside the corporation and communicates with the corporation e-mail servers. Similar to RIM NOC, Good Technology operates a Good Network Operations Center in the USA. Finally, Good Mobile Messaging clients must be installed in the devices. The communication between the devices and the corporations are handled by the Good NOC and are end-to-end encrypted.

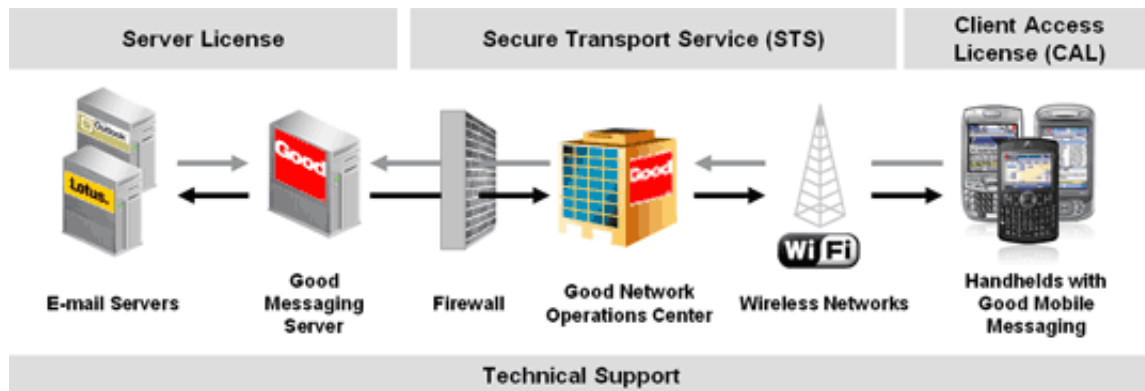


Figure 3: Good Mobile Messaging Solution from Good Technology

The Good Technology pricing scheme involves a server license, secure transport services and client access licenses. AT&T, Verizon and Bell Mobility are Good Technology resellers. When a user receives cellular service from one of these carriers, the user must purchase an authorized Good Data Plan which includes Good STS fees.

7. User Experience

When comparing the user experience provided by mobile devices supporting EAS and BlackBerry devices, many users consider the BlackBerry a more practical utilitarian device [17]. For example, BlackBerry users claim that they can forward attachments no matter how large they are in a second or two, because the BES performs the forwarding. On the contrary, when using an EAS solution they have to wait for the attachment to be downloaded and then sent. This can be very frustrating with a spotty connection as in the train or subway. Therefore, the RIM-type solution offers several advantages, which will be described next.

7.1. Wireless Carrier Agnostic

RIM's deployment of a network operations center (NOC) as a sub-network, allows users to utilize nearly any wireless carrier. In fact, the RIM NOC connects to more than 300 wireless carriers around the world.

7.2. True Push

Indexing BlackBerry devices on the network using PIN codes instead of assigning an IP address and maintaining the open connection, allows the BES server to call the device at any time to push information.

7.3. Scalability

The fact that the BlackBerry devices have a unique and permanent PIN or ID associated with their BES SPR ID, facilitates larger deployments than in the EAS case where there is no fixed IP address on the device.

EAS supported devices continually ping the network to prevent time-out and maintain their IP address, thus mimicking the push-like experience without a NOC. As these devices proliferate, scalability issues will arise as a growing number of devices are squatting on a finite allocation of IP-addresses.

7.4. Network Efficiency

The use of the NOC approach helps carriers manage traffic flow – throttling back at times of capacity overload. Also, as a central point, there is control and options for improvement to compression and routing. An example of this is RIM's Dynamic Packet Allocation (DPA) technology, which determines how many packets (and how quickly) a BlackBerry can accept based on connection quality in a specific cell-site, among other factors.

In addition, RIM's BES component manages bandwidth consumption by reducing the size of the data packets through proprietary compression technologies better suited for wireless transfer.

Finally, in comparison with EAS solutions, EAS supported devices consume in excess of 2–10 times the bandwidth of RIM's approach because of their permanent IP sessions.

7.5. Battery Life

The fact that the BlackBerry devices are in listening mode rather than in active ping-ing state increases battery life as compared to their EAS counterparts.

7.6. Easier for IT Managers

The BES architecture provides IT managers with a single point of management for an entire fleet of hand held devices belonging to an organization, including remote activation, security “wiping”, and the ability to perform over-the-air software installation. In addition, RIM provides a suite of tools for reporting and logging, apparently superior to Microsoft's offering.

8. Security

8.1. Transport Security

A recent report from American Technology Research [18] identified several technical limitations in the EAS approach, including: 1) security, 2) scalability, 3) network efficiency and 4) power efficiency, as well as nontechnical issues related to multiple vendors' involvement (Microsoft, device maker, carrier).

In particular, the report indicated that security may be a major drawback due to EAS's reliance on an inbound port remaining open on the device (users are more likely to misplace or lose a hand held device than similarly configured notebook computers running Outlook). In addition, the report points out scalability concerns brought about by the lack of a fixed IP address on cell phones.

This requirement of leaving an inbound firewall port open increases the opportunity for denial of service attacks, and the opportunity for “bad packets” to reach the devices.

Furthermore, the BES server and the BlackBerry hand held share a unique randomly generated security key based on triple-DES encryption. The BES server encrypts all information with this key while behind the corporate firewall. The only decryption key in existence resides on the hand held device, which gives BlackBerry the highest level of security in the industry, according to the report.

As such, the analysts noted that RIM is the only vendor to have thus far received top-level security accreditations in North America and Europe. This has helped make BlackBerry the exclusive smart phone of security conscious agencies like the US Department of Defense and the Department of Homeland Security. For this reason, the analysts say "claims of security issues raised by ActiveSync advocates seem completely meritless."

8.2. Device Policies

Device policies are not trivial to enforce. An enterprise can either limit usage to Windows Mobile 6.1 devices to get reasonable control over policies or it can open access to all devices. In the latter case, an enterprise cannot prevent a user from connecting his or her private cell phone to the enterprise Exchange server. For example, if an organization wants to support company issued iPhones, it cannot prevent personal iPhones from connecting to Exchange.

9. Exchange Replacements

The Microsoft Exchange Server's ability to let users easily share information using a familiar structure such as mail and folders contributed to its early success. However, as Exchange has grown to meet the needs of the largest organizations (and increased its cost), it surrendered the simplicity that let smaller organizations with fewer technical resources use it comfortably. Several companies have attempted, with different degrees of success, to capture a part of the Microsoft Exchange server market share. All of them are Outlook compatible or offer an Outlook plug-in, allowing an organization to migrate from Exchange without the need to install new client software and without the end users noticing. The following paragraphs describe some of them.

9.1. PostPath (Cisco)

PostPath [19] is a Linux-based e-mail, calendaring and collaboration solution, which offers an AJAX web client and is compatible with several mobile devices. PostPath was acquired by Cisco in September 2008 to enhance their collaboration portfolio.

9.2. Zimbra (Yahoo)

Zimbra [20] is an open-source collaboration suite, which provides e-mail, calendar, address book, and mobile devices support, among other features. Zimbra was acquired by Yahoo! in September 2007.

9.3. Open-Xchange

Open-Xchange [21] is another open-source collaboration suite, which is offered as an appliance, a server or a hosted solution, and also includes support for mobile devices.

9.4. Scalix

Scalix [22] is another Linux-based open-source collaboration suite. Similar to all the previously described solutions.

9.5. Unison

Unison [23] is server/client solution for unified communication, which attempts to replace e-mail server, instant messaging solution and corporate PBX. Its novelty is that it's free if the users accept some advertisement.

9.6. Citadel

Citadel [24] is an open-source e-mail and groupware solution, which even supports push e-mail and mobile devices.

9.7. Lotus (IBM)

Lotus [25] is the IBM offering for collaboration with a large set of features and integration modules to compete head-to-head with Microsoft offerings.

9.8. Novell Open Workgroup Suite (NOWS)

NOWS [26] is another competitor of IBM and Microsoft in the collaboration arena, which almost a year ago released this open-source version.

9.9. Openchange

As a consequence of the European Community lawsuits against Microsoft, Microsoft was forced to release several of their protocols. As a result of this, the Openchange project [27] was created with the goal to provide a portable open source implementation of Microsoft Exchange Server and Exchange protocols.

9.10. The Future of Enterprise E-Mail

While Microsoft has a firm lock on the market dominance of its Outlook client, there are signs that it may lose market share of its Exchange server. A 2008 Computerworld article [28] describes several cases where organizations have reduced cost by replacing their Exchange servers with a different product without impacting their end users. Furthermore, the article states that "there is definitely a trend in the data center toward Linux."

Another indication that third parties may take market share away from Exchange is the fact that two large companies (Cisco and Yahoo) recently purchased two of the Exchange replacement vendors (PostPath and Zimbra). It appears that Cisco and Yahoo see a growing market for Exchange replacement products.

The main Exchange functionality in use is e-mail and scheduling. That functionality has not changed significantly in many years which makes it hard for a single company like Microsoft to maintain near-monopoly status of a product.

If third-party Exchange replacement products do gain in popularity then the importance of EAS will be reduced.

10. Conclusions

Microsoft EAS essentially promises to provide the same functionality as the BlackBerry but without the extra cost of a BlackBerry Enterprise Server and with support of many devices from many vendors. However, several key factors limit this claim:

- ◆ To be anywhere near BlackBerry security, an organization has to limit the devices to Windows Mobile 6.1 which is a tiny percentage of the devices sold.
- ◆ Device policies are not trivial to enforce. An enterprise can either limit usage to Windows Mobile 6.1 devices to get reasonable control over policies or it can open access to all devices. In the latter case, an enterprise cannot prevent a user from connecting his or her private cell phone to the enterprise Exchange server. For example, if an organization wants to support company issued iPhones, it cannot prevent personal iPhones from connecting to Exchange.
- ◆ EAS requires the enterprise to leave an incoming port through their firewall open in order for EAS devices to access Exchange. This is another security concern because it lets hackers exploit vulnerabilities of the Exchange server which would otherwise not be exposed to the outside.
- ◆ The user experience has significant flaws. For example, in order to forward an attachment, an EAS user has to first download the entire attachment to the device, then upload it again to send it out.
- ◆ Bandwidth requirements of EAS devices are typically 2-10 times higher compared to BlackBerry requirements for the same service.
- ◆ The battery life of a device is reduced when using EAS.
- ◆ One of the most important travel e-mail devices, i.e., the laptop, is not supported. Laptops have to use the traditional VPN configuration and do not get the benefit of e-mail push while on the road. Users therefore still waste a lot of time, e.g., after entering a hotel room, before their laptop is ready and has synchronized with Exchange.
- ◆ While numerous devices do support EAS (most of them with limited security), a secure web based mobile e-mail access system would have far greater reach and also give the enterprise more control over the features and user interface.
- ◆ There seems to be no support for Linux phones and open source phones (such as Google Android).
- ◆ Enterprise data access is limited to Exchange. This prevents it, for example, from being integrated with other valuable data sources, such as missed call log.
- ◆ EAS requires Exchange version 2007 which is not yet widespread and which only runs on 64-bit architectures (EAS support in Exchange 2003 is very limited).
- ◆ BlackBerry provides superior system administration tools compared to EAS.

In the end, true control of security requires true control of the client. This is best done with two levels: 1) web access, and 2) additional client custom software for enhanced user experience, such as an offline mode.

Furthermore, web access can let enterprises control the UI (Exchange only lets them control what data can be accessed but not the functionality or the page flow, i.e., application control).

Bibliography

- [1] Microsoft, Exchange Server 2007 Support for Mobile Devices, 2007, http://www.microsoft.com/australia/servers/exchange/evaluation/features/owa_mobile.aspx
- [2] Microsoft, Microsoft Exchange ActiveSync Licensees, 2009, http://www.microsoft.com/exchange/evaluation/features/owa_mobile.aspx
- [3] Microsoft, Client Features in Exchange ActiveSync, 2007, <http://technet.microsoft.com/en-us/library/aa996303.aspx>
- [4] Microsoft, Managing Exchange ActiveSync Security, 2007, <http://technet.microsoft.com/en-us/library/bb232020.aspx>
- [5] Microsoft, Exchange Server 2007 Product Overview, 2008, <http://www.microsoft.com/exchange/evaluation/overview/default.aspx>
- [6] Microsoft, Understanding Mobile Devices, 2007, <http://technet.microsoft.com/en-us/library/bb232129.aspx>
- [7] Microsoft, Exchange ActiveSync Devices and Compatible Features, 2009, <http://technet.microsoft.com/en-us/library/bb232162.aspx>
- [8] Nokia, Microsoft Exchange ActiveSync to 43 Nokia S60 3rd Edition devices, 2008, <http://blogs.s60.com/2008/09/microsoft-exchange-activesync-to-43-nokia-s60-3rd-edition-devices>
- [9] AstraSync, AstraSync, 2009, <http://www.astrasync.com/>
- [10] Microsoft Exchange Blog, Mobile Device Connectivity to Exchange using IMAP vs Exchange ActiveSync , 2009, <http://msexchangeteam.com/archive/2007/07/10/446015.aspx>
- [11] UnwiredView.com, Microsoft to limit number of Windows Mobile devices on the way to announcing something major at MWC 2009, 2009, <http://www.unwired-view.com/2009/01/09/microsoft-to-limit-number-of-windows-mobile-devices-on-the-way-to-announcing-something-major-at-mwc-2009/>
- [12] Getjar.com, Manufacturer market share in North America - United states (February 2009) , 2009, <http://stats.getjar.com/statistics/NA-US/manufacturer/All>
- [13] Microsoft, Step-by-Step Guide to Deploying Windows Mobile-based devices..., 2006, <http://go.microsoft.com/fwlink/?LinkId=118666>
- [14] Microsoft, MDM System Overview, 2008, <http://technet.microsoft.com/en-us/library/cc135589.aspx>
- [15] BlackBerry.com, BlackBerry Enterprise Server (BES) - What is it?, 2009, <http://blackberry.com/blackberry-enterprise-server-bes-what-it>
- [16] Good Technology, Structure Overview, 2009, http://www.good.com/corp/collateral/whitepapers/Good_Mobility_Suite_WP.pdf
- [17] BlackBerry Forums, BEA vs. ActiveSync, 2008, <http://www.blackberryforums.com/blackberry-versus/141490-bes-vs-exchange-activesync.html>
- [18] Marsal K., Push email systems from RIM, Apple set to square off, 2008, http://www.appleinsider.com/articles/08/03/10/push_email_systems_from_rim_apple_set_to_square_off.html

- [19] Cisco, PostPath Acquisition and the Cisco Collaboration Platform, 2008, http://blogs.cisco.com/collaboration/comments/postpath_acquisition_and_the_cisco_collaboration_platform/
- [20] Zimbra, Zimbra, 2009, <http://www.zimbra.com/>
- [21] Open-Xchange, Open-Xchange, 2009, <http://www.open-xchange.com/>
- [22] Scalix, Scalix, 2009, <http://www.scalix.com/>
- [23] Unison, Unison, 2009, <http://www.unison.com/what-is-unison/overview.php?ref=what-is-unison>
- [24] Citadel, Citadel, 2009, <http://www.citadel.org/doku.php>
- [25] IBM, Lotus, 2009, <http://www-01.ibm.com/software/lotus/>
- [26] Novell, Novell Open Workgroup Suite, 2009, <http://www.novell.com/products/openworkgroupsuite/>
- [27] Openchange, Openchange, 2009, http://www.openchange.org/index.php?option=com_content&task=view&id=15&Itemid=49
- [28] Todd R. Weiss, Linux-based Exchange Replacement Helps 3 Health Care Systems Cut Costs, 2008, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Software&articleId=9109998&taxonomyId=18&pageNumber=1>